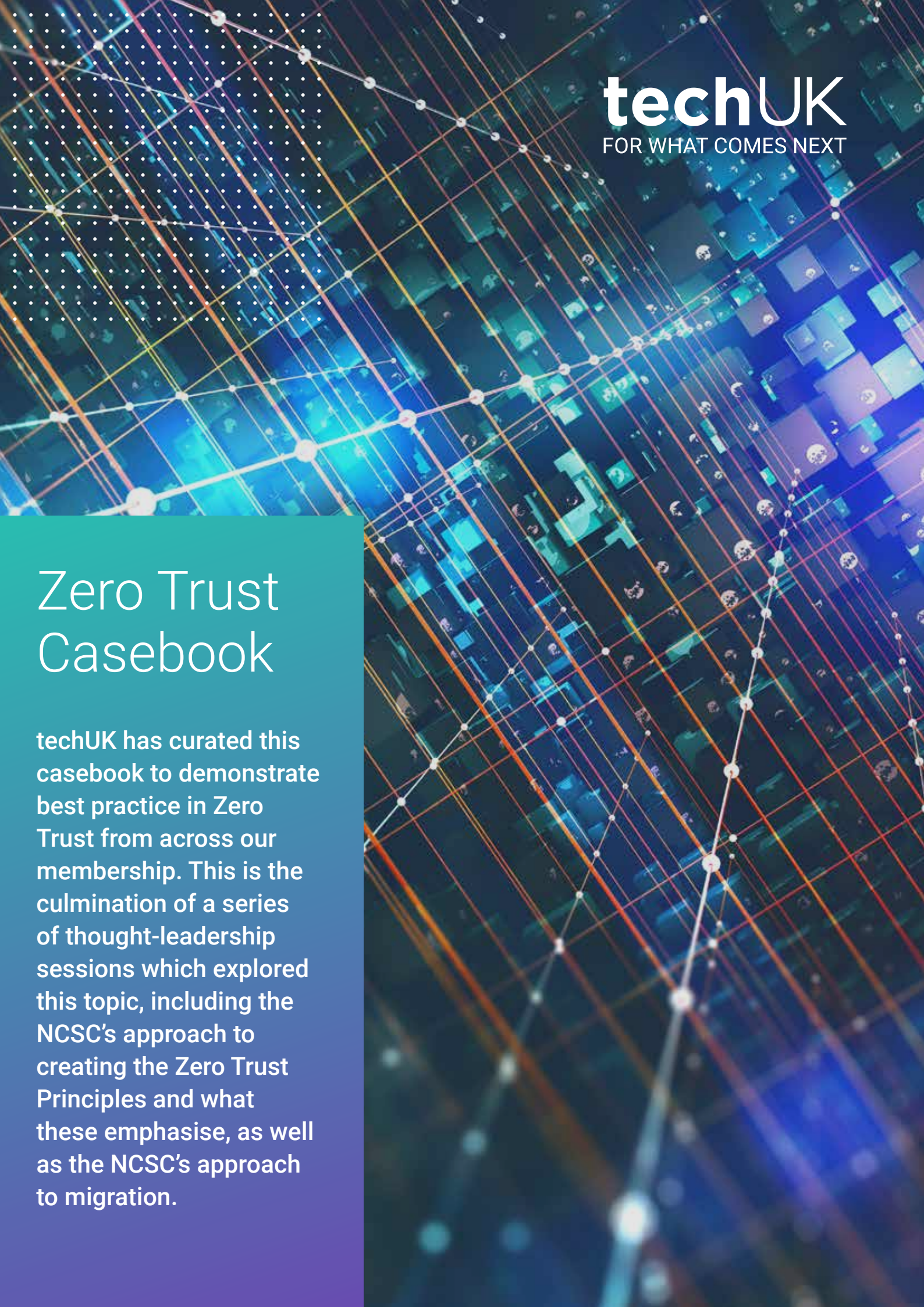
techUK
FOR WHAT COMES NEXT

Zero Trust Casebook

techUK has curated this casebook to demonstrate best practice in Zero Trust from across our membership. This is the culmination of a series of thought-leadership sessions which explored this topic, including the NCSC's approach to creating the Zero Trust Principles and what these emphasise, as well as the NCSC's approach to migration.



Foreword | Dr. Bernard Parsons MBE CEO, Becrypt

I have recently had the fortune and pleasure of Chairing a number of techUK Zero Trust workshops that have bought together diverse representation from industry and government, and included the participation of architects from the National Cyber Security Centre (NCSC).

This case book represents one output of this collaboration, forming a suitably diverse collection of perspectives and capabilities provided by a number of techUK industry members. Zero Trust is a topic that invites a wide range of perspectives. Today Zero Trust is defined by NIST[1] as

"A collection of concepts and ideas designed to minimize uncertainty […] in the face of a network viewed as compromised".

There continues, however, to be much debate and variety of definition. Given the term's popularity, I was surprised a year or so ago by the absence of a Wikipedia entry for Zero Trust. Out of interest and amusement, I used NIST's definition and a summary of NCSC's emerging Zero Trust principles to help author a page that has slowly evolved with new insights and perspectives. Typically, the common ground of contributors here and elsewhere is that while not a new concept, the absence of clearly defined network perimeters, which is at the heart of the Zero Trust rationale, has grown in significance for most organisations, resulting from the increased prevalence of technologies such as mobile and cloud, and the increased interconnectivity of our industries and economies.

The diversity of technologies and corporate IT infrastructures requires that Zero Trust is defined through the use of tenets or principles that describe what should be achieved or at least aimed for, as opposed to what might be excluded (e.g. a corporate VPN).

Removing inherent trust from the network, requires an organisation to undertake its own unique journey to establish how confidence can be established for the transactions that occur on its networks.

This case book has been compiled by techUK to reflect various parts of such journeys being undertaken or supported by member organisations. Contributions include approaches to phasing a journey to Zero Trust, assessing its relevance and potential benefits, and assessing organisational maturity of implementation. Tools and technologies discussed range from the essential components of authentication; network and micro segmentation; monitoring an analytics, including gaining visibility into encrypted data; the potential role of AI; and supporting dynamic policy enforcement within the mobility space.

Contributions explore the application of Zero Trust within sectors such as Defence, Medical, Utilities, Border security and the Supply Chain, with the latter referencing some early work on Zero Trust supported by NCSC.

On behalf of participating organisations, I would like to thank techUK for organising the recent Zero Trust workshops that generated interesting debate amongst members and broader stakeholders, and creating a case book that through its diversity will hold some value to any with an interest in the evolving topic of Zero Trust.

1 US National Institute of Standards and Technology.

Contents

TriCIS
Secure Integrated Solutions

Booz | Allen | Hamilton®

DISTRICT DEFEND®

SECURE MOBILITY

OVERVIEW

Organisations today understand the need to embrace mobility but doing so comes with inherent risks that many organisations are not adequately equipped to assume. Cyber-attacks become more sophisticated daily, and employee negligence results in an ever-increasing number of breaches that cost organizations millions to contain and remediate.

In Fiscal Year 2018-2019, the United Kingdom (UK) Ministry of Defence (MoD) reported 62 incidents of lost electronic devices or paper records. Another report showed that total losses of data and devices within the MoD exceeded 450 incidents in Fiscal Year 2019, an increase of nearly 300% over the two financial years prior. After accounting for downtime, support, and management time, estimated costs for a single data breach can exceed £40,000 per device, resulting in tens of millions of pounds of cost that can be minimized by implementing proper cybersecurity policies and practices. Even more damaging than the financial impact, is the potential loss of classified data – impacting critical missions or jeopardizing lives.

While the risks associated with lost data and devices are high, the advantages of adopting mobility are well understood: organizations see a 34% increase in overall productivity, while individual employees save 58 minutes per day as a result of going mobile. These improvements not only mean more work gets done, they also provide cost savings, workplace flexibility, and improved employee retention. When considering each of these factors together, there is a significant quantifiable business impact from adopting mobility, and it becomes clear that for organizations to survive and thrive in the future, they must embrace mobility and develop a strategy to manage the associated risks. Mobile technology also provides defence and intelligence members with immediate access to critical information when they need it most; no longer limiting the ability to perform mission critical work or make timely decisions.

Booz Allen Hamilton developed District Defend® - a location-based, context aware platform that dynamically enforces configurable security policies for endpoint devices, even when powered off - to address gaps in the mobility space by bridging the intersection of proactive protection, Zero Trust access on existing devices, and availability everywhere users are approved to support their mission. District Defend takes advantage of a convergence of technology from the commercial sector, lessons learned from defending the United States (US) Federal Government from nation-State actors, and novel concepts from some of the world's best innovators to establish a technology solution able to meet the most challenging needs of the UK MoD. TriCIS Ltd partnered with Booz Allen whose experience

building mobile and wireless platforms across the Department of Defense (DoD) and Intelligence Community (IC) informed our approaches for enabling flexibility and modular designs for automated protections, data security, and endpoint hardening.

ENTERPRISE APPLICATIONS

Remote Monitoring and Management of Enterprise Assets

The Challenge

UK MoD security administrators are faced with the challenge of continuously tracking how many devices are active in the enterprise, where they are, who owns them, and how they behave. Staff and leaders are required to move through various spaces within MoD facilities to execute their mission responsibilities, and these spaces often have unique organizational security policies.

As a result, many staff and leaders are forced to carry multiple devices, as well as understand – and comply with – security requirements across different spaces, adding significant complexity to the monitoring and management of enterprise assets. Administrators need a tool that enables them to remotely monitor and manage enterprise end point devices without having to rely on end user compliance to protect mission sensitive data and information.

How District Defend Enables the Mission

District Defend enables security administrators to establish 'Districts' for each organization, with policies that determine and automatically enforce how devices behave based on organization, physical location, contextual behaviors, user rank, and/or clearance level. Administrators gain access to valuable pattern-of-life data, allowing them to perform advanced threat analytics with tools such as Splunk to inform decision making for devices within MoD spaces and beyond.

Automated Defense for Lost or Stolen Devices

The Challenge

As today's missions become increasingly globalised, it is not only assumed, but expected that staff and leaders will traverse multiple countries and time zones, all within the span of a few days. This means countless hours spent in airport terminals, hotel rooms, and conference halls. Malicious actors exploit the vulnerabilities associated with these scenarios and often seek to gain physical access to endpoints.

Additionally, the portable nature of today's classified workstations increases the potential for insider threats to remove devices from classified environments. These devices can be used to export classified data; or can be modified with malicious software and reintroduced into the classified environment to infect other systems and networks.

How District Defend Enables the Mission

District Defend continuously checks for contextual security triggers to ensure data is only accessed by authorized users and responds to changes in user or environmental conditions to enforce defensive actions. Required 'check-ins' and wipe timers ensure devices (and stored data) are not left unprotected for extended periods. Virtual boundaries ensure stolen devices are automatically disabled and/or wiped if removed without authorization. Administrators can also execute a remote forensic wipe of the devices as well, providing added flexibility and security.

Responding to Catastrophic Threats

The Challenge

The UK government and MoD has access to some of the most sensitive information in the world, and this information frequently must be accessed from hostile or remote environments. In the event of a catastrophic event requiring widespread containment action, system administrators must dispose of, or otherwise protect, all data and information that would pose a risk if it fell into the wrong hands. Similarly, troops rely on classified operational data while on the go – potentially jeopardizing valuable data in the case of vehicle disablement or overrun.

Traditional containment strategies (including burn bins and physical destruction of devices) lose valuable time in these scenarios, creating a heightened risk of data spillage. The government needs to be able to instantly react to evolving threats and take immediate action to protect mission data and national security.

How District Defend Enables the Mission

District Defend leverages enhanced security to prevent physical device compromise and enforce agency-approved architectures to securely connect to classified networks from unclassified access points outside of agency control**.** A variety of device lockdown and data wipe options provide deployed users with numerous options to secure devices against unexpected threat scenarios. Devices can be secured into a "thin" mode of operation, limiting access to information from a dedicated Virtual Desktop environment and reducing the threat signature by not allowing data on the device in remote access scenarios.

CLASSIFIED APPLICATIONS

Leadership Briefing Books and Executive Classified Workstations

The Challenge

Today's military leaders are often forced to consume complex, multi-dimensional mission and intelligence data in static, text-based formats. Briefings can be conducted in a variety of environments with different security rules and requirements, as well as network access. Leaders need hardened devices that can safely store and secure classified data locally, while also connecting to approved networks when available. Unfortunately, local storage of highly classified data introduces risks as devices are moved frequently between facility spaces.

Additionally, many leaders are forced to switch between multiple devices for different use cases, scenarios, and operating environments. This requires managing, maintaining numerous endpoints; as well as complicating their ability to take notes, respond quickly, and consume all necessary information for critical decisions.

How District Defend Enables the Mission

District Defend enables leaders to use classified endpoints to consume and collaborate on valuable mission data without the need to worry about manually safeguarding actions. District Defend automatically conforms devices to each environment (enabling/disabling components as appropriate) and provides the ability to lock and/or forcibly shut down and disable devices if removed by unauthorized personnel.

MISSION APPLICATIONS

Data Defense for Front-Line, Forward Deployed Mission Scenarios

The Challenge

Critical missions can force field operatives to be deployed to high-risk environments at a moment's notice to observe and report developing situations at the mission's edge, collecting critical data in the process. Additionally, the transportation of devices across the World introduces risks of tampering and malicious compromise.

Operators in these tactical environments are frequently targeted by nation-state style attacks for counter-intelligence purposes. To protect against these threats, they need tools that minimize attack vectors by preventing unauthorized users from accessing or stealing critical data.

How District Defend Enables the Mission

District Defend enabled devices can be equipped with a proprietary secure file system that allows operators in hostile environments to take notes, encrypt them, hide the files, and once back online send the encrypted files securely to agency servers. When necessary, field operatives can enter a secret, unique keystroke to wipe their secure notes/files to ensure classified data is protected. Secure 'locked-in-transit' capabilities enable the secure transportation of devices in hostile or physically vulnerable environments.

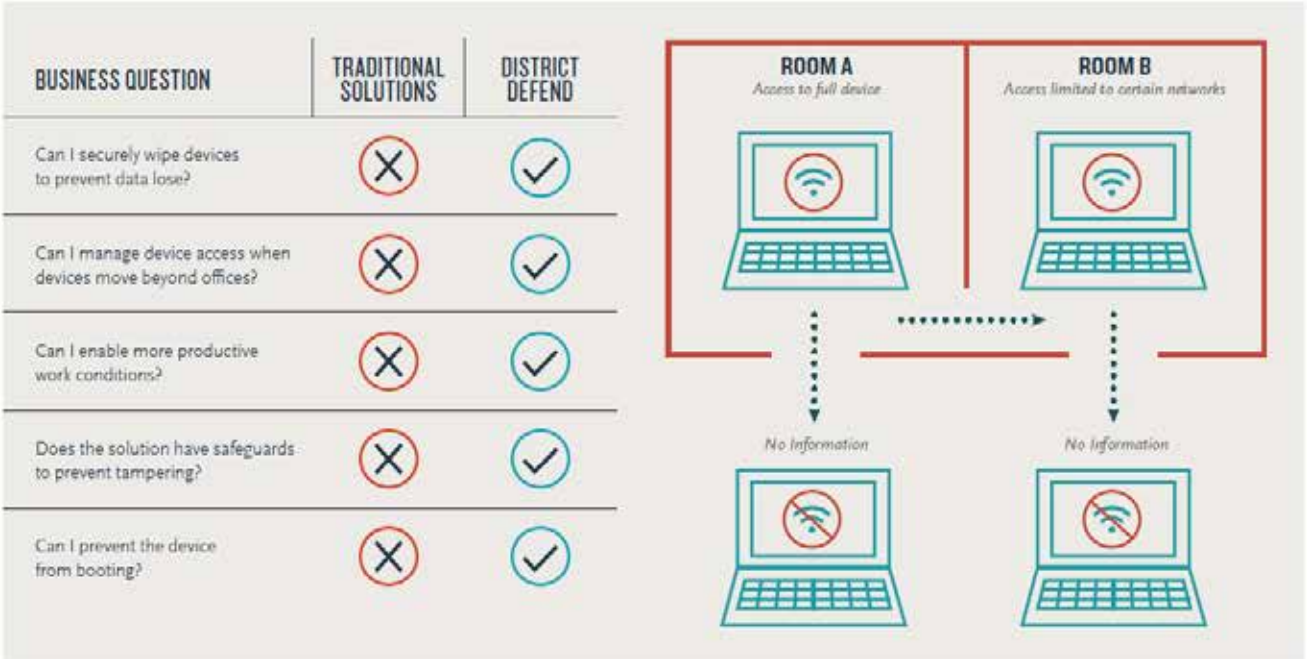
Secure Data-in-Transit in Tactical Environments

The Challenge

Deployment of secure, mobile capabilities across the Ministry of Defence landscape requires confidence that classified mobile devices are used only in the way they are authorized, to include operating only within approved spaces such as aircraft or tactical vehicles. Operators require a solution that disables vulnerable hardware components, prevents adversarial access in case of aircraft/vehicle loss, protects content while the device is in transit, and reduces the need to "trust" that an operator will follow established protocol.

How District Defend Enables the Mission

District Defend was architected to ensure the security of data-in-transit, regardless of end-user environment. Not only can users take their devices between approved static locations, but District Defend can be deployed in various aircraft and/or ground-based vehicles. In these scenarios, District Defend uses a 'heartbeat' model for intermittent policy delivery to enable systems operations within an aircraft or vehicle environment. Administrators receive notifications when District Defend enabled devices leave the controlled section of a vehicle, and devices will automatically shut down and/or execute a full disk wipe if removed from the vehicle.



TAKE THE NEXT STEP

Talk to a team member about options for deploying District Defend in your enterprise.

www.tricis.co.uk
www.DistrictDefend.com

ABOUT BOOZ ALLEN HAMILTON

Booz Allen Hamilton is at the forefront of technological innovation, collaborating with clients, academic institutions, and the business community to address urgent information security challenges. Having been engaged in offensive and defensive cyber capabilities surrounding the nation's most sensitive data, Booz Allen's computer forensic experts know firsthand which data and application-protection solutions are most effective, and how to render them ineffective. Drawing on this expertise, Booz Allen's engineers developed District Defend, a new way to protect mobile devices in civil, IC, health, and commercial environments without sacrificing either device security or employee productivity.

FOR MORE INFORMATION, PLEASE CONTACT:

Ann-mariewarner-read@tricis.co.uk
Jeffvanhorn@tricis.co.uk

Case Study

FORESCOUT
Active Defense for the Enterprise of Things™

South Central Power Company

Electric Utility Gains Visibility, Compliance and Zero Trust Network Segmentation with Forescout

$600,000+
saved in three-year ROI benefits

1 WEEK
to discover all devices

5+ MONTHS
saved on asset inventory

Industry
Utilities/Energy

Environment
1,400 wired and wireless devices across five locations; 250 employees

Challenge

- Lack of visibility into all devices on the network
- Physical segmentation of network causing visibility blind spots
- Compliance with PCI and critical infrastructure regulations
- Confidence that security tools in layered, multivendor defense are doing their job
- Enforce policies without disrupting operations

Overview

South Central Power Company (SCP) is a member-owned electric utility serving more than 120,000 residential, commercial and industrial customers across 24 counties in the U.S. state of Ohio. To provide continuous device visibility, network access control (NAC) and network segmentation, rather than turn to multiple vendors, the company implemented the Forescout platform. With the Forescout solution, the company achieved 100% device visibility and control while simplifying and accelerating the design and deployment of Zero Trust network segmentation and reaping additional efficiencies estimated to save more than $600,000 in three years.

Business Challenge

"Besides helping us to see more clearly, we wanted a 'Big Brother' to double-check our other security tools. We also knew we needed help with segmentation."
— Jeff Haidet, Director of Application Development and Architecture, South Central Power Co.

Despite its multilayered defense and multivendor security stack with best-of-breed security tools, South Central Power Company still had no idea how many devices were on its network. To protect personally identifiable information (PII) and business operations and comply with PCI regulations, the SCP security team knew they needed a way to continuously identify, segment and enforce compliance of every connected thing on its heterogeneous network. They also desired a way to validate that other security tools in the environment provided accurate information and performed as intended. In addition, SCP staff suspected that the corporate network's physical design hindered security but did not know how to confirm the problem or implement more logical segmentation.

Security Solution

- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeSegment
- Forescout eyeExtend for Carbon Black

Use Cases

- Network access control
- IoT security
- Network segmentation
- Asset inventory
- Device compliance
- Security orchestration

Results

- Rapid time to value – full visibility and 100% device classification in weeks
- Continuous, comprehensive visibility across all network-connected things
- Accurate, real-time asset inventory system replaced cumbersome manual method
- Simplified, accelerated Zero Trust network segmentation, thanks to a clear understanding of traffic flows and ability to simulate policy changes
- Ability to switch network hardware without penalty due to vendor-agnostic visibility
- Oversight to validate other security tools in the environment
- Zero Trust NAC to block rogue and noncompliant devices
- Visibility and control that aids both security operations and networking teams daily
- Significant ROI – $612,500 three-year savings projected

Why Forescout?

During an independent penetration test that reconfirmed the need for better visibility and NAC, the pen tester highly recommended Forescout. They implied that if the Forescout platform is on site when they arrive, it has already done their job. This glowing recommendation led the company to learn more about the solution, which led to a deep-dive proof of concept. "As soon as we saw and understood the power of the Forescout platform to bridge visibility and control security gaps – and of eyeSegment to noninvasively rectify segmentation shortfalls – we knew that it was what we were looking for," claims SCP Manager of Applications and Security Jeff Haidet. "Vendor independence was also a huge selling point because we are constantly upgrading or replacing networking hardware."

Business Impact

Comprehensive Visibility Opens Eyes and Overhauls Asset Inventory

The Forescout platform was up and running and providing granular visibility in hours. The SCP security team then let it run for a week. It discovered a total of 1,400 endpoints – an average of seven to eight endpoints per employee, which made a significant impression on senior management. The system auto-classified 85% of the devices, with the remaining devices classified shortly after that. Without the Forescout platform, locating and classifying all devices in the company's five locations would have easily taken six months, if it happened at all. Such comprehensive, real-time visibility allowed SCP to scrap its inaccurate, paper-based asset inventory process. Processes for onboarding and offboarding equipment also improved dramatically.

Non-Disruptive Approach to Zero Trust Segmentation

To improve segmentation, Haidet and his team turned to Forescout eyeSegment. "We used eyeSegment to map traffic flows and determine which devices, users and services on the network need to talk to each other," explains Haidet. "The ability to logically define segments, as opposed to physically defining them, accelerates visibility into behavior. For example, eyeSegment showed us how two different groups of devices were passing information back and forth from one switch port to another undetected because their communication never hit a gateway. So, we moved gateways to gain the visibility we need. It is also helping us redesign our physical segmentation and do so noninvasively. We can simulate policies to see if anything breaks, and fine-tune and re-simulate as needed before we actually implement."

Oversight for Device Compliance and Security Tool Validation

SCP security uses the Forescout platform to continuously monitor endpoints for the presence of appropriate antimalware agents and patching, as well as for critical vulnerabilities or unauthorized apps like Dropbox. If a device does not comply with corporate policy, the Forescout platform blocks it from accessing the corporate network or pushes it to the guest network. "When the Covid-19 pandemic caused most of our employees to work from home via VPN, the ability to continue monitoring their device's compliance became even more important," notes Haidet. "In addition, Forescout lets us double-check that the pieces of our layered security stack – from firewall to switch to antivirus – are doing what they need to be doing."

"To gain the functionality that Forescout provides—from seeing and managing assets to triggering control actions and accelerating Zero Trust segmentation—we would have needed multiple tools. Going with Forescout was far more cost-effective."

— Jeff Haidet, Director of Application Development and Architecture, South Central Power Co.

A Truly Collaborative Partnership and Undeniable Business Value

At South Central Power Company, both security operations and networking teams rely on the Forescout platform daily. "The Forescout team is also an extension of what we do," notes Haidet. "We have a truly collaborative relationship – which is very difficult to achieve with vendors when you acquire new tools. I think we've hit a homerun here. With just 250 employees, we're small potatoes for Forescout. However, the level of support and commitment Forescout has given us makes us feel like a Fortune 100 company."

To quantify the economic benefit of turning to Forescout, Haidet used a customer-based ROI tool developed by IDC. The ROI analysis showed $612,500 savings over three years from IT staff efficiencies, risk mitigation and business productivity benefits and IT infrastructure cost reductions. When talking with peers, Haidet tells them: "Forescout is your vendor-agnostic, 'one-stop oversight shop.' The bigger your network gets, the bigger the cost savings and stronger your case for it becomes."

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com

unival group and oneclick accelerate physical security checks by a factor of 25

In today's threat landscape, well-organized cybercriminals are working to steal your data for economic, political or military gain. To counteract this, it is recommended that security managers should implement a Zero Trust model and develop robust processes for detecting and responding to incidents. Zero Trust has become the security model of choice for businesses and government agencies. Implementation does not require abandoning of all current security controls to start over.

The oneclick™ platform is based on the principles of a Zero Trust Architecture (ZTA). In this approach, no actor who wants access to resources or services in the network is trusted from the outset. Every access, whether from outside or inside, is individually authenticated. Users are not only checked each time they log in, but their trust status is continuously validated during the sessions. If a change is detected that poses a risk, the granted access to a service is interrupted. Zero Trust focuses on the protection of defined company resources instead of individual network segments.

This approach to security appealed unival group, that offers a wide range of integrated and AI based security control systems for State borders, security check points at prisons, industries, sports and event arenas. Implementation and management of these security control systems is complex, expensive and lengthy process. Any delays caused by the system can have drastic impact on the processing times and the economy. This situation came to the forefront during current pandemic due to necessity of thermal scanning of passengers and individuals at various locations. The company also had to consider safety of the on-site operators of these systems.

To increase efficiency and security of the operators, unival's control systems were to be connected to the cloud so that they could be operated and processed remotely at a secure

location. In order to achieve this objective, large image files must be transferred via the Internet to achieve the desired productivity gains. Imaging security and thermal scanners can generate files several hundred MB to several GB in size per scan based on resolution and use of several sensors. Besides secure delivery of the images to a remote-control centre, having a trusted security solution was also of utmost importance as the solutions are implemented in the most secure-sensitive areas of a country.

To solve the problem, unival selected oneclick™ platform due to its adherence to Zero Trust, use of streaming technology and ease of implementation.

“For future logistics applications, the speed and processing of the data will have a considerable influence on real-time handling,” says unival managing director David Vollmar. “The new formula is, time is money is security, because current figures clearly show that a large proportion of illegal merchandise is made possible by the absence of controls. The shorter the processing time per check, the more checks can be carried out logically. Thus, the use of oneclick™ de facto enables more and better security checks to be carried out.”

To provide a stronger argument for Zero Trust Architecture, oneclick™ has created special Cyber Assurance” in partnership with one of the leading German insurance companies Wurttembergische and the leading global insurance underwriter Victor Insurance. The insurance covers cyber incidents for every device equipped with the software (information security breaches), e.g. through hacker attacks, malware, denial of service and even the failure of information and communication technology. The scope of the insurance cover includes, among other things, the costs of IT forensics, interruption of operations, restoration of data and repair or replacement of IT systems. The Cyber Assurance is automatically attached to each oneclick license.

How Bridging the Gap Between Zero Trust and Zero Touch with AI Benefits Your Organization

Zero Trust is…

- An overlapping security approach that continues to evolve as an environment changes with new users, devices, applications, and technologies.
- A combination of processes and technology.
- Not a single product or a one-time checklist.

Fundamental principles:

- Users access data that resides anywhere, from anywhere, in any way
- External and internal threats exist on the network and endpoints at all times
- Every device, user, and network flow must be authenticated and authorized
- Policies must be contextual, dynamic, and data-driven, not static

Foundational Zero Trust elements

People – Zero Trust starts with people and the need to identify them as trusted users or not – and not just upon intermittent login events but on a continuous basis throughout the app usage lifecycle. Because users don't tolerate frequent, active re-authentication, this drives the need for authentication technologies that are both unobtrusive and continuous in their application.

Devices – Continual assessment should include whether the device is in a compromised state, is using older software, and has encryption enabled with sufficiently strong password controls to ensure its integrity. Should span mobile and desktop.

Network – Traditional VPN gateways can make the problem of ubiquitous cloud access and growing Wi-Fi network access worse by bringing traffic from BYO devices that's destined for the cloud inside the enterprise perimeter, exposing internal networks to lateral traversal threats, only to send it back out again. A new generation of secure web gateways become a foundational element of Zero Trust, as they can dynamically adapt not only to the network risk, but also of the people, apps and devices using it.

Apps - securing and properly managing the app layer as well as compute containers and virtual machines is central to Zero Trust adoption. Multi-factor authentication on its own is proving a barrier to productivity – Continuous Authentication is needed.

Security Analytics and AI – while it's true you can't combat a threat you can't see, it's also true that needing to a see a threat many times before you can identify and prevent it necessarily leaves you exposed, and on a continuous basis. That's why a well-designed Zero Trust architecture must leverage advanced, AI-based threat identification and prevention, user and entity behavior analytics (UEBA), and other analytics-based approaches to learn from the past, understand what's happening in real-time and apply preventative measures intelligently. The goal is not just identifying threats and data loss events after the fact, but actively preventing threats and data loss from occurring in the first place.

Automation – it's simply not possible for security analysts to be actively involved in every access decision at the time requests are being made or even a small portion. Cost-effective Zero Trust necessarily makes full use of automation and intelligence-based dynamic policy adaptation and response to deliver the real-time Zero Touch experience that people demand while still enabling Security Operation Center (SOC) oversight and interaction in a much more targeted, high-value, and insight-driven way.

The Zero Trust dilemma…

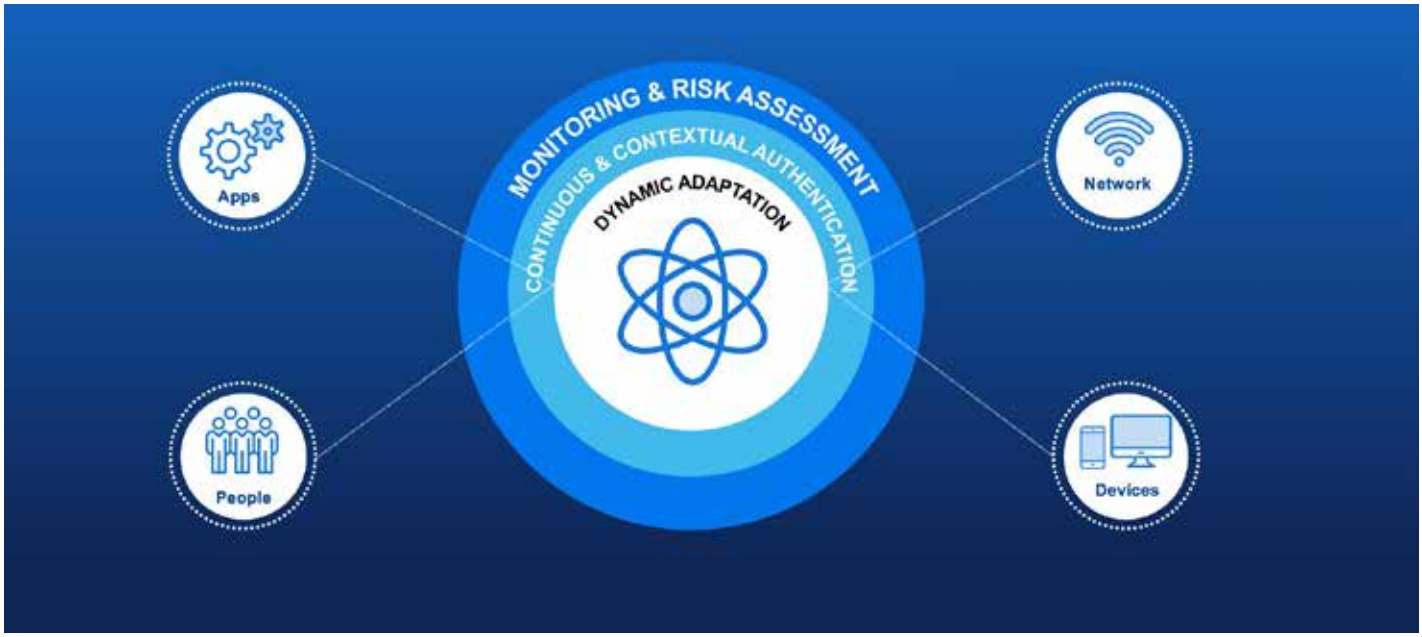
Zero Trust architecture
This is what every security team wants – nobody gets or keeps access to anything until they prove and continue to prove who they are, that access is authorized, and they are not acting maliciously.

Zero Touch experience
This is what users/employees want – immediate gratification with instant access to anything and everything they believe they need without hassles of passwords, timeouts, special permissions, multiple authentications, etc.

Zero Trust Architecture by BlackBerry solves the dilemma

Zero Trust Architecture (ZTA) by BlackBerry incorporates all of the necessary foundational elements and solves the Zero Trust dilemma by applying its strong Security AI and Analytics expertise to deliver the Zero Trust architecture that the security team needs, with the Zero Touch experience that end users crave.

Figure 1: Zero Trust Architecture by BlackBerry



Constant Monitoring and Threat Detection
AI monitors mobile and desktop devices and the apps running on them for any new or known threats and takes appropriate action to remediate such as preventing phishing attacks. BlackBerry's Secure Edge Framework enables MTD to be easily integrated into any app.

Contextual Authentication
AI modeling of user behavior learns whether the user's 'macro' context conforms with trusted behavior and dynamically adjusts the network perimeter to either (i) grant access when behavior is trusted and conformant with policy, (ii) challenge the user when behavior is novel but otherwise conformant with policy, or (iii) block access outright when behavior is either non-conformant with policy or otherwise highly anomalous.

Continuous Authentication
After initial access grant, Continuous Authentication assesses the 'micro' context of a user's ongoing behavior and decides if access should be allowed to continue. Combining biometric, app usage, and process invocation patterns across mobile and desktop, Continuous Authentication assesses 'who you are' based on how you use the device as opposed to the static way of continually asking for passwords which is 'what you know'.

Dynamic Policy Adaptation and Response
Dynamically and intelligently applies the right policy, at the right time to ensure policies are optimized for the user's current context and are neither too strict, nor too lenient. EDR using AI thwarts attacks before they can execute and automates investigation and response with playbook-based workflows.

Real world example

An employee just left their smartphone in a restaurant during lunch hour after using it to check emails and access apps in the cloud and on the corporate intranet.

A typical static mobile policy, e.g. based on a 30-minute timeout, combined with a 'network-only' approach to Zero Trust necessarily leaves data exposed in this case because the legitimate user was already and recently granted access. For the malicious user who now picks up that phone, this means:

- Access from this mobile/Wi-Fi network won't be denied
- Access to apps was just granted, re-authentication won't come into play
- Timeout may eventually come into play, but only after active use stops

The irony of this all-too-common case: it is the legitimate user's beneficial and productive behavior that leads to this exposure. But, to be clear: it's not the user's fault, but rather the fault of the static, context-unaware policy and overly narrow 'network-centric' conception of Zero Trust focused on the initial access grant.

How Zero Trust Architecture by BlackBerry handles this case…

ZTA by BlackBerry continuously monitors all devices and apps and applies strong AI to understand how people use devices, apps, and networks to actively prevent data loss and optimize, not degrade, the legitimate user's experience.

Contextual Authentication
The restaurant is already known to be a low-trust location for this user. Device and/or app timeouts would already have been adjusted to reduce the threat window associated with any 'left-behind' device. In addition, if the user subsequently accesses apps from another device in another location – e.g., upon logging back into their laptop when returning to the office – ZTA by BlackBerry would detect that event and take proactive action to lock the 'left-behind' phone and/or its apps until it's been recovered by the legitimate user.

Dynamic Policy Adaptation: Timeout is dynamically reduced upfront upon the user's initial usage in the restaurant, and then the device and its apps are explicitly locked when the user's return to the office is detected.

Continuous Authentication
Additional layers of AI-based defense based on a combination of passive biometrics and anomalous usage detection ensure that only the legitimate user can enjoy continued access to apps and services.

Dynamic Policy Adaptation: A malicious user is automatically challenged and blocked from accessing apps when they fail passive biometrics checks and/or exhibit anomalous behavior that doesn't fit with legitimate user's learned, trusted behavior. This eliminates any remaining threat should the malicious user gain access before reduced timeout expires.

BlackBerry AI techniques

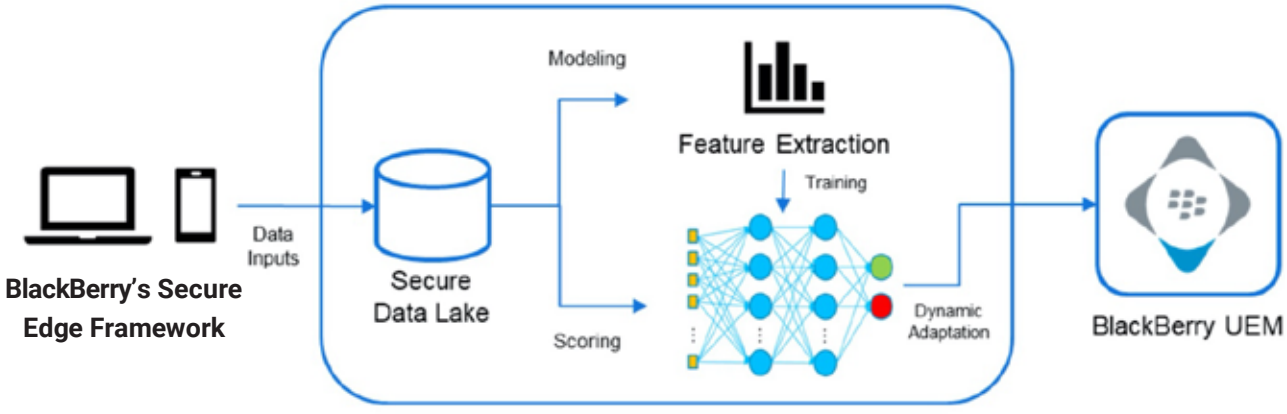
BlackBerry uses a combination of AI techniques that work together as "ensemble" to deliver Continuous Monitoring & Threat Detection, Contextual Authentication, and Continuous Authentication.

Unsupervised Learning
Learns trusted and normal behavior and locations for individuals, groups, and roles, and dynamically applies policy tuned to the user's context and current risk profile.

Deep Learning
Turns passive biometrics and other behavioral and security analytics into continuous, 'n-factor' authentication of the legitimate user.

Anomaly Detection
Applies supervised and unsupervised techniques to app usage and security analytics to distinguish exploit patterns from normal usage, for malicious outsiders and malicious insiders alike.

Figure 2: BlackBerry Intelligent Security AI-based risk modeling & scoring across all endpoints



Modeling inputs

Context

- Location
- Date and time
- App/services used
- Network used

Biometrics

- Motion/touch metrics
- Device orientation angles
- Device tremor
- Mouse movements
- Keystroke speed

App Usage & Security Analytics

- Authentication
- Process Initiation
- Search/Download
- Send/Forward
- Share/Open In
- Copy/Paste
- Screen Capture

Zero Trust Architecture by BlackBerry – total solution, full coverage across all endpoints

While other solutions address parts of the problem, ZTA by BlackBerry provides a total solution for Zero Trust with full coverage across the full spectrum of devices, network, apps and people.

- Provides a path from Zero Trust architecture to Zero Touch experience powered by strong AI
- Works across all endpoint types for complete coverage and better insight into trusted behavior
- Provides continuous monitoring and threat detection to ensure data and AI integrity
- Provides contextual and continuous authentication that spans devices, networks, apps, and people
- Builds on an open platform to enable seamless integration with existing solutions

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.

A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

October 2020

How To Get From Here To Zero Trust

FORRESTER®

Table Of Contents

Project Director:
Lisa Smith,
Principal Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

The global COVID-19 pandemic has exposed gaps in the security infrastructure for enterprises around the world. As countries and companies worked to mitigate the impact to people and business operations, a host of issues has risen to the surface. At the outset of the coronavirus pandemic, business operations needed to transform almost overnight, as a large percentage of workers began working from home. This shift increased a reliance on not only mobile devices, but also on a distributed infrastructure environment. Over time, businesses also increased their adoption of services and applications in the cloud. The speed and complexity of this transformation exposed some organizations to new security risks.

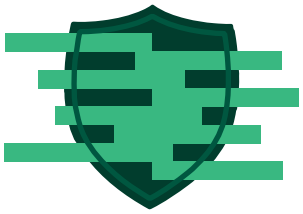
The initial rush towards remote work now shifts to a sustained effort as we enter the later stages of the pandemic, and organizations are focusing on going back and securing their distributed employees, devices, enterprise applications, and cloud environments using a combination of security and IT management. Security leadership wants to find ways to reduce environmental complexity and increase their team's efficiency and precision.

VMware commissioned Forrester Consulting to consider how organizations are securing distributed environments with intrinsic security capabilities, and Zero Trust strategies. Identifying key technological and policy milestones associated with the most successful implementations will help others move forward on their journey toward Zero Trust.

KEY FINDINGS

- **The explosion of data, applications, remote users, mobile devices, and bring-your-own-device (BYOD) capabilities has increased security risks.** This explosion has increased the potential blind spots for security teams trying to identify and control enterprise risks.
- **Enterprises are vulnerable, as distributed environments can shade visibility and increase attack area.** More than 75% of respondents report an increased level of vulnerability in their organizations due to an increased attack surface. Additionally, too many disparate security solution and integration challenges leave gaps in security protection.
- **Technology solutions can make or break your security strategy.** Our research found that 70% of enterprises lack a cohesive security strategy. And while IT leaders are facing more pressure from the board, they are also grappling with cultural issues between IT and security teams.
- **Zero Trust is the relief to these challenges.** Forrester's Zero Trust strategies can provide a roadmap for enterprises to follow in order to overcome these challenges and mitigate security risk.
- **Intrinsic security reduces complexity and costs.** Intrinsic security solutions are built-in versus being bolted-on, and they have the opportunity to increase collaboration with IT, operations, and security teams. This allows faster investigation and remediation and reduced complexity, which ultimately leads to reduced capex and opex.

The Varying Security Dynamic Increases Risks



Prior to the pandemic, business models required enterprises to actively transform how they utilize business technology to win customers and enable their workforce. In the current environment, adopting Zero Trust security strategies are more important than ever. And to successfully secure distributed environments, companies must take a data centric approach to security because:

- **The growth in remote users, BYOD, and device platforms further expands an enterprise's attack surface.** Employees are now working outside of the bounds of the office's security infrastructure, i.e., more users are using more devices, which are connecting to a greater number of unknown and personal networking infrastructures, than ever before. Increases in remote work have put consumer internet-of-things (IoT) and mobile devices into contact with sensitive enterprise resources. And unfortunately, the end result no longer provides security teams with the same visibility and control over the devices that employees use to get work done. Decreasing efficacy of network-based security controls such as VPNs and firewalls, along with poor segmentation between sensitive devices, apps, and data, further adds to the challenges in trying to protect the expanding attack surface created by employee devices.
- **The shift to highly distributed environments opens companies up to a larger range of security risks.** Data sits at the center of any business, and the applications that access and move workloads create more access points. In addition, the increasing use of software as a service (SaaS) and cloud impacts securing applications and data.
- **Applications have reshaped data center complexity.** Most enterprises are plagued by infrastructure complexity that is driven by disparate platforms and configurations, which have accumulated over the years. As organizations trade out monolithic app architectures in favor of highly distributed microservices across multicloud environments — leveraging app containers and serverless functions — environmental complexity increases the potential blind spots for security teams trying to identify and control enterprise risks.

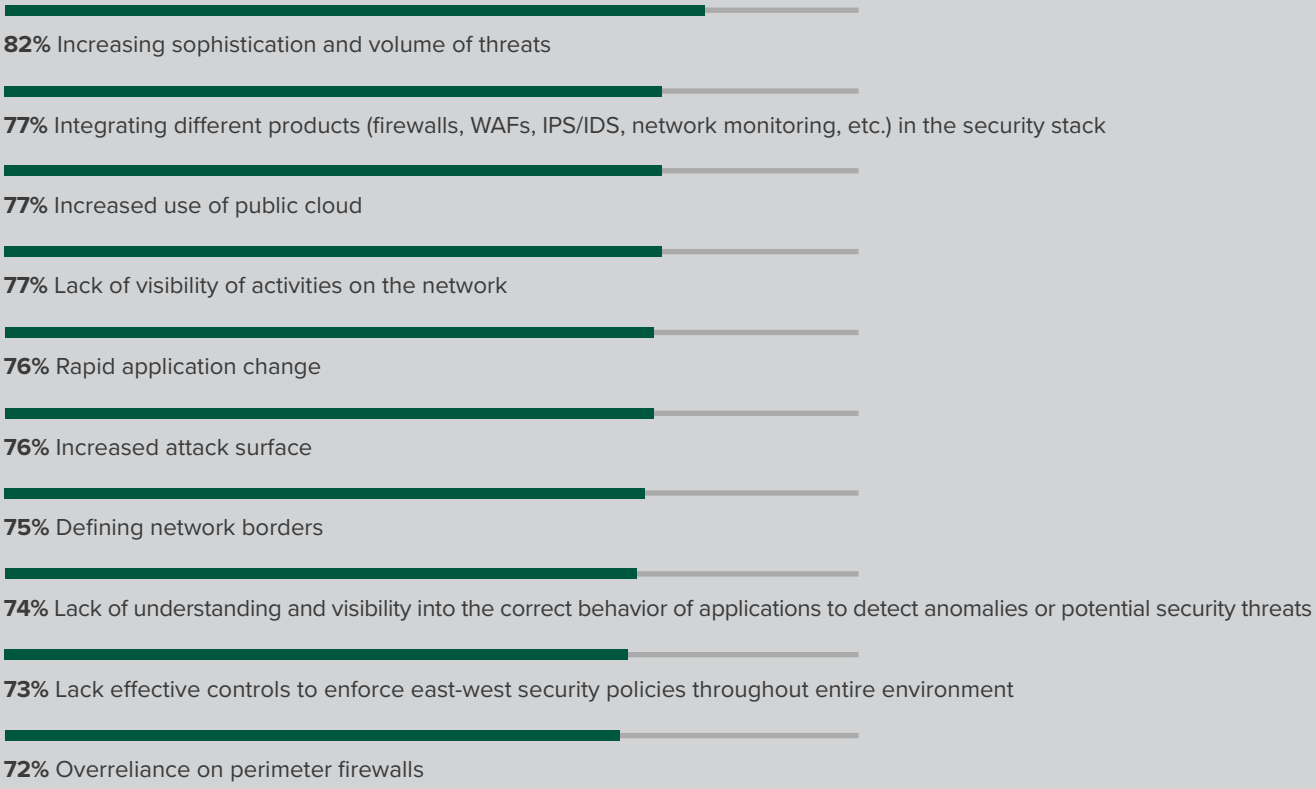
THIS SECURITY TRANSFORMATION PRESENTS BOTH TECHNICAL AND ORGANIZATIONAL/CULTURAL CHALLENGES

The transformation to a more distributed environment is challenging many enterprises as they work to secure their data, applications, and workloads. And the impact of the pandemic is only exacerbating these challenges. Recent research conducted by Forrester Consulting in partnership with VMware found these technical challenges:

› **A distributed environment clouds visibility and increases a network's attack surface.** Nearly three-quarters of IT security professionals say there's a lack of understanding and visibility into the correct behavior of applications, making it challenging to detect anomalies or potential security threats (see Figure 1).[1] In addition, more than three-quarters of enterprises report their organization is more vulnerable due to an increased attack surface.

Figure 1: Companies Face A Multitude Of Technical Challenges

"Thinking about your organization's security vulnerabilities, how challenging are each of the following technical factors?"
(Percentages represent top "moderately/very challenging")



Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

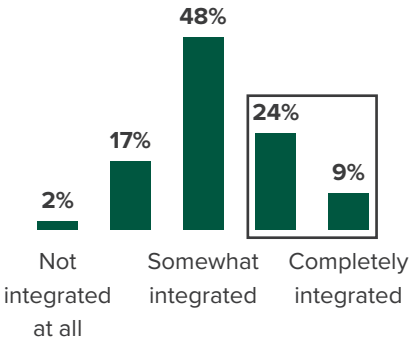
- **Too many point solutions and an overreliance on perimeter firewalls adds complexity and leaves gaps.** Seven out of 10 enterprises report an overreliance on perimeter firewalls when securing the internal network.[2] And the sheer number of security products adds complexity as more than three-quarters of companies manage 10 or more security products, while nearly 20% of companies manage 50 or more security products.[3] The multitude of these projects have either been added or bolted on over time, and they've subsequently created a patchwork that may not completely secure enterprise data and applications.
- **Disparate security solutions are creating integration challenges.** The sprawl of devices and the proliferation of different control requirements and tools compromise enterprises' security postures. It's not surprising that a majority of IT security professionals have significant integration challenges. This lack of integration hinders adaptability, creates security gaps due to misaligned controls, and makes management difficult. On average, companies have 27.4 security products. However, only one-third of respondents said their solutions are mostly or completely integrated (see Figure 2).[4]

While technical challenges are often the first identified, challenges stemming from organization and culture dynamic between senior corporate management, IT, and the security teams can have a significant impact on security enterprise data and applications. Recent research conducted by Forrester Consulting in partnership with VMware found these organizational and cultural challenges:

- **Seventy percent of enterprises lack a cohesive security strategy.** In addition, 69% report there's a lack of clear ownership over the security strategy, and 68% feel there's a lack of executive support (see Figure 3).[5]

Figure 2: Integration Of Security Solutions

"How well integrated are the security solutions in your organization?"



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision-making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Figure 3: Nearly Three-Quarters Of Companies Are Unaware Of The Risks Posed By Security Vulnerabilities

ORGANIZATIONAL CHALLENGES

Base: 224 IT security and infrastructure decision makers and practitioners at global enterprises
Note: Selected variables shown.
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, July 2019

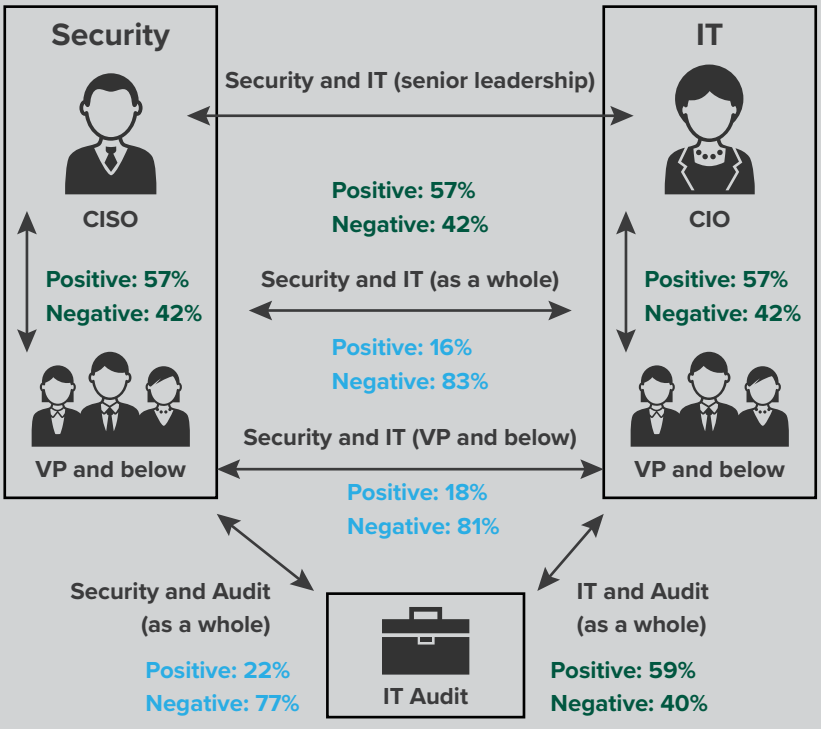
› **IT leaders face pressure from the board.**[6] Our research showed that senior leadership and boards have a greater focus on security (89%) and IT (73%) than they did two years ago. CIOs and CISOs also said that the top concerns of the board include:

- Brand protection (81%).
- Security threats and risks to the business (78%).
- Reducing risk and exposure (77%).

› **IT and security teams often work in silos.** These board priorities mean that CIOs and CISOs in IT and security must collaborate, despite having conflicting objectives. The push for collaboration across teams is a focus from the top down, in addition to reducing risk and protecting the company's brand, but there is clearly a cultural difference between these teams.

› **Friction between IT and security teams hinders collaboration.** In assessing these relationships, the senior-most team members had the most positive relationships, followed closely by the relationships between the two teams. The personnel of the teams were most likely to have a negative relationship with the other team (see Figure 4).[7]

Figure 4: Nature Of IT And Security Relationships



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Friction between security and IT teams hamper collaboration.

FORRESTER®

Build Your Zero Trust Strategies To Overcome Challenges

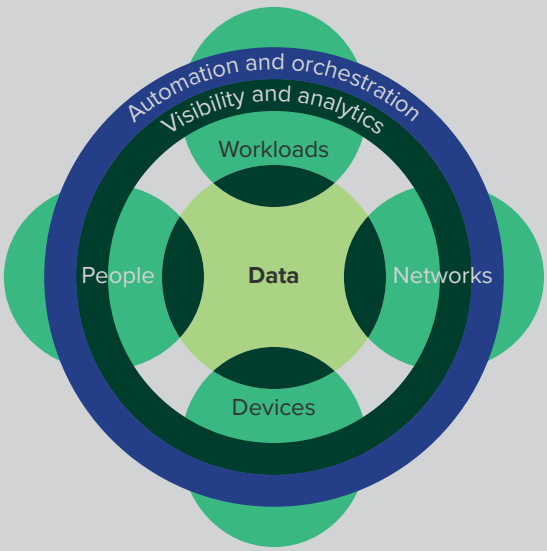
When not following Zero Trust strategies, enterprises face a wide array of challenges associated with securing their distributed environments. Forrester's Zero Trust model of information security is a conceptual and architectural model for how security teams should: 1) redesign networks into secure microperimeters; 2) use obfuscation to strengthen data security; 3) limit the risks associated with excessive user privileges; and 4) use analytics and automation to dramatically improve security detection and response.

There are seven pillars of Forrester's Zero Trust model (see Figure 5):[8]

- **Zero Trust data.** Securing and managing the data, categorizing and developing data classification schemas, and encrypting data both at rest and in transit are key to any Zero Trust approach.
- **Zero Trust users.** Limiting and enforcing user access and securing users as they interact with the internet, by continuously monitoring and governing access and privileges, is a critical component of Zero Trust.
- **Zero Trust workloads.** The workloads are front- and back-end systems that run the business and help it to win, serve, and retain customers. Just as with any other area of Zero Trust, these connections, apps, and components must be treated as a threat vector and have Zero Trust controls such as policy-based API inspection and control, container file and active memory protection, and guest host firewall. Of particular concern are workloads running in public clouds.
- **Zero Trust networks.** The ability to segment, isolate, and control the network is an important point of control for Zero Trust. Segmentation and isolation help to better secure networks.

Achieving Zero Trust is not easy, but you need to start somewhere.

Figure 5



Source: Forrester Research, Inc.

- **Zero Trust devices.** Device discovery, isolation, and management are key to controlling the risks associated with the device hardware, user behavior, apps, and data accessed from the device.
- **Visibility and analytics.** The security analyst needs to have the ability to accurately observe threats that are present and orient defenses more intelligently.
- **Automation and orchestration.** Organizations and security leadership need to use tools and technologies that enable security automation and orchestration (SAO) across the enterprise, to shorten incident response times and integrate disparate security solutions. Orchestration extends security policies to cloud environments.

HOW TO ACHIEVE ZERO TRUST SUCCESS

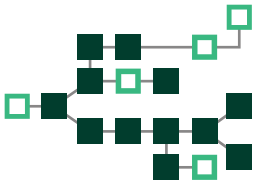
To improve effectiveness of your Zero Trust efforts, there are two things to do: 1) implement solutions with intrinsic security and 2) alleviate organizational and cultural issues hampering collaboration between the IT and security teams.

Recent research conducted by Forrester Consulting in partnership with VMware found the following:

- **Intrinsic security minimizes the remaining risk of technical failure.** Intrinsic security solutions are built-in, software solutions that help companies reduce their threat vectors by being built-in versus bolted on, by unifying tools and teams to improve visibility, and by using real-time context to better detect and respond to threats.
- **Intrinsic security reduces complexity and costs.** Faster investigation and remediation and reduced complexity driven by intrinsic security ultimately lead to reduced capital and operational expenditures.
- **Increase your chances for success by making Zero Trust a collaborative activity.** Zero Trust success hinges on the entire organization focused on the same objective, with IT and Security professionals working in partnership. Break down the IT and Security siloes by bringing the teams together to set agreed upon goals, objectives and measures of success.

Steps To Take On Your Zero Trust Journey

Creating a detailed roadmap that outlines the main workstreams and projects necessary to implement your Zero Trust strategy is critical for success. A good Zero Trust roadmap shows exactly what you plan to deliver, how much your executives will need to invest, and what specific business and security outcomes will be achieved.

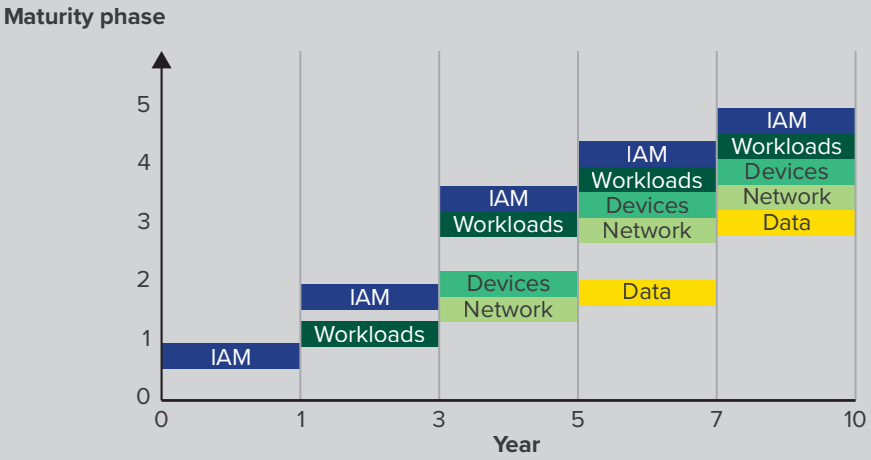


- **Security and IT must work with the business together.** Identify key players that are critical to the Zero Trust strategy; include a board member if you can, IT executives (where budget will come from), and enterprise architects and application owners, who will ensure Zero Trust supports the broader IT strategy, which in turn will support the broader business strategy.
- **Identify interdependencies.** A Zero Trust effort needs to include existing security, IT, and business projects in order to succeed. Cloud migration, network modernization, and partner onboarding can be catalysts for a Zero Trust transformation. Ensure that you are properly mapping and clearly communicating project dependencies.
- **Assess and goal Zero Trust maturity.** Conduct a Zero Trust security assessment of your current capabilities and then set a desired future state maturity (see Figure 6). From there, you can build a roadmap of technological and process progression around the seven pillars of the Zero Trust extended ecosystem: data, people, devices, networks, workloads, visibility and automation. Forrester recommends at least a two- or three-year horizon overall (see Figure 7).

As remote work moves into being a prolonged effort, companies are going back and securing their distributed employees, devices, and enterprise applications using a combination of security and IT management. Both IT and security leadership want to find ways to reduce environmental complexity and increase teams' efficiency and precision.

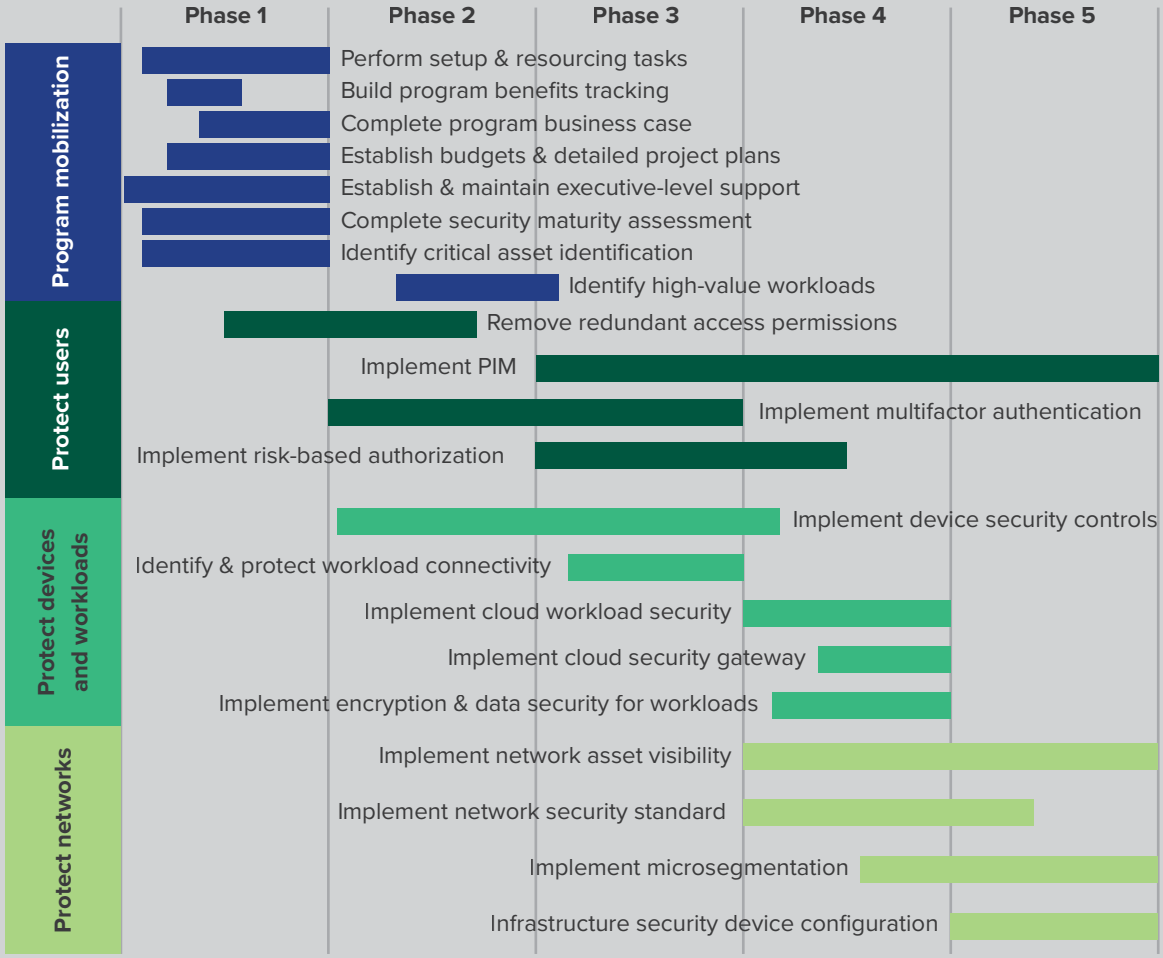
While technology solutions are partly the answer, many companies are facing both pressure from the board and collaboration challenges between IT and security teams. Forrester's Zero Trust strategies can provide a roadmap to overcome these challenges. And in combination with intrinsic security solutions, companies can quickly find and remediate security vulnerabilities.

Figure 6: Sample Desired Future State Maturity



Source: Forrester Research, Inc.

Figure 7: Sample Zero Trust Roadmap



Source: Forrester Research, Inc.

Workloads

For workloads, VMware provides visibility and analysis of configuration, state, and vulnerabilities for hardening; prevention mechanisms against malware, ransomware, and non-malware/file-less attacks; and detection and response mechanisms for attacks that circumvent both of those processes and controls. It covers workloads in private and public clouds, for both traditional virtual machines and Kubernetes containers. Their approach can also leverage some unique integrations with the virtual fabric that enable it to be agentless on vSphere (and a single lightweight sensor in other environments), and integrated with vCenter — providing a single source of truth to both security and infrastructure teams. That enables better collaboration between security and IT, and more effective operationalization of workload security through the infrastructure team. Combined with the NSX microsegmentation technology, it can set up a Zero Trust posture from both the workload and network standpoint — both aligned to the applications they serve.

Networks

VMware's distributed approach to firewalling goes from macro to microsegmentation offering stateful L7 controls and advanced threat prevention. Its unique distributed architecture requires no network changes. Built into the hypervisor, the distributed firewall platform has complete visibility into application topology and automatically formulates microsegmentation policies. A single solution provides consistent policy across virtualized, containerized, and bare metal workloads spanning private and public cloud environments.

With network security and access controls built into the SD-WAN architecture with global POP locations, VMware enables Zero Trust network access for users from anywhere to applications in multicloud locations.

Analytics

VMware solutions include built-in analytics to provide complete visibility and alerting to security operators. In additional to the built-in analytics, VMware Threat Analysis Unit (TAU), a central team of threat researchers and data scientists, leverages product telemetry, partner feeds, and AI techniques to ensure the platforms are powered with best threat intelligence and up-to-date algorithms.

Orchestration And Automation

VMware solutions feature orchestration options across workload, device, and networking. Detailed visual workflows can be constructed to automate tasks including workload deployment, network segmentation, device provisioning, and threat isolation.

Forrester Total Economic Impact Studies Commissioned By VMware

Total Economic Impact (TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The objective of the TEI framework is to identify the cost, benefit, flexibility, and risk factors that affect investment decisions.

VMware commissioned Forrester Consulting to conduct the following recent TEI studies:

The Total Economic Impact™ Of VMware NSX[9]	**ROI: 95%**	**Payback: <12 months**
The Total Economic Impact™ Of VMware Carbon Black Cloud[10]	**ROI: 379%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware vRealize Network Insight[11]	**ROI: 477%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware End User Computing[12]	**ROI: 152%**	**Payback: <3 months**
The Total Economic Impact™ Of VMware Workspace ONE[13]	**ROI: 206%**	**Payback: <6 months**
The Total Economic Impact™ Of VMware Workspace ONE For Windows 10[14]	**ROI: 139%**	**Payback: 7 months**

Appendix A: Supplemental Material

RELATED FORRESTER RESEARCH

"Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model," Forrester Research, Inc., July 2, 2020.

"The Zero Trust eXtended (ZTX) Ecosystem," Forrester Research, Inc., July 11, 2019.

Appendix B: Endnotes

[1] Source: "To Enable Zero Trust, Rethink Your Firewall Strategy," a commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020.

[2] Source: Ibid.

[3] Source: Ibid.

[4] Source: Tension Between IT And Security Professionals Reinforcing Silos And Security Strain, May 2020

[5] Source: "To Enable Zero Trust, Rethink Your Firewall Strategy," a commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020.

[6] Source: Tension Between IT And Security Professionals Reinforcing Silos And Security Strain, May 2020.

[7] Source: Ibid.

[8] Source: "A Practical Guide To A Zero Trust Implementation," Forrester Research, Inc., January 15, 2020.

[9] Source: "The Total Economic Impact™ Of VMware NSX," Forrester Consulting report prepared for VMware, May 2020.

[10] Source: "The Total Economic Impact™ Of VMware Carbon Black Cloud," Forrester Consulting report prepared for VMware, May 2020.

[11] Source: "The Total Economic Impact™ Of VMware vRealize Network Insight," Forrester Consulting report prepared for VMware, July 2019.

[12] Source: "The Total Economic Impact™ Of VMware End User Computing," Forrester Consulting report prepared for VMware, April 2019.

[13] Source: "The Total Economic Impact™ Of VMware Workspace ONE," Forrester Consulting report prepared for VMware, October 2018.

[14] Source: "The Total Economic Impact™ Of VMware Workspace ONE For Windows 10, Forrester consulting report prepared for VMware, October 2018.

THE DIGITAL WORKSPACE JOURNEY MODEL PATH TO ZERO TRUST

AT A GLANCE

Using the Digital Workspace Journey Model to implement a Zero Trust security model, VMware Professional Services can help you develop the required capabilities that support a Zero Trust philosophy.

KEY BENEFITS

- Replace legacy "Castle and Moat" security model
- Regularly verify the security posture of devices and users
- Leverage rich context to make dynamic app access decisions
- Mitigate risk of data breaches originating within the network perimeter

SAMPLE PROBLEMS ADDRESSED

- Unable to provide secure access to corporate apps and data on BYO devices
- Unable to verify security posture for users and devices on the corporate network
- Enable secure access to applications even when devices are off the corporate network

Empower the Digital Workspace

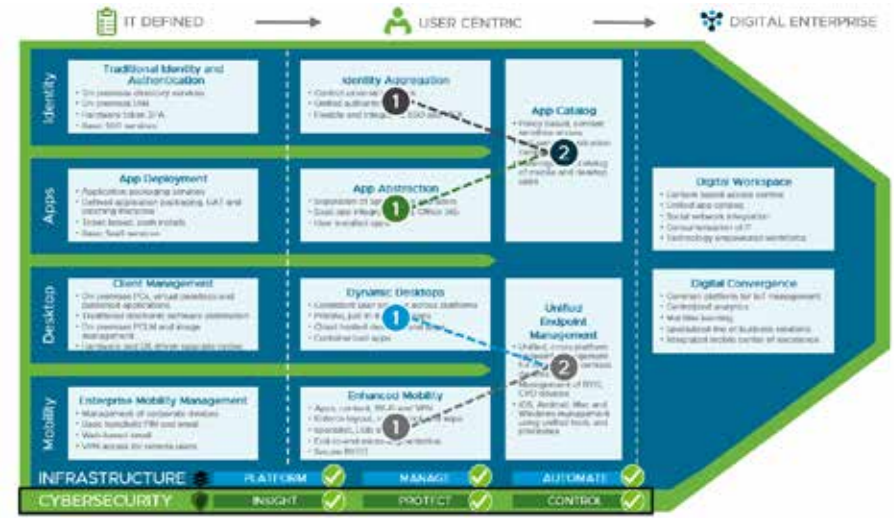
Implement a Zero Trust security philosophy

Zero Trust is not a specific technology or product, but a security philosophy that combines device and user trust with a rich conditional access model that requires verification of trust prior to allowing application access. In an ideal state, the verification happens almost continuously and is supported by a degree of analytics providing insight, orchestration and automation.

Most organizations will embark on a Zero Trust journey and will take a step-by-step approach that is part of a larger security transformation initiative. Workspace ONE is uniquely positioned to provide the technical framework to achieve various milestones on the journey.

VMware Professional Services can help your organization address the following on your journey to a Zero Trust security model:

- Device Management & Compliance
- Conditional Access
- App Tunnel and Proxy
- Risk Analytics
- Automated Remediation and Orchestration



The Digital Workspace Journey to Zero Trust

Industry Example: Finance

The financial services industry has lately encountered multiple security breaches, many of which originated from within the physical and logical network, yet they are trying to modernize by enabling workers with more mobility and a better customer experience. Traditionally, once a device is within the physical network it has access to resources on the network as it is considered "trusted."

A Zero Trust security model can greatly mitigate the risks of a breach by assuming all devices are hostile, even when connected to the internal network or physically located within the corporate building. With a Zero Trust model, the device is constantly verified against policies, and if conditions change, conditional access can present the user with additional layers of authentication. For finance workers that are constantly mobile, a Zero Trust solution can establish a per-app-VPN so that their devices never have access to the entire corporate network, while providing mobile workers with a greater choice in the devices they use

Capabilities supported

- Manage corporate mobile devices
- Manage specialized devices
- Provide a customized mobile device management configuration
- Provide a self-service application catalog
- Provide secure access to enterprise systems
- Push configurations of corporate applications
- Track and report on the status of the device fleet

Strengthening Security with Zero Trust

e

Drivers

Governments around the world are managing data more broadly and rapidly than ever, enabling critical missions that underpin our national security, economic stability, and public safety. Partnerships with the private sector to safeguard these valuable systems and data are critical to executing these missions. Whether data is stored, in-transit, or shared, all systems that handle data—wherever they are—must be able to ensure its confidentiality, integrity, and availability.

Government departments and agencies simply cannot afford to have cybersecurity incidents disrupt their normal operations, and "trust" has proven to be an exploitable vulnerability. One effective strategy for ensuring cybersecurity resilience is to pursue a Zero Trust architecture.

Challenge

Today's cyberthreat landscape is complex, and digital transformation is moving quickly. Competing priorities and initiatives can often distract departments and agencies from their primary mission: ensuring the continuation of government Mission Essential Functions (MEF) enabled by a secure digital operating environment.

As agencies transition to Zero Trust, the top concerns include:

- Preventing unauthorised lateral movement
- Preventing unverified network activity
- Ensuring only legitimate users have access to authorised network resources

Traditional Approach

In a traditional model, agencies rarely spend time understanding what they are trying to protect. Most efforts centre around system functionality, while security has traditionally been implemented from the network perimeter, in the network's endpoints, and overlaid on top. As new threats emerged, discrete point products were added to this model to address them. For example, security vendors countered application-level attacks with intrusion prevention systems (IPS). As computer viruses became more prevalent, governments added antivirus to endpoints. When phishing email attacks increased, so did the deployment of content filtering to counter that threat.

This approach, known to many as "defence in depth," has resulted in a string of disjointed products that do not holistically interoperate to address the scope and breadth of all potential threats. The principle drawbacks of this security model are:

- **Reduced situational awareness**: With multiple non-integrated security products, it's difficult to get a comprehensive view of network traffic and threats.
- **Lack of access management**: Minimising the risks of unauthorised access is a fundamental security principle. This is best achieved by implementing integrated security from the inside out—the opposite of the defence-in-depth approach.
- **Diminished security with complex management**: When each point product is separately managed and not integrated, agencies get less effective security and greater overhead.

Palo Alto Networks Zero Trust Approach

Zero Trust is a cybersecurity strategy designed around the concept that users, applications, and data should never be inherently trusted—their actions should always be verified, in every environment. The strategy involves limiting the scope of an attack and blocking lateral movement by leveraging micro segmentation based on users, data, and location. We present the concept of a Zero Trust architecture to help form a security strategy that supports continuity of government operations by only allowing communications that are essential, validated, and approved. Palo Alto Networks secures governments globally by helping them adopt three cybersecurity principles that increase the efficacy of protection and reduce the workloads on network and security teams:

- Implement a Zero Trust approach
- Apply consistent security regardless of location
- Adopt security automation

We have helped government agencies establish effective Zero Trust outcomes in a wide range of urgent situations and attack-related emergencies. To execute on Zero Trust, we use the five-step methodology depicted in figure 1. This method helps senior agency officials, mission owners, and engineers implement a robust security framework based on prioritising the protection of MEFs.

Zero Trust Adoption Methodology

Whether you are implementing a Zero Trust strategy on a private network or in the cloud, and regardless of infrastructure, the five-step methodology takes you through:

Figure 1: Five-step methodology

- **Step 1**: Define your protect surface
- **Step 2**: Map the protect surface transaction flows
- **Step 3**: Architect a Zero Trust network

- **Step 4**: Create the Zero Trust policy
  Step 5: Monitor and maintain the network

Palo Alto Networks Next-Generation Firewalls are designed to deny all and permit by exception. Combining this with the five-step methodology, a system inherently includes Zero Trust by design, resulting in:

- Closed-loop process for establishing least-privileged network access policies for any use case.
- Enhanced command and control (C2) over MEFs and network connectivity.
- Process integration between network and security operations.
- Positive control over a range of threats (e.g., passive, active, insider, integrator).
- Complete understanding of expected communications and easy spotting of unusual patterns.

During the briefing, the stakeholders quickly realised several benefits of our Zero Trust approach with regards to gaps they had previously identified in their network: gaining more visibility into internal network activity and recognising abuse of privilege instances. Recognising that our technology would bridge these gaps and help the agency achieve its desired outcomes, the stakeholders asked our team to help them execute.

As a part of our Transformation Services package, we helped the agency develop and deliver a Zero Trust architecture with micro segmentation that included advanced threat prevention. In consultation with the key stakeholders, we defined and inserted strict network security policies to permit by exception, and approved network traffic using the Kipling Method. Figure 2 shows the agency's MEF and endpoints protected with end-to-end policy enforcement points (PEPs) that are centrally managed and locally enforced Guided by the five-step methodology, the protect surfaces had been defined, and micro segmentation architecture had been

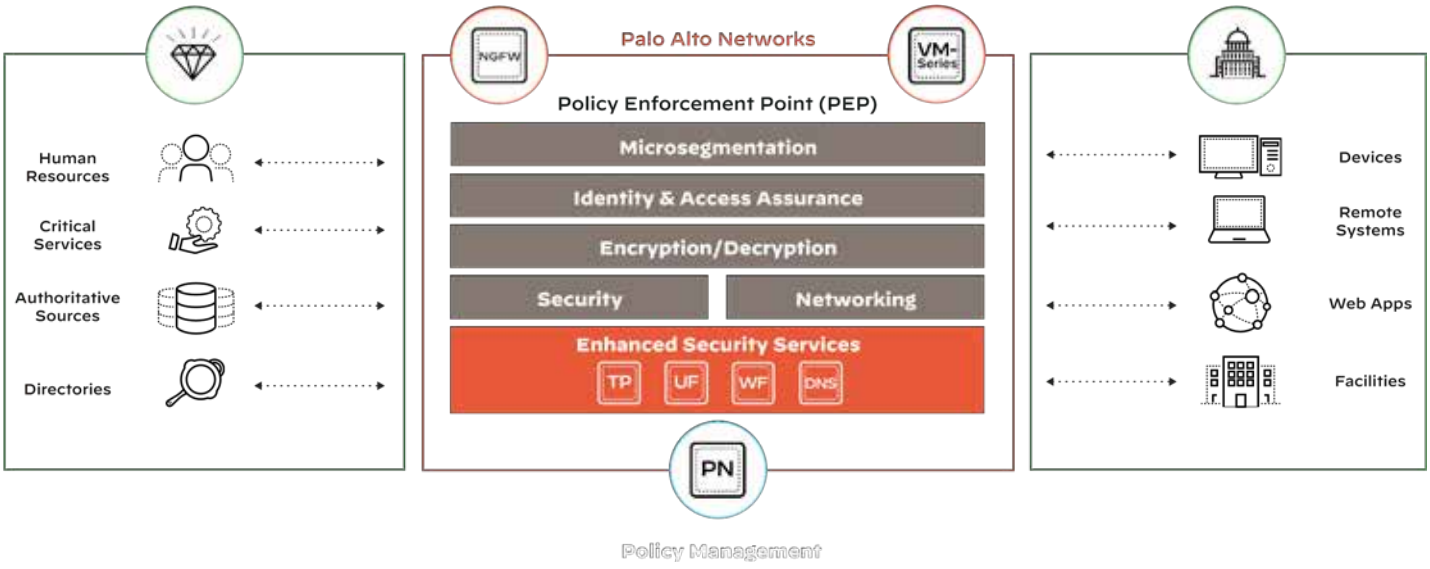


Figure 2: Micro segmentation architecture

Monitoring and maintaining the Zero Trust lifecycle is an integral part of IT Service Management (ITSM). The ITSM process will help administrators answer the questions of "why" and "how" before approving changes that will modify the defined protect surface. For example, making changes to an existing application or introducing a new application will trigger a change management process supported by ITSM. This helps agencies quickly shift their mindset to standardising cyber defence capabilities and automating processes since security is built into the operating framework.

Customer Implementation

Zero Trust was first introduced to one of our government customers as part of a briefing we provided ahead of their network re-accreditation. This agency, a large joint service organisation that serves a strategically important user base, has numerous facilities, and operates on a multimillion-dollar cybersecurity budget. It also manages separate private networks that service several branches of government as well as data centres that connect to a joint information system environment.

selected as the Zero Trust approach for two of the agency's independent private networks. Next, stakeholders specified the Zero Trust policies they wanted to apply to those private networks. Consistent with designing security from the inside out, user access played an essential role in the architecture, supported by our Next-Generation Firewalls User-ID™ technology, which answered the question of who was seeking to access specified data or systems. The ability to identify all users on the network, ensured policy enforcement for authenticated users from an authoritative identity source (in this case, Active Directory®).

To answer "what" and "where," we enabled App-ID™ technology, which can uniquely classify critical services and accurately identify applications before establishing connectivity for privileged users at each endpoint. The agency was able to achieve its gap analysis objectives through closed-loop network security policies. Figure 3 shows where to find answers to help inform the creation of the agency's Zero Trust policies.

Figure 3: Creating a Zero Trust policy

Benefits of a Zero Trust Architecture

By leveraging the Palo Alto Networks platform, any organisation can reap numerous benefits like those presented in this use case.

Mission Benefits

- Greater cyber resilience, contributing to the availability of essential functions that enable the mission.
- Improved network visibility, which helps close the gap between threat detection and decision-making, enhancing situational awareness and increasing confidence to operate safely in cyberspace.
- Insider threat deterrence by recognising and limiting opportunities to exploit trust.

Operational Benefits

- Increased command and control over enterprise computing activities.
- Simplified compliance with applicable standards and regulations, using zone boundaries to segment sensitive resources.
- Simplified management operations through automation and standardised rule sets.
- Immediate flagging of unexpected or anomalous traffic by Zero Trust segmentation gateways.

Security Benefits

- Limited potential for data exposure through a reduction in the attack surface.
- Strict enforcement of a least-privileged network access policy.
- Enhancement of the organisation's ability to prevent exfiltration of sensitive data.
- Visibility into and control over applications and services throughout the environment.

Conclusion

With more data in more places, a government wide Zero Trust strategy is critical to modern environments. With the help of automation and consistent security across defined networks, a Zero Trust architecture is possible. As your agency extends its mission to the cloud, our security-as-a-service capabilities— including our Prisma™ and Cortex™ product suites—will help expand your Zero Trust environment. For instance, Prisma Access is a comprehensive secure access service edge (SASE) solution that delivers networking and security, ideal for agency branch offices and remote users (two TIC 3.0 use cases).

Palo Alto Networks is a trusted partner of hundreds of national and federal departments, bureaus, and offices. Our enterprise and cloud offerings protect the mission for civilian and defence agencies in critical operating environments globally.

Additional Resources

To learn more about how Palo Alto Networks can help organisations improve cyber risk management, visit our website. Visit our Federal Government webpage to learn how to modernise your agency operations. We can also help you understand more about Zero Trust.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Cyber Health in the Supply Chain
A Zero Trust Use Case

If you need to allow third parties access to IT services, you probably face a multitude of options to confidently control the identity of service users. However, it is unlikely that you will have equal confidence in the health of their networks and devices.

Knowing the identity of a user, and even the identity of their machine, may do little to mitigate cyber risks if endpoints or networks are themselves compromised. Addressing such risks is ideal territory for the Zero Trust Networking model that extends access control beyond user and device identity management to incorporating rigorous system health measurements as part of fine-grained access control to protected services.

The increasing examples of regulatory requirements and guidelines specifically referencing supply chain risk reflect the frequency with which such attacks occur. Many suppliers are easier prey than the larger organisations they serve, and many represent a significant aggregation of risk across sectors such as Telecoms or Defence.

Using a Defence Supply Chain use case, this paper discusses the role of health measurements within the Zero trust model.

The Zero Trust concept in brief

A high-level and vendor-neutral overview of Zero Trust principles is provided by the National Cyber Security Centre (NCSC), as follows:

- Provide a single strong source of user identity
- Implement strong user authentication
- Implement machine authentication
- Include additional context, such as policy compliance and device health
- Set authorization policies to access applications
- Set access control policies within an application

Without repeating guidance here, in essence the Zero-Trust Networking approach advocates checking the identity and integrity of devices irrespective of location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication.

Identity management: necessary but not sufficient

User identity and authentication platforms have matured with extensive support for multi-factor and certificate-based authentication. Integration across federated systems with standards such as OAUTH or SAML can help to maintain a single source of user identity. Device identity management has also matured, with certificate-based identities tied to hardware-based roots of trust (e.g. IEEE 802.1AR). These excellent building blocks will suffice on their own for many use cases, but where the full benefits of Zero Trust are sought, equal consideration should be given to device health.

Common approaches to device health measurement lack the rigour of the cryptographically-based protocols used for user or device *identity* Management. Software agents will typically do a 'best efforts' check of platform configuration. However, if an attacker compromises an endpoint and gains sufficient privileges, the software agent responsible can be undermined.

"Existing approaches to device health measurement lack the rigour of the cryptographically-based protocols …..

While such agents have value in many environments, organisations that face elevated threats, or have significant liabilities accruing within their supply chains, will be better served by a device health measurement protocol that can validate the integrity of *all* executing firmware and software on the endpoint, with a cryptographic protocol tied to a hardware root of trust. The strength of such an approach is then based on the properties of cryptography, as with other protocols, providing confidence in the detection of attempted compromise that cannot be achieved by simple software agent inspection.

Towards Device Health Measurement

Modern general-purpose operating systems often include a level of system health measurement. *Secure Boot*, and *Trusted Boot* technologies can protect firmware, boot and system files. But such mechanisms do not extend to much of the vulnerable software that executes, including third-party drivers and applications, leaving the endpoint reliant on weaker forms of defence such as application whitelisting, driver signing (without full PKI), and malware detection software. If an

attacker can compromise an application, the compromised health of the system may go un-detected.

To address these limitations, NCSC initiated a research project, referred to as CloudClient[i] that demonstrated how health measurements could be extended to include *all* firmware and software components. The project's *Measured Execution* architecture cryptographically validates that all software executing on a powered-up device is authorised, and has not been tampered with.

Generating device health measurements that confirm that a device has not been compromised has significant value on its own, drastically simplifying an organisation's endpoint security monitoring challenge. However, within the context of Zero Trust, the health measurements need to feed in to access control policy.

For the CloudClient project, integration with a device identity management server was achieved through the use of a standards-based *Remote Attestation Protocol*[ii].

Health measurements allowed device and software state to be compared with a known-good state allowing subsequent access from the device to protected services.

(Zero) Trusting Your Supply Chain

Managing supply chain IT risk for many organisations has often been a case of influencing supplier processes through on-boarding and audit activities. Reducing the reliance on people and process, and gaining confidence through technical controls in the health of devices used by third-parties to access your IT systems, has clear value from a cyber-risk perspective. But what are the practicalities of using such technologies within the supply chain?

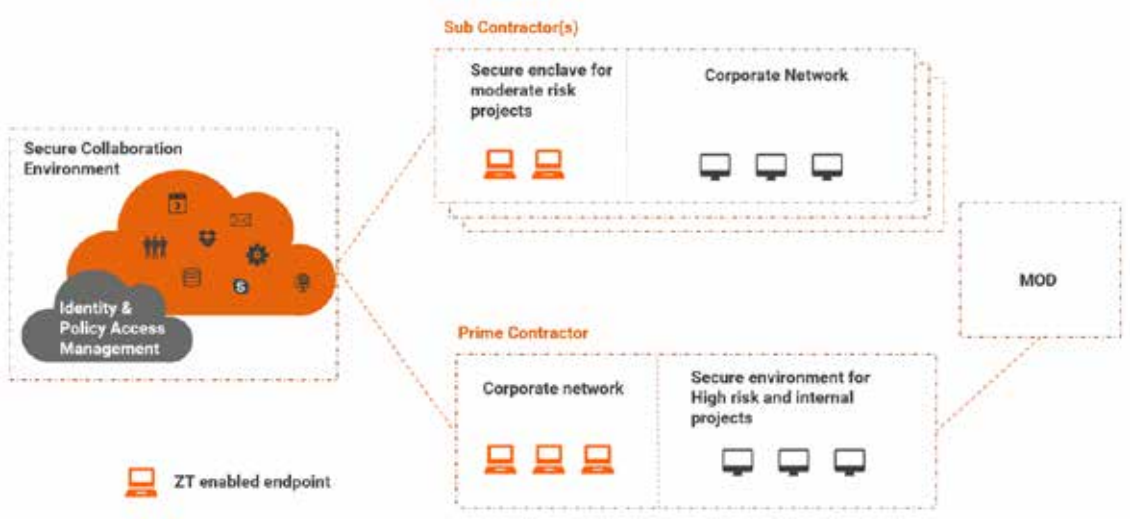
Importantly, the common federated approach of authentication protocols, means that organisations don't need to get involved in directly managing third-party IT to encourage the use of Zero Trust. Additionally, the increasing support of major platforms for Zero Trust principles, provides flexibility of implementation, allowing organisations to adopt the technologies that best fit their budgets or preferences.

Applying ZT Principles to Defence Supplier Collaboration

Through extensive collaboration with industry, the UK Ministry of Defence (MOD) developed and published a set of standards and guidelines (DefStan 05-138) that set out the *Information Assurance* (IA) processes and controls that organisations are expected to adhere to when handling MOD information. The standards seek to ensure that an organisation's risk management processes match corresponding project risks, the levels of which are assessed during the contracting process.

The standards are informative and comprehensive, but organisations with limited IA and risk management experience or resource can perceive the requirements as an unwelcome overhead. From a Lead Integrator or Prime Contractor's perspective, the challenge exists to confirm that their suppliers have met and continue to adhere to the appropriate standards.

One approach being taken within the Defence Sector is the use of secure collaboration platforms designed to host the applications and tools that a project requires. Such platforms can be built for compliance with appropriate standards, allowing its subsequent consumers to inherit the compliant configuration. However, as both the users and devices that connect to the platforms fall within scope of compliance, the use of Zero Trust principles can extend the scope of compliance and trust boundaries to the accessing organisation's environment.



The combination of secure collaboration platforms, with device identity and health measurements through the use of compatible endpoints devices, provides an effective mechanism for organisations to create secure enclaves guaranteed to be compliant with relevant standards.

Summary

The origins and increasing relevance of Zero Trust can be traced to and tracked against the disappearance of well-defined boundaries to corporate networks, as we become increasingly mobile, interconnected and cloud dependent. Supply chain collaboration by definition works across corporate boundaries, requiring the establishment of trust and transparency to support effective risk management. As outlined above, Zero Trust supporting technologies that enable access to protected resources to be based on timely and context-relevant policies, provide the means for organisations to simplify and automate risk management across the supply chain, reducing the dependency on process and blind faith.

About Becrypt

Becrypt is UK supplier of cyber security software and services. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services – from mobile and endpoint to cloud; from funded research, to commercially available products and managed services. Becrypt have worked with UK Government and platform vendors to pioneer and deploy device health identity management products and services.

[i] While references to CloudClient are made with permission, currently NCSC authored content relating to CloudClient is not in the public domain. Principles and objectives relevant to CloudClient are published by NCSC in the context of Zero Trust.

[ii] Remote Attestation implemented as per Trusted Platform Group (https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf)

Privileged Access Workstations

A Zero Trust Use Case

A common factor for many cyber incidents, has been the targeting and compromise of privileged users, such as Systems Administrators, and their devices. Hardly surprising as they represent the keys to the IT kingdom.

Unfortunately, many organisations have struggled or been slow to implement adequate controls to protect privileged administrator tasks. It is not uncommon for devices that are used for administrator access to double-up as corporate devices with email and internet access, exposing administrators and their systems to commodity cyber-attacks.

A common but weak form of defence has often been to deploy a remote desktop infrastructure via a 'Jump Box', to isolate an administrator's device from management systems. As highlighted by the National Cyber Security Centre (NCSC), such 'browse up' architectures remain vulnerable. If an attacker compromises the administrator's device, subsequent remote access sessions are vulnerable, and an attacker may still retain a foothold for lateral movement and later compromise.

The Zero Trust concept, with its emphasis on identity management and device health, may provide the ideal model for organisations seeking to improve privileged access security.

Applying Zero Trust to Privileged Administrator Access

The key themes of NCSC's recently published *advice* on protecting administrative systems may be summarised as: gain trust in your management devices; protect the interfaces to administrative systems using a tiered model where required; appropriately control privileged access to systems, and audit related activities.

The style of NCSC advice is typically outcomes based, focusing on the objectives rather than tightly prescriptive methods, helping to avoid tick box compliancy exercises and encouraging organisations to reflect on the processes and technologies that make most sense for them. One approach to achieving secure system administration objectives, is to view the challenge through a Zero Trust networking lens.

The popularity and relevance of Zero Trust has grown in response to the disappearance of well-defined boundaries to corporate networks, as we become increasingly mobile, interconnected and cloud dependent. The Zero Trust Networking approach advocates checking the identity and integrity of devices irrespective of location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication. NCSC summarise the principles as:

- Provide a single strong source of user identity
- Implement strong user authentication
- Implement machine authentication
- Include additional context, such as policy compliance and device health
- Set authorization policies to access applications
- Set access control policies within an application

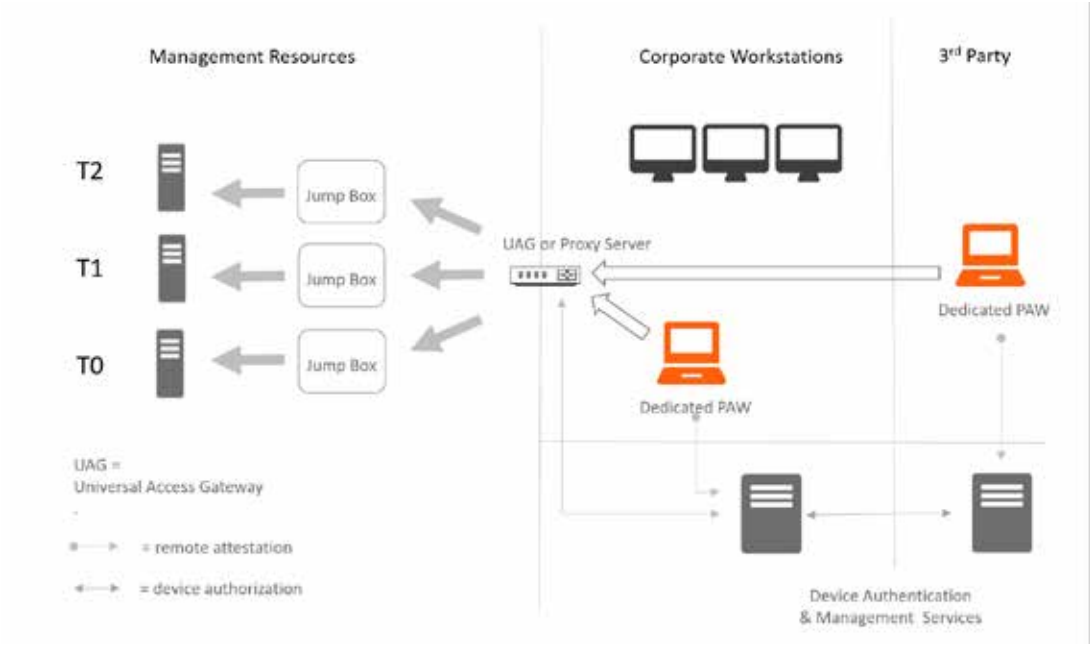
Zero Trust supporting technologies enable access to protected resources to be based on timely and context-relevant policies.

Controlling Privileged Access with ZT

Privileged Access Workstation (PAW) is the term used for a dedicated administrator endpoint. PAWs should ideally be locked-down to a known-good state, and only be used for administrative purposes, with no access to email, internet or other less-trusted resources. Health measurements as advocated within Zero Trust architectures can allow continued assurance that PAWs remain in a known good state, supporting access control polices to combine device and user authentication factors to enable management service access at the appropriate tier.

The diagram below illustrates how a basic proxy server or gateway architecture may be implemented to include device health measurements within policies protecting administrative resources in a tiered model. Where federated identity management is supported, access control may be extended to 3rd party privileged access. Combining device health with device and authentication allows an end-to-end tunnel to be created from a trusted device, by an authorised user, over an un-trusted network to a protected service.

In such a model, how well services are protected, ultimately depends on how well user, and device identity, as well as device health can be validated. While protocols and standards are relatively mature for user identity management, device identity and health measurement has been a different story.

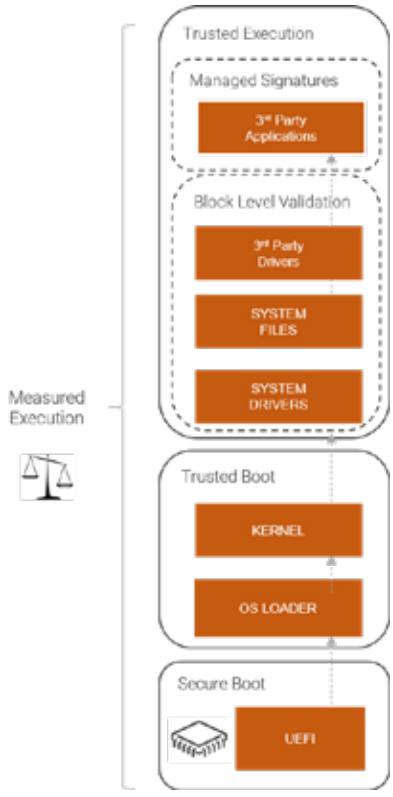


Towards Device Health Measurement

Many existing approaches to device health measurement lack the rigour of the cryptographically-based protocols used for user identity Management. Software agents will typically do a 'best efforts' check of platform configuration. However, if an attacker compromises an endpoint and gains sufficient privileges, the software agent responsible for checking known system characteristics and patch-levels can be undermined.

"Existing approaches to device health measurement lack the rigour of the cryptographically-based protocols …..

While such agents have value in many environments, where organisations face elevated threats, such as to administrative systems, they will be better served by a device health measurement protocol that can validate the integrity of *all* executing firmware and software on the endpoint, with a cryptographic protocol tied to a hardware root of trust. The strength of such an approach is then based on the properties of cryptography, as with other protocols, providing confidence in the detection of attempted compromise that cannot be achieved by simple software agent inspection.



Modern general-purpose operating systems often include a level of system health measurement. *Secure Boot*, and *Trusted Boot* technologies can protect firmware, boot and system files. But such mechanisms do not extend to much of the vulnerable software that executes, including third-party drivers and applications, leaving the endpoint reliant on weaker forms of defence such as application whitelisting, driver signing (without real PKI), and malware detection software. If an attacker can compromise an application, the compromised health of the system may go un-detected.

To address these limitations, NCSC initiated a research project, referred to as CloudClient[i] that demonstrated how health measurements could be extended to include *all* firmware and software components. The project's *Measured Execution* architecture cryptographically validates that all software executing on a powered-up device is authorised, and has not been tampered with. Software resulting from the CloudClient project is deployed across sensitive UK Government systems today, where there is a need to have high confidence of device health, in the face of constant elevated threat.

Trust but Verify

Generating device health measurements that confirm that a device has not been compromised has significant value on its own, drastically simplifying an organisation's endpoint security monitoring challenge. However, within the context of Zero Trust, the health measurements need to feed in to access control policy.

For the CloudClient project, integration with a device identity management server was achieved through the use of a standards-based *Remote Attestation Protocol*[ii].

Health measurements allowed device and software state to be compared with a known-good state allowing subsequent access from the device to protected services.

Summary

Security controls for access to administrative and privileged systems should match the elevated threat that many such systems face. While standard user authentication, and agent-based endpoint security may be sufficient protection for many users within an organisation, such mechanisms fail to deter sustained and targeted attacks that higher value targets attract. The Privileged Access Workstation model, providing isolation with robust identity and health measurements as components of access control policy, allows organisations to significantly increase cyber resilience, reducing both the risk of compromise, as well as the ability to detect and recover. The Zero Trust principles provide a proven and workable model to achieve this.

About Becrypt

Becrypt is an agile London-based UK SME with 20 years cyber security expertise, established through the development and delivery of cloud, mobile and endpoint platforms. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services - from funded research, to commercially available products and flexible managed services. Becrypt have worked with UK Government and platform vendors to pioneer and deploy device health identity management products and services, based on the NCSC CloudClient Architecture.

https://www.becrypt.com/uk/products/paradox/

[i] While references to CloudClient are made with permission, currently NCSC authored content relating to CloudClient is not in the public domain. Principles and objectives relevant to CloudClient are published by NCSC in the context of Zero Trust.

[ii] Remote Attestation implemented as per Trusted Platform Group (https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf)

Establishing Zero Trust and Network Segmentation in MedTech

Global MedTech Manufacturing

Situation & Challenges

- Client desire to conduct a Global IT optimisation program (including Factory/Production IT)
- Existing factory/production technology operational on a single network alongside traditional Enterprise IT with no segmentation in place
- Client had a self-admitted low level of security maturity, with cybersecurity focus on Enterprise IT and limited to no knowledge of OT Security
- Healthcare globally is the #1 attacked vertical by cyber-criminals and the client is at the heart of technology innovation in Healthcare
- Core Enterprise IT and production technology largely legacy in nature and not aligned to technology innovation

Solution Highlights

- Wipro undertook site assessments to document and assess the current state architectures, define and document the new target reference architecture and derive the remediation and implementation roadmap
- Wipro architected a defence in depth and “zero trust reference architecture” that will segment the Enterprise IT and Factory/Production IT environments
- Reference architecture blueprints developed with future state CISCO technology in mind and enabling scalability and technology advancement as a central tenet of larger global infrastructure and security remediation program

Value Proposition

- Highly experienced industry focused team undertook assessment to identify current state and maturity gaps requiring remediation to deliver enhanced cyber resilience
- Advanced zero-trust reference architecture designed delivering rapid security enhancements
- Standardized enterprise architecture delivering trusted zones and active network segmentation
- Delivery of rapid remediation to all global sites on topic of Factory/Production IT
- New target operating model and governance/policy system established to coordinate future state architecture

Gigamon®

SURVEY

The IT & Security Landscape for 2020 and Beyond and the Role of Zero Trust

Executive Summary

The Gigamon EMEA Zero Trust Survey was born out of the idea that perceptions surrounding Zero Trust are changing and attracting increased interest. Typically, Zero Trust held negative connotations due to its 'never trust, always verify' message – the idea being that employee productivity would be hindered. However, our survey opposed this theory, with **87 percent** of those who had started on their Zero Trust journey reporting that adopting the framework has improved their productivity.

What's more, the current economic climate has significantly changed working practices, creating new challenges and an increase in security threats – something **84 percent** decision makers reported – and Zero Trust is now being viewed as a strategic approach to help alleviate this additional burden.

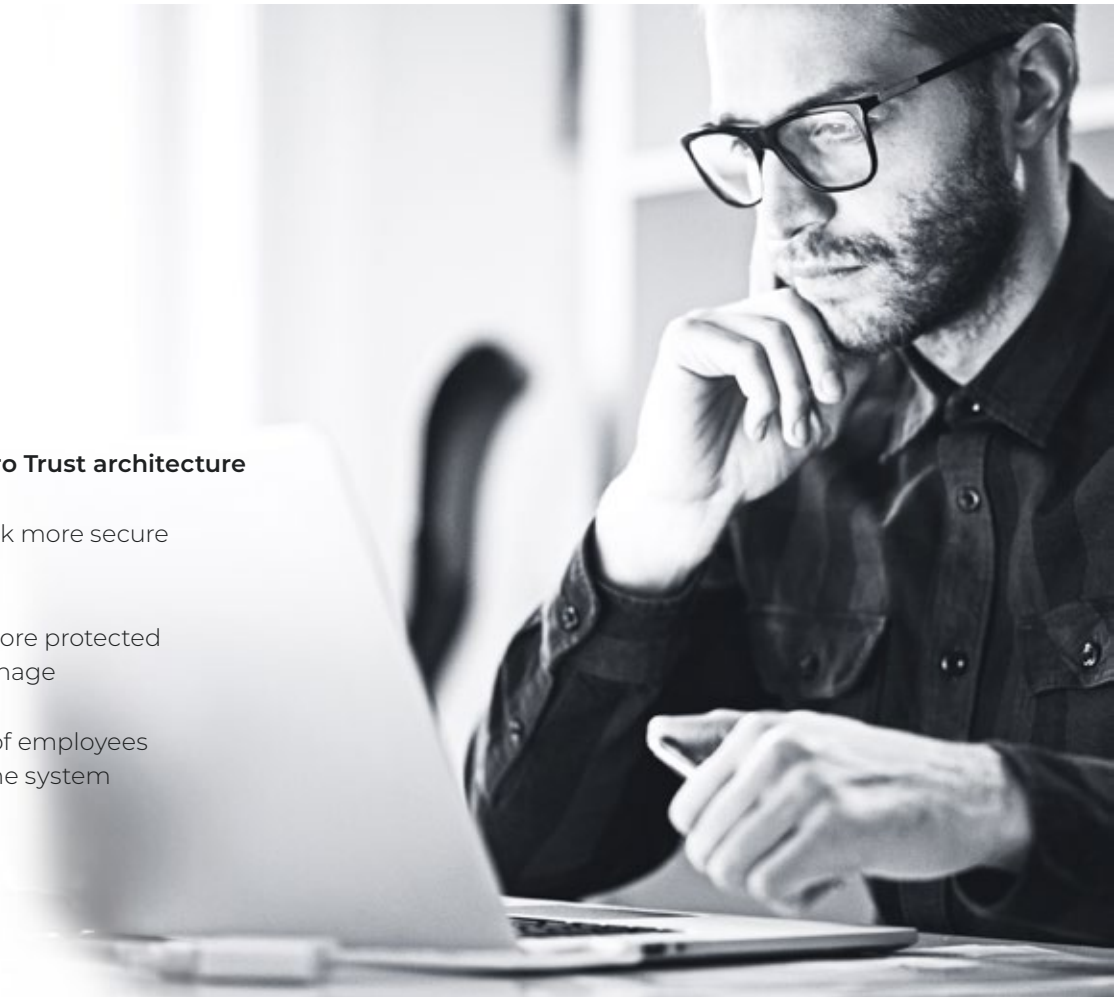
97 percent of respondents who had started their Zero Trust journey stated that the framework has or could help their business as it deals with the current global situation.

The survey collated the responses of 500 IT and security decision makers across the UK, France and Germany, and supported our hypothesis that Zero Trust is a force for good. More and more companies are delving into the concept of Zero Trust and starting on their own journeys towards adopting this architecture. As such, comprehensive awareness of the framework is growing.

The survey found that **89 percent** of respondents had a high awareness of Zero Trust.

As adoption therefore increases – **76 percent** of those who had a high awareness of Zero Trust were adopters or potential adaptors – so does the awareness of its benefits, and adopters are proof that a Zero Trust framework is a competitive advantage for businesses, rather than a necessary evil.

The main reason for adopting Zero Trust architecture is increased security – with **54 percent** stating that the reason they started or are looking to start a journey towards Zero Trust is to secure the network and mitigate risk. With the network constantly evolving, Zero Trust doesn't assume that any user or device is safe based on pre-existing credentials, but instead scrutinises asset behaviour and only grants access to the network and its resources based on this information.



Main reasons to adopt Zero Trust architecture

54% Make our network more secure and mitigate risk

51% Make our data more protected and easier to manage

49% Reduce the risk of employees compromising the system

Protecting data and making it easier to manage was the second most cited reason for adopting Zero Trust architecture at **51 percent**. It's impossible to monitor what you can't see, so companies need a clear view of everything that is happening on their network in order to adopt a Zero Trust framework. Finally, **59 percent** cited that they started adopting Zero Trust to reduce the risk of employees compromising the system.

This 'New Normal' is providing Zero Trust the opportunity to prove its value, as businesses adjust their practices and processes to cope with the changing landscape. Cybercriminals are looking to take advantage of fluid working as employees must protect their corporate network from home. Interestingly, company culture and employee behaviour were both a motivator behind starting on a Zero Trust journey and a barrier.

Shadow IT and employee education were cited as top challenges facing respondents, signalling that businesses may look to adopt Zero Trust to minimise the insider threat. Conversely, **65 percent** of respondents who decided not to adopt the framework cited wrong company culture as the top reason behind this decision and getting employees on board was named the most important thing to have in place before starting the journey towards Zero Trust.

In this challenging time, businesses must continue to transform in order to uphold security and remain competitive. With Zero Trust, IT and security teams can ensure their organisation stays secure without compromising productivity or user experience.

Read the full survey report to find out more.

Gigamon

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 www.gigamon.com

EMEA Headquarters
100 Brook Drive, Green Park, Reading, RG2 6UJ United Kingdom
+44 (0)118 304 0300 emea-info@gigamon.com

09.20_04

BUSINESS BRIEF

Zero Trust

Secure your network by managing trust

Plus, best practices for getting started

The Zero Trust Journey

Myth: It's just the latest unrealistic trend

Reality: Zero Trust is not a trend, but arose out of necessity, and will not go away. Highly publicized breaches (e.g., Google and 35+ other technology companies being compromised as part of Operation Aurora) gave rise to the notion that existing security measures are not enough, and a more comprehensive approach to security is required to defend against all forms of threats.

Myth: It's unattainable.

Reality: Many organizations are shying away from Zero Trust because they don't know where to start, or don't think they can achieve it, predominantly because they don't have the resources, or have a pre-existing mixed batch of technologies. Zero Trust, however, is not an end-state. It's a process that involves making changes and upgrades that improve security each time, and incorporating this process is definitely attainable.

Myth: You have to start from scratch.

Reality: It isn't necessary to 'have a starting point'; you can work with your existing processes, investments and infrastructure.

Myth: It must be done all at once.

Reality: In fact, it's smarter to focus on your business-critical functions and data first.

Myth: Zero Trust...isn't it bad to not trust my people?

Reality: Zero Trust doesn't have to do with not trusting your people; it's about reducing the implicit trust extended to anyone (or anything) that has access to resources on your network. To look at it another way, Zero Trust helps to ensure that the right people are accessing the right systems.

Business is built on trust, right? And trust underpins most of our societal norms, our financial system, our day-to-day interactions...and much of our technology.

Times have changed — especially when it comes to securing your network. The 'implicit trust' we extended within our networks is used against us, via attacks that could expose critical data or bring the network down – and they are coming from every angle. In fact, Zero Trust as a strategy came about as a reaction to large scale attacks where the need to combat attacks from both from outside and within your network perimeters, was identified.

So as a network security best practice...you can't *implicitly* trust anyone or anything trying to connect to your network or systems.

Why Zero Trust — and Why Now?

Traditionally, we set up our network and gave any device on the network open access to everything inside of the perimeter walls of the Local Area Network. Telecommuting and remote work has further pushed us to enable LAN access to remote employees. Now that the gig economy has landed, we're granting access to freelancers and contractors who are performing a variety of tasks. Sometimes consultants, partners and investors even get a peek.

To complicate matters even more, various people across departments are granting access to areas of the network as personnel and roles change.

Too many organizations don't know who is accessing what and when — and any device, account or person could be up to no good. It makes perfect sense: People using devices that have access to storage systems and applications constantly interact with critical data, and any one of their devices and accounts can be targeted and used to compromise the organization as a whole.

In addition, if your organization is like most, you have inherited a legacy of IT and security infrastructure and configurations that conflates devices, users, networks, identities, access and permissions to the point that they're described as flat networks, meaning anyone in the enterprise has or can easily gain access to other users' information, data or applications. This is a veritable paradise for threat actors – compromising what may be seemed as an unimportant device or identity in a network often provides ease of privilege escalation and access to the entire network. And many of today's most highly publicized breaches involve these types of acts.

Zero Trust is a strategy for understanding, managing — and most importantly, decreasing — *implicit* trust in your computing environment. It provides a target framework to address complexity introduced by enterprises that are increasingly embracing mobility, cloud and web-facing applications and services.

In the most basic terms, it means you have zero trust for any person, device or identity that's accessing the network, until you take some steps to verify that the person, device and their associated identity belongs there. Once verified, is also means opening the least amount of access necessary to perform a task…and providing continual monitoring and verification that nothing 'has gone off the rails' – in other words, that your security measures (and your security stack as a whole) are functioning as intended. If it isn't the case, the ability to quickly detect, respond and shut down threats is also a central to Zero Trust.

Zero Trust also has a flip side: you are also enabling trust, helping to ensure that the right people — the people who deserve your trust and have validated themselves — have the right access to the right resources at the right time, while keeping your most critical assets safe.

Zero Trust Is a Journey, Not a Destination

First things first, a magic bullet doesn't exist. You won't find a single solution that will get you to Zero Trust. Instead, think of Zero Trust as a journey, always changing and requiring consistent monitoring. It is an ongoing process, but you're going to be markedly more secure with each step.

You just have to start.

As you plan, and begin to embark on your Zero Trust journey, follow these best practices.

#1. Define Strategies to Monitor and Secure Your Environment
Taking a security stance is also about ensuring that your stance has not been compromised. That involves a well-implemented security process, with threat detection and response as its centerpiece. Adopting a data-centric security model is important, to ensure you have the information you need to quickly identify problems and resolve them quickly. But the focus can't be just on external threats. You need to be monitoring north-south as well as east-west traffic.

Beyond that, you can't fix it and forget it. You also need to *continuously monitor your solutions* and security measures to ensure that they are working as intended and to pinpoint weaknesses.

#2. Understand Where the Highly Critical Data Resides
You must know what data is most important for you to protect and start there.

It requires a shift to data-centric security, where you build layered defenses from the data outwards, with data access controls at the storage layer that enforce strong authentication for the data; for example, allowing only certain users from certain locations to access it.

So, as a first step, take inventory of what is in your environment so that you can create a smaller perimeter — that you can realistically monitor — around your critical data and applications. From there, you can ensure you have deployed the right tools and established the right policies to protect your crown jewels.

The harsh reality is that you can't always protect your entire network, so focus first on what matters most first.

#3. Know Where Implicit Trust Exists
Before you take another step, know exactly where you have granted open access to employees, contractors and third parties. Implicit trust exists typically in one or more of these areas, so it's a good place to start your evaluation:

- VPN connectivity
- LAN/network core
- Specific network segments (or lack thereof)
- Authentication and directory services (active directory)
- Service accounts
- Single-factor authentication

This step is critical because once you know which areas are most vulnerable, you can prioritize your efforts.

#4. Establish Who and What Should Have Access to the Network
Employees are hired, fired, promoted, moved off-site — roles continuously change, as does access to various parts of the network. It is critical to know what every stakeholder's role is and what access each role requires at any point in time.

You need to understand and manage these roles, and you need to revisit them on a regular basis to ensure you are removing and updating permissions as needed. The process requires consistent upkeep because roles change from year to year and even month to month.

That isn't possible without a holistic view of your network, gained only through pervasive visibility not just into the network, but into the people using the resources, devices and network.

#5. Adopt a Zero Trust Strategy
The Zero Trust strategy — that you must verify everyone and everything trying to access your network — must be at the core of your IT strategy. That means looking at existing and new solutions through a 'Zero Trust lens' and prioritizing purchases and changes based on those goals.

Going forward, evaluate each product not just by the direct problem it solves, but how it supports your Zero Trust efforts.

#6. Start Small — and Tackle One Thing at a Time
Guess what. You can back into the process. You don't need to scrap everything and start over. In fact, it's highly likely that you already have most of the technologies needed to secure your network. Once you know where the crown jewels reside, you can segment your network and focus on those critical areas first.

It makes the overall process less overwhelming — and more doable.

The key however is to continue to look at your overall security posture through that Zero Trust POV. You need to assess how all your tools work together — and that requires intelligence behind each security tool.

#7. Gain More Visibility into Encrypted Traffic
More and more traffic is encrypted, which is traffic you can't see. If you can't see it, you have no way of knowing if threats are lurking within it. You simply cannot secure what you cannot see, and you cannot analyze what's hidden.

You need the ability to inspect and facilitate analysis on the massive amount of encrypted traffic traversing your network, while conforming to any regulations you must adhere to. The challenge is that most organizations struggle to keep up with decryption – they often have no plan on how to tackle it.

Adopting a centralized approach to decryption allows you to offload decryption to prevent straining network tools and test new upgrades on the fly without disrupting operations.

It's Time to Start Your Zero Trust Journey

As both the number and sophistication of attacks increase, so does the pressure to protect your network — but you can't fight with blinders on. Network visibility is essential to your success.

Contact Gigamon today to learn how we can help you take the first step in your Zero Trust journey. Or better yet, let us show you ways to get started: request a demo today.

Bassam Khan
VP of Product and Technical Marketing, Gigamon

Bassam Khan serves as Gigamon Vice President of Product and Technical Marketing Engineering, responsible for positioning and promoting the company's products and solutions, as well as corporate and go-to-market strategy. Bassam brings a strong track record of more than 20 years managing products and marketing for security, cloud and collaboration technology companies. Prior to Gigamon, he held executive positions at ControlUp, AppSense, PostPath (acquired by Cisco), Cloudmark and Portal Software. Bassam holds degrees from Carnegie-Mellon University and Boston University.

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 I www.gigamon.com

10.19_01

A Zero Trust security approach for government: Increasing security but also improving IT decision making

Public sector organisations are in the middle of a massive digital transformation. Technology advances like cloud, mobile, microservices and more are transforming the public sector to help them deliver services as efficiently as commercial businesses, meet growing mission-critical demands, and keep up with market expectations and be more agile.

This allows public sector employees and constituents to work remotely and have access to their organisation's applications and services, from anywhere at any time using any device. While digital transformation and cloud migration can help departments reap many benefits such as efficiencies, agility, and happy citizens, it moves precious data out of the perceived safety of on-premises systems. This has subsequently led to the dissolution of the traditional enterprise perimeter.

This transformation also opens new avenues for cyberthreats and expands the attack surface. Fears tied to these threats and the perceived challenges of moving to the cloud have slowed down the government's migration and adoption of modern tools and is perhaps one of the main reasons many legacy systems still dominate in the UK government.

Governments across the world should assume they've already been compromised and take the necessary steps to protect themselves. With this mindset, every user, device, and service that requires access is considered hostile, even if it is a known and approved entity.

The traditional approach is to collect data at the rapidly eroding perimeter, subsequently ignoring users as they continue into the network. Zero-trust architectures require government departments to continuously monitor, detect, evaluate, and enforce policy as users move about the network.

By definition, a successful zero trust security program must:

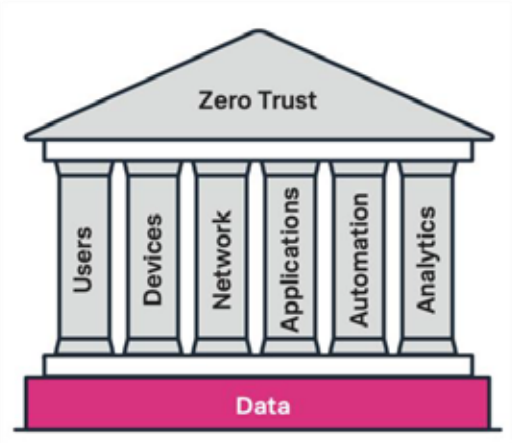
- Assume the network is always hostile.
- Accept that external and internal threats are always on the network.
- Know that the location of a network locality is not enough to decide to trust in a network.
- Authenticate and authorize every device, user, and network flow.
- Implement policies that are dynamic and calculated from as many data sources as possible.

- Log/audit every device, user and object action, and network flow.

Our approach is to offer a continuous monitoring and analytics solution for chief information security officers (CISOs) and security professionals who need to ensure secure access to their data and applications in the modern, perimeter-less enterprise. This helps drive confidence and ongoing trust in access decisions, while ensuring component performance, policy adherence and availability across the zero-trust ecosystem. It is important to be able to ingest data from any source, monitor its infrastructure end-to-end, to optimise and increase effectiveness of the zero-trust ecosystem.

Zero Trust Security Model

The six pillars of a zero trust security model that are built upon a foundation of data!



Users	The ongoing authentication of trusted users, the continuous monitoring and validating of user trustworthiness to govern their access and privileges.
Devices	Measuring the real-time cybersecurity posture and trustworthiness of devices.
Network	The ability to segment, isolate and control the network, including software-defined networks, software-defined wide area networks and internet-based technologies.
Applications	Securing and properly managing the application layer as well as containers and virtual machines.
Automation	Security automation, orchestration and response (SOAR) allows organizations to automate tasks across products through workflows and for interactive end-user oversight.
Analytics	Visibility and analytics are tools like security information and event management (SIEM), advanced security analytics platforms, user and entity behavior analytics (UEBA) enable security experts to observe what is happening and orient defenses more intelligently.

By deploying these tools, you can increase confidence and trust in access decisions to enterprise resources by continuously monitoring and delivering visibility and context across users, assets, and services. Through delivering full-stack visibility into service health, component relationships and infrastructure, ensuring performance and availability, and predicting issues before they happen with machine learning, it will help reduce manual effort, analyst fatigue and costs by enforcing zero trust policies through task automation and workflow orchestration.

This design allows departments to collect enormous amounts of data that can be used to build patterns, trends and analysis that has value far beyond security. Such data can be also used to determine application load demands, maintenance timing, needs for network or system upgrades and much more.

Implementing zero-trust architectures is an opportunity for UK Government Departments to both significantly augment department security postures while also increasing the amount of data that can be leveraged to improve decision making across their IT infrastructure.

For further information please see the following links:

- The essential guide to Zero Trust: https://www.splunk.com/en_us/form/the-essential-guide-to-zero-trust.html
- How zero trust helped insulate Splunk from supply chain attack: https://www.cyberscoop.com/radio/zero-trust-help-insulate-from-supply-chain-attack/
- A guide to embracing a zero trust security model in government: https://www.splunk.com/en_us/pdfs/resources/e-book/zero-trust-security-model-in-government.pdf

To make contact with a Splunk expert please email: pubsec_uk@splunk.com.

techUK
FOR WHAT COMES NEXT

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, Government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

linkedin.com/company/techuk

@techUK

youtube.com/user/techUKViews

info@techuk.org