Threat Landscape Management

The Threat Landscape: Evolve or Die

The cost of cybercrime is predicted to hit $8 trillion in 2023, growing to $10.5 trillion by 2025.[1] That's eye-opening, even for those of us who work in the cybersecurity industry every day. Now think about this—if the cost of cybercrime were measured as a country, then "cybercrime would be the world's third-largest economy after the U.S. and China."[1]

These costs—which translate to $21.9 billion per day in 2023—include damages to and destruction of data, lost productivity, intellectual property theft, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, as well as reputational damage.

What does this mean for your customers? As technology continues to majorly disrupt nearly all aspects of our lives, ensuring resiliency requires your customer to continuously adapt their security capabilities to keep bad actors from preying on vulnerabilities. The result is that preparing for an all-too-inevitable attack has become mission critical. Yet, the goal is less about defending against an attack and more about ensuring resiliency when an attack occurs.

It's also becoming more important than ever for security leaders to clearly communicate their risk and mitigation strategies to business leaders. Yet there's a disconnect between c-suite business executives and security executives (CISOs and other IT security leaders).

For example, 92% of business executives believe that cyber resilience is integrated into enterprise risk management strategies, but only 55% of security executives agreed with this statement. In addition, 59% would find it challenging to respond to a cybersecurity incident due to the skills shortage, but where security executives see this as a key vulnerability, business executives appear less aware of the skills gap. Finally, 84% consider cyber resilience a business priority, but just 68% see cyber resilience as a major part of their overall risk management.

With that in mind, here are some statistics that point to the need for a new approach to security.

This [$8 trillion cost of cybercrime in 2023] represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Cost of a data breach

- $4.45 million in 2023 (an all-time high), 15.3% more than in 2020[3]
- $4.75 million on multi-cloud environments [3]
- $10.93 million is the average cost of healthcare data breach [3]
- $9.48 million is the total average cost of a U.S. data breach [3]
- 53.3% higher healthcare data breach costs since 2020[3]

Cost/time to identify and contain a breach using AI and automation

- 108 fewer days[3]
- $1.76 million less [3]

The unlucky 13

- The healthcare sector has reported the most expensive data breaches for 13 straight years.[3]
- Not to be outdone, the U.S. has had the highest data breach costs for 13 consecutive years.[3]

Top 5 costliest industries[3]

1. Healthcare
2. Financial
3. Pharmaceuticals
4. Energy
5. Industrial

Time to identify and contain a breach in 2023

- 204 days to identify a breach
- 73 days to contain a breach

Most common initial attack vectors in 2023

- Phishing–16%
- Stolen/compromised credentials–15%
- Cloud misconfiguration–11%
- Business email compromise–9%

Most active threats with 10x more queries than other threats

- Cryptomining
- Phishing
- Ransomware
- Trojans

[1]"2022 Official Cybercrime Report," Cybersecurity Ventures, 2022. [2]"Global Cybersecurity Outlook 2022 Insight Report," World Economic Forum, 01/2022. [3]"Cost of a Data Breach Report 2023," IBM.com/Ponemon Institute, 07/2023.

What is Zero Trust?

Infrastructures today have grown increasingly complex. Where once walls were put up around rooms and then buildings and then networks, it's become impossible to rely on traditional "moat around the castle" perimeter security when there's isn't an easily identifiable perimeter. The network is becoming "edgeless." A typical organization, for example, may have several internal networks, remote offices or branches with a separate local infrastructure, remote and/or mobile employees, and cloud services.

In addition, perimeter-based network security is no match for today's more sophisticated network attacks. Once an attacker gains entry, they can pretty much move laterally throughout the network unhindered. Enter zero trust: A zero-trust approach no longer presumes that anyone or anything within the perimeter is safe. Trust must be continually "earned" and granted to users, endpoints, applications and other network components that require access—and only after verification.

Zero trust (and zero-trust architecture) defined ›

Addressing the challenges associated with zero trust ›

Patience is a process, follow the stepped journey ›

What is Zero Trust?

Infrastructures today have grown increasingly complex. Where once walls were put up around rooms and then buildings and then networks, it's become impossible to rely on traditional "moat around the castle" perimeter security when there's isn't an easily identifiable perimeter. The network is becoming "edgeless." A typical organization, for example, may have several internal networks, remote offices or branches with a separate local infrastructure, remote and/or mobile employees, and cloud services.

In addition, perimeter-based network security is no match for today's more sophisticated network attacks. Once an attacker gains entry, they can pretty much move laterally throughout the network practically unhindered. Enter zero trust. A zero-trust approach no longer presumes that anyone or anything within the perimeter is safe. Trust must be continually "earned" and granted to users, endpoints, applications, and other network components that require access—and only after verification.

Zero trust (and zero-trust architecture) defined

Another way to think of it is as the concept of least privilege. In other words, users (and devices and applications) cannot be fully trusted and therefore will be granted access to only the resources they absolutely need to perform their job roles—a continuous process that ensures they are who they say they are. This is vastly different from perimeter-based cybersecurity strategies of just a few years ago.

Generally speaking, we all know what "zero trust" is (and, sometimes, what it isn't). But how does your thinking align with your customer's thinking on network security?

The National Institute of Standards and Technology (NIST) recently updated their definition of zero trust. According to NIST, zero trust "provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

Following that logic, a zero-trust architecture, then, is one "that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero-trust architecture plan." [21]

They go on to say that the goal of zero trust is to "prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible." [21]

Addressing the challenges associated with zero trust

Patience is a process, follow the stepped journey

[21] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Version 2.0, 04/2023

What is Zero Trust?

Infrastructures today have grown increasingly complex. Where once walls were put up around rooms and then buildings and then networks, it's become impossible to rely on traditional "moat around the castle" perimeter security when there's isn't an easily identifiable perimeter. The network is becoming "edgeless." A typical organization, for example, may have several internal networks, remote offices or branches with a separate local infrastructure, remote and/or mobile employees, and cloud services.

In addition, perimeter-based network security is no match for today's more sophisticated network attacks. Once an attacker gains entry, they can pretty much move laterally throughout the network practically unhindered. Enter zero trust. A zero-trust approach no longer presumes that anyone or anything within the perimeter is safe. Trust must be continually "earned" and granted to users, endpoints, applications, and other network components that require access—and only after verification.

Zero trust (and zero-trust architecture) defined

Addressing the challenges associated with zero trust

IT leaders are increasingly adopting zero trust for their network architectures, but it also comes with challenges. First, zero trust isn't a "thing" insomuch as it's an ongoing process toward an ideal. But some believe that a zero-trust approach means that everyone is under suspicion, a cultural mindset that may complicate efforts to successfully introduce and implement zero trust into a customer environment. If this is an issue for your clients (and/or their stakeholders), ask them this: if someone knocks on their door and they don't know who they are, would they let them in? Probably not. They'd ask for an identity to build "real trust" before allowing them to enter.

Another issue relates to third-party sites and the digital supply chain. Cyberattacks against third parties are on the rise. Your customer may contract with a third-party supplier who contracts with its own third-party suppliers, which brings huge downstream security risks. The challenge is that just 23% of security and risk leaders monitor third parties in real time for cybersecurity exposure.[23] Shadow IT also continues to be an issue, as does the problem of security silos. In fact, 75% of employees will acquire, modify, or create technology outside IT's visibility by 2027, up from 41% in 2022.[24] If your customer has undiscovered resources on the network and uses tools that aren't integrated for a single source of truth, their business is automatically at risk. But this would be true, regardless of which security framework they're using.

The old standbys of legacy technologies, budget constraints, talent shortages, and resistance also come into play when it comes to risk. That said, a zero-trust approach requires you to address these and other challenges up front. Not doing so invites advanced threats into your customer's environment, putting their sensitive data, networks, and resources at risk. Implementing the right solutions not only helps your customer to overcome these challenges, but it also protects them against the most sophisticated cyber threats. As Gartner says:

> *A mature, widely deployed zero-trust implementation demands integration and configuration of multiple different components, which can become quite technical and complex. Success is highly dependent on the translation to business value. Starting small, an ever evolving zero-trust mindset makes it easier to better grasp the benefits of a program and manage some of the complexity one step at a time.*[25]

As the role of IT leaders continues to shift, from those who control the technology to those who facilitate risk decisions, it's important to re-frame your customer's perspective and steer them toward a zero-trust approach. Gartner recommends "thinking beyond technology and automation to deeply engage with employees to influence decision making and ensure they have appropriate knowledge to do in an informed way." The same applies to your customer.

Patience is a process, follow the stepped journey

[23] "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," Gartner.com, 01/30/2022. [24] "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," Gartner.com, 03/28/2023. [25] "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," Gartner.com, 03/28/2023.

What is Zero Trust?

Infrastructures today have grown increasingly complex. Where once walls were put up around rooms and then buildings and then networks, it's become impossible to rely on traditional "moat around the castle" perimeter security when there's isn't an easily identifiable perimeter. The network is becoming "edgeless." A typical organization, for example, may have several internal networks, remote offices or branches with a separate local infrastructure, remote and/or mobile employees, and cloud services.

In addition, perimeter-based network security is no match for today's more sophisticated network attacks. Once an attacker gains entry, they can pretty much move laterally throughout the network practically unhindered. Enter zero trust. A zero-trust approach no longer presumes that anyone or anything within the perimeter is safe. Trust must be continually "earned" and granted to users, endpoints, applications, and other network components that require access—and only after verification.

Zero trust (and zero-trust architecture) defined

Addressing the challenges associated with zero trust

Patience is a process, follow the stepped journey

Finally, zero trust isn't a "thing" to achieve. It's a journey—a years-long process that requires continuous attention and a stepped approach, given the challenges, the numerous policies and procedures and the massive scope of work involved. As you work with your customer, consider the steps you can help them take today, the steps to do next and what can be dealt with later.

By 2026,

10%

of large enterprises

will have a comprehensive, mature, and measurable zero-trust program in place, up from less than 1% today.[26]

Just

23%

of security and riskleaders

monitor third parties in real time for cybersecurity exposure.[27]

> *"The path to zero trust is an incremental process that may take years to implement."*[28]

[26] "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," Gartner.com, 03/28/2023. [27] "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," Gartner.com, 01/30/2022. [28] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Version 2.0, 04/2023.

Why a Zero Trust Framework?

The 7 tenets of zero trust

The security maturity journey: The road is long

Why a Zero Trust Framework?

The 7 tenets of zero trust

Here are some basic tenets of zero trust[29] to consider as you're designing and deploying a zero-trust architecture for your customer. While these are all ideals in a perfect world, your customer's specific strategy will drive how or to what extent each is implemented.

1. **All data sources and computing services are considered resources.** For example, BYOD, SaaS, and other systems and devices—anything that requires access to your customer's data.

2. **All communication is secured regardless of network location.** In other words, network location alone does not confer trust, so all access requests coming from "inside the house" must meet the same requirements as requests coming from outside the organization.

3. **Access to individual enterprise resources is granted on a per-session basis.** Generally speaking, access requests are granted on a case-by-case basis; having been authenticated and authorized once does not imply access in the future.

4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.** Rules and attributes are based on the needs of the business process and acceptable level of risk.

5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** Since no asset is trusted, organizations should deploy a continuous diagnostics and mitigation (CDM) or similar system to provide actionable data about the current state of network resources—including BYOD, unmanaged and other resources—and apply patches and policies as needed.

6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** In other words, network resources undergo a continuous cycle of scanning and assessing threats, adapting, and continually reevaluating trust in response to access requests.

7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** Finally, your customer should use any and all info received to improve policy creation and enforcement.

The security maturity journey: The road is long

[29] "Zero Trust Architecture," NIST Special Publication 800-207, National institute of Standards and Technology, U.S. Department of Commerce, 08/2020.

Why a Zero Trust Framework?

The 7 tenets of zero trust

The security maturity journey: The road is long

NIST likens the zero-trust journey to climbing a mountain. Everyone starts on flat terrain (or the traditional model) and traverses the mountain until they reach the top, or optimal stage. As they increasingly mature, the required levels of effort and realized will grow exponentially as they take advantage of increasingly "dynamic updates, automated processes, integrated capabilities and other characteristics."[30] But because this journey can take place over many years, the stages are naturally dynamic; progress from one stage to another may shift in scope and impact over time.

According to recent research, organizations that achieved mature zero-trust implementations were twice as likely to report excelling at these five security practices:[31]

- Accurate threat detection
- Proactive tech refresh
- Prompt disaster recovery
- Timely incident response
- Well-integrated tech

Where is your customer on the zero-trust continuum? What can you do to help them find the quick wins, gain momentum and continue to make progress towards maturing their zero trust security?

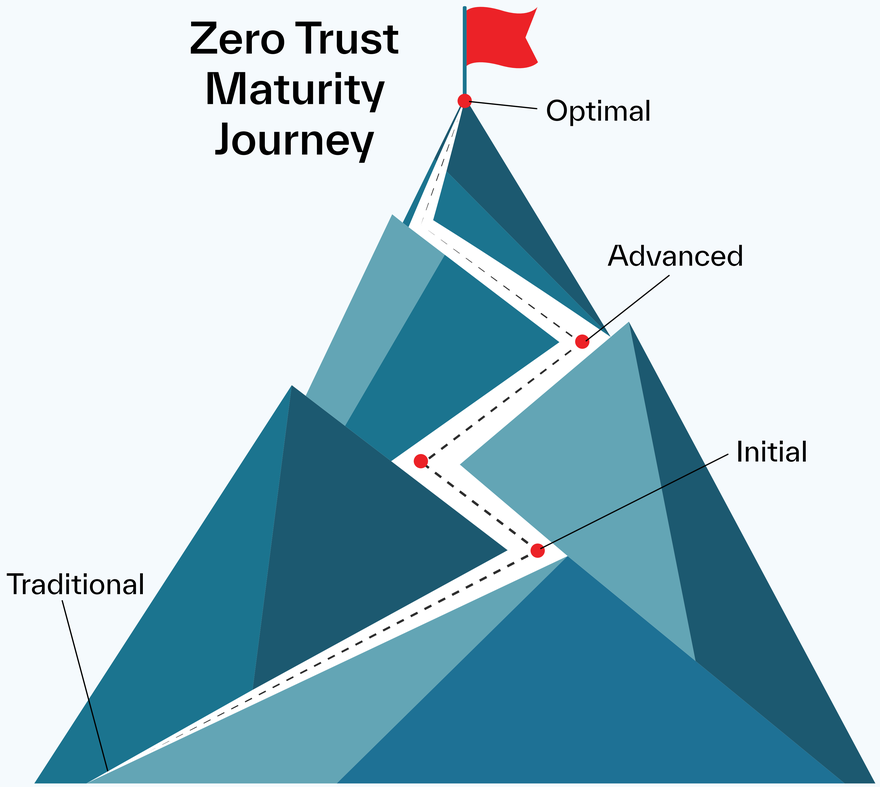
Organizations that reported a mature implementation of zero trust were more than twice as likely

63%

to achieve business resilience

than those with a limited zero trust implementation.[33]

> *"...start by developing an effective zero-trust strategy which balances the need for security with the need to run the business."*[32]



[30]National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Version 2.0, 04/2023. [31]"Cisco's Guide to Zero Trust Maturity: How to Find Quick Wins," Cisco.com, 2022.
[32]"Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026," Gartner.com, 01/23/2023. [33] "Cisco's Guide to Zero Trust Maturity: How to Find Quick Wins," Cisco.com, 2022.

The Zero Trust Architecture

Once the strategy is defined, you can turn your attention to building a zero-trust architecture for your client. A zero-trust architecture comprises multiple security technologies, but identity—including the people, processes and technologies to build those identities—are foundational to zero trust. These technologies include identity and access management (IAM), single sign-on (SSO), and multi-factor authentication (MFA). Network segmentation and micro-segmentation also play a role as does zero trust network access (ZTNA). Rather than protect a finite perimeter, these technologies help your customer protect a boundless perimeter with continuous identity verification and activity monitoring, ensuring that only authorized users and devices have access to sensitive resources.

Additionally, zero trust technologies go beyond in terms of helping your client meet compliance requirements, particularly as they regard data privacy and security. Again, this continuous verification enables you to better protect sensitive data, while helping your customer prove compliance.

Types of zero trust solutions

- **Multi-factor authentication (MFA)–** Zero-trust architectures rely on implementing multiple points of authentication and require users to continually authenticate themselves. Without these controls, your customer cannot sufficiently control access to resources.

  MFA requires users to provide two or more authentication factors—typically something a user knows, has, and is—to verify their identity before they're allowed to access the requested resource. For example, a password or PIN is something a user knows, a mobile phone or security token is something a user has, and fingerprints or facial recognition is something the user is.

  By requiring at least two authentication factors, MFA makes it much more difficult for bad actors to gain access. And by using MFA in conjunction with an identity and access management (IAM) system, you can add yet another layer of security.

- **Identity and access management–** IAM systems help your customer ensure that only authorized users have access to sensitive resources. It enables them to set and enforce policies for who has access to what, and continuously verifies identities to ensure authorization to access.

  As such, these technologies typically include capabilities, such as user provisioning, access control, and identity federation, enabling organizations to manage user access to systems and resources.

  Finally, IAM technologies can detect instances of unauthorized activity, helping organizations to not only prevent potential security breaches, but also to meet compliance requirements. Single sign-on works with IAM to enable users to access multiple resources with a single set of credentials.

- **Zero trust network access (ZTNA)–** With a cloud-driven, remote-enabled, device-agnostic future comes a new zero-trust approach to security: zero trust network access. ZTNA is often defined in terms of its chief use case: as a VPN alternative. Unlike VPNs, ZTNA is more scalable, enables a blanket security policy, works across hybrid IT, and offers more granular access. In other words, where VPNs provide network-wide access, ZTNAs grant access to specific resources and require frequent reauthentication.

  But there are other ZTNA use cases as well, including location- or device-specific authentication and access, holistic control and visibility, application-based access for third parties, and immediate access to internal resources for M&A projects.

  Depending on your customer's use case, there are two implementation approaches: agent-based ZTNA is typically deployed as part of a larger SASE architecture or SSE offering, while clientless ZTNA often supports third-party and BYOD initiatives.

  Finally, the key benefit of ZTNA is that it allows your customer to apply zero trust security to their networks without exposing other services to potential attackers. It reduces the attack surface, minimizes risk and spread, limits internet-based threats, and restricts access to cloud environments and applications.

- Network segmentation/micro-segmentation – Dividing networks and workloads into smaller zones helps to minimize the impact of an intrusion when it occurs. Microsoft offers a more colorful description when it says that:

  "Organizations should not just have one single, big pipe in and out of their network. In a Zero Trust approach, networks are instead segmented into smaller islands where specific workloads are contained. Each segment has its own ingress and egress controls to minimize the "blast radius" of unauthorized access to data.

  By implementing software-defined perimeters with granular controls, you increase the difficulty for unauthorized actors to propagate throughout your network, and so reduce the lateral movement of threats."[34]

In the following pages, you'll find a set of technologies and practices to help you build a zero-trust architecture that helps protect your customers' systems from cyberattacks.

"Zero trust progress can be achieved no matter the size of an organization or the level of complexity in the IT infrastructure."[35]

[34] "Secure Networks with Zero Trust," Learn.Microsoft.com, 03/29/2023.

[35] "Cisco's Guide to Zero Trust Maturity: How to Fnd Quick Wins," Cisco.com, 2022.

Managed Detection & Response (MDR)

With IT staffing issues across nearly every vertical and thousands of alerts coming at your customer every day, it's impossible to make intelligent decisions about how to handle every alert. Mistakes are bound to happen, creating gaps for security incidents and breaches. With a zero-trust architecture and skilled security specialists monitoring your client's network, we can limit the scope of attacks with fast detection that minimizes damage to their organization.

Managed detection and response (MDR) services "provide customers with remotely delivered, human-led, turnkey, modern SOC functions; ultimately delivering threat disruption and containment." In other words, it adds the human element to detection and response. These 24x7 remotely delivered modern security operations center (SOC) monitoring capabilities feature experts who can quickly parse massive numbers of alerts to detect, analyze, investigate and actively mitigate incidents across endpoints, networks, logs and cloud.

You can leverage a pre-defined technology stack to collect relevant logs, data and contextual information and provide a turnkey experience for your customer. Telemetry is analyzed by the platform, enabling deep investigation by experts skilled in threat hunting and incident management who deliver outcomes that your client can act on. MDR is an established high-growth market. Gartner predicts that by 2025, 50% of organizations will be using MDR services and the MDR market will reach $2.15 billion, up from $1.03 billion in 2021, for a CAGR of 20.2%.

By 2025,

60%

of organizations

will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today.[39]

Consider these solutions:

ActZero

- **ActZero Free –** Secure five mobile devices with Mobile MDR, including 24/7 SOC and support, on-device protection, real-time alerting and auto blocking and access to their MDR platform.
- **ActZero MDR –** Secure endpoints, network, mobile devices, cloud, identity and email accounts with 24/7 SOC and live support, daily threat hunting, vulnerability management, real-time alerting and auto blocking, active response, managed remediation, incident response, on-demand dedicated security advisor and access to our MDR platform.
- **ActZero Premier –** Secure it all with ActZero's MDR bundle, including management, endpoint hygiene, device control, cloud security posture, asset discovery, proactive check-ins, VCISO and compliance advisory.

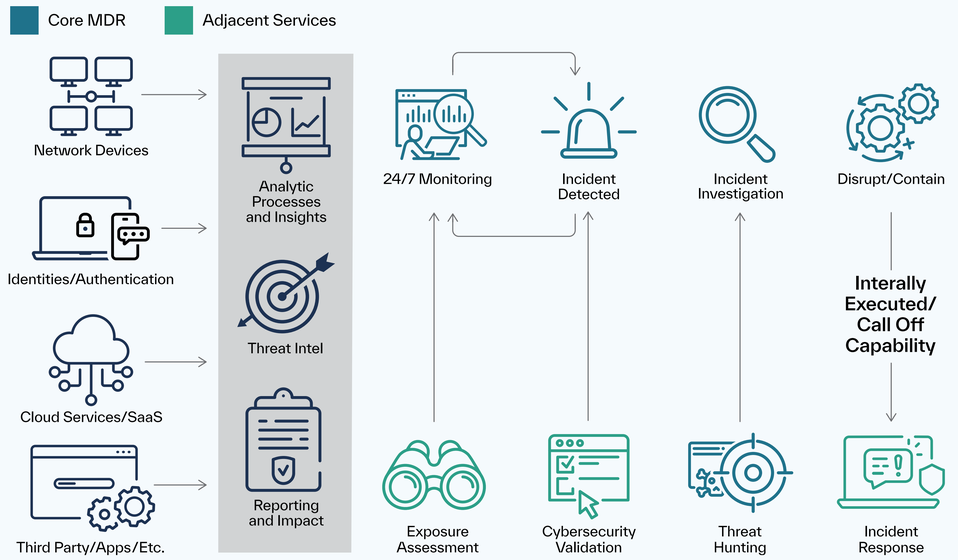
Dell

- **Dell MDR Pro Plus –** Experience Dell MDR Pro Plus, our fully managed, 360⁰ security operations solution—including our most cutting-edge, preventive and responsive cybersecurity services—to help alleviate your customers' top security concerns and enable them to focus on their core business goals.
- **Dell MDR, MDR Pro, MDR Pro Plus –** Earn valuable services tier credit towards Dell Partner Program metal status (3X, for each dollar purchased with a minimum of 50 endpoint devices), plus earn 3.5% rebate on order revenue.

WatchGuard

- **WatchGuard Endpoint Security –** Easily manage the technologies—including next-generation antivirus, EDR, and DNS filtering solutions—required to stop advanced cyberattacks, along with a full stack of integrated modules for additional layers of protection for patching, extended visibility and data control.

Managed Detection and Response and Adjacent Services



[34] "Secure Networks with Zero Trust," Learn.Microsoft.com, 03/29/2023. [35] "Cisco's Guide to Zero Trust Maturity: How to Fnd Quick Wins," Cisco.com, 2022. [39] "Market Guide for Managed Detection and Response," Gartner.com, # G00761083, 02/14/2023.

Network Security

Network security includes a set of technologies that protect the usability and integrity of your customer's network infrastructure by preventing the entry or lateral spread of potential threats. It combines multi-layered defenses that are scalable and automated, along with policies and controls at the edge and in the network. The goal is to prevent unauthorized access, misuse, or theft and enable users, devices, and applications to securely work. Authorized users are allowed access, while bad actors are blocked.

The core elements of network security in a zero-trust architecture are access control and threat control. Access control restricts the movement of bad actors throughout the network, while threat control prevents bad actors, after gaining entry, from doing damage within the network. Some types of network security technologies include access control (for example, IAM, SSO, etc.), firewalls, intrusion prevention systems, network segmentation, cloud security, application security, SIEM and others.

In a zero-trust architecture, the "trust, but verify" model of network security has gradually evolved into "never trust, always verify." This transformation began with the cloud migration of business transformation initiatives but was accelerated by work-from-home initiatives and distributed environments during the pandemic. While all organizations can benefit from network security and a zero-trust architecture, your customer will especially benefit if they have a lack of security expertise, compliance requirements, user experience issues, or concerns about getting cyber insurance in light of fast-changing market conditions. It's especially important if they need to protect:

Consider these solutions:

Fortinet

- **Fortinet FortiSandbox –** Identify and isolate advanced threats in real time—using machine learning to inspect network traffic, files, and URLs and detect malicious activity, including zero-day threats—and analyze suspicious threats in a secure virtual environment via sandboxing technology.
- **Fortinet FortiRecon –** Get complete visibility into your external threat landscape with this digital risk protection service—which includes External Attack Surface Management (EASM)—to identify exposed, vulnerable known and unknown assets and prioritize remediation.

Progress

- **Progress Flowmon Collector –** Collect, store, and analyze flow data and enable highly scalable data storage and built-in analytics for full network visibility and troubleshooting—plus, choose a virtual, cloud, or hardware appliance for anywhere use.

SonicWall

- **SonicWall TZ Series Next-Generation Firewalls (NGFW) –** Easily manage the technologies—including next-generation antivirus, EDR, and DNS filtering solutions—required to stop advanced cyberattacks, along with a full stack of integrated modules for additional layers of protection for patching, extended visibility, and data control.
- **SonicWall Switches –** Deliver high-speed switching with feature-rich switches that enable you to add more devices, keep up with SaaS proliferation, and gain more control—all while protecting your network and your budget.
- **SonicWall NSa Series Next-Generation Firewall –** Enable businesses of 250+ users to know, with confidence, that they're protected against day-to-day incursions—along with advanced threats like ransomware, attacks against non-standard ports, and breaches in firewalls—all at the speed of business.

Veritas

- **Veritas Alta Data Protection –** Deliver the industry's broadest protection for cloud workloads, spanning 60+ cloud environments—with AI-powered automation, flexible recovery options, cloud-native storage technology and elastic infrastructure for reduced costs and carbon footprint.
- **Veritas Alta SaaS Protection –** Provide multi-layered data protection for SaaS applications for a powerful data management and protection solution that provides fully managed, cost-effective, automated backup as a service (BaaS) through a single, intuitive interface.

VMware

- **VMware NSX-T Data Center –** Enable micro-segmentation with this network virtualization and security platform that enables you to create granular security policies and isolate workloads to prevent lateral movement of threats within the data center.

WatchGuard

- **WatchGuard AuthPoint Identity Security–** Work confidently and worry-free with easy-to-use, cost-effective and complete security needed to protect identities, assets, accounts, and information and stop advanced cyberattacks.
- **WatchGuard Firebox Network Security –** Put security professionals back in charge of their networks with a comprehensive advanced network security appliance with widely deployable, enterprise-grade securityand threat viability tools.

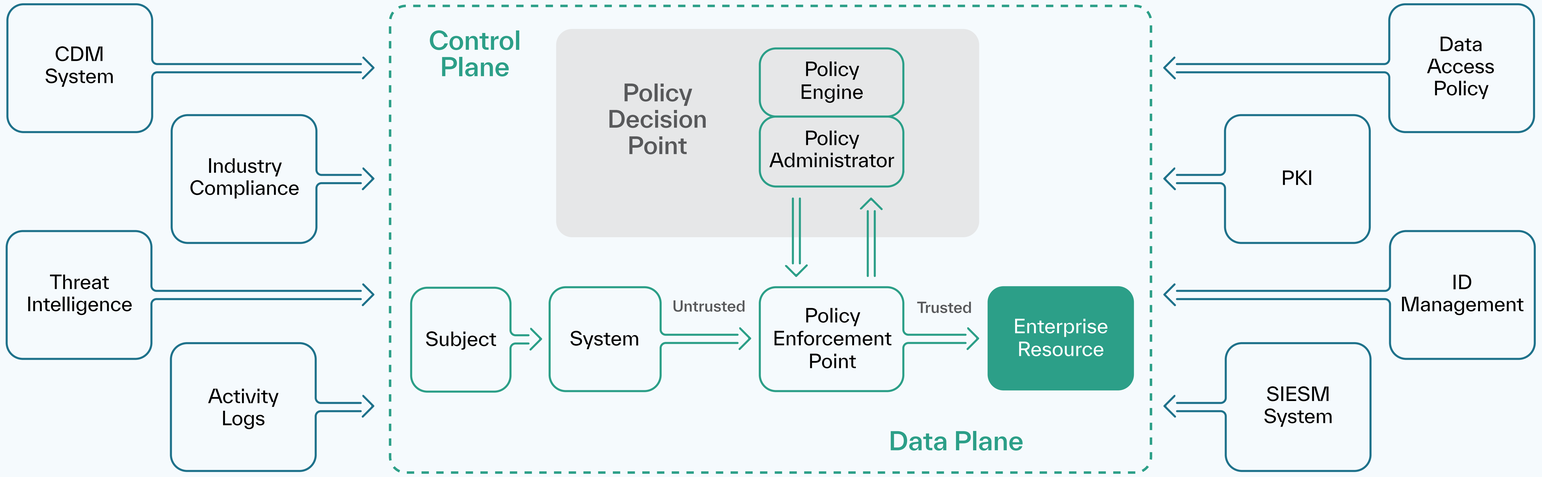
Threat Intelligence

A zero-trust architecture uses multiple technologies to achieve its aims, including threat intelligence. That makes it a core component of a zero-trust architecture, according to NIST. These threat intelligence tools gather data from internal and/or multiple external sources to help the policy engine make access decisions and provide relevant information to your customer about potential attacks or vulnerabilities. It can also include newly discovered flaws in software, newly identified malware and reported attacks on other assets so the policy engine can deny access to enterprise assets.

By then infusing threat intelligence with AI and machine learning, your client can boost zero trust with comprehensive diagnostics and mitigation. With this data, you'll know which controls you can implement to prevent attacks in their initial stages. Threat intelligence can also identify behavioral anomalies by comparing network traffic against previously known threat actors and the tactics, techniques, and procedures (TTPs) they use and trigger additional verification or even block the user or device entirely.

According to NIST, it's important to ensure that to be integrated into a zero-trust architecture, threat intelligence should be scalable, automated, and well-integrated with other security controls. They further recommend establishing a process to collect, analyze, and disseminate threat intelligence—a process that should also be well-integrated with other security controls, such as network segmentation and access control.

Zero-Trust Architecture Deployment Cycle



Consider these solutions:

Fortinet

- **Fortinet FortiGuard Labs 2H 2022 Threat Landscape Report –** Download the latest report from the FortiGuard Labs team and check out the cyber threat landscape over the year's second half.

Download Now

Progress

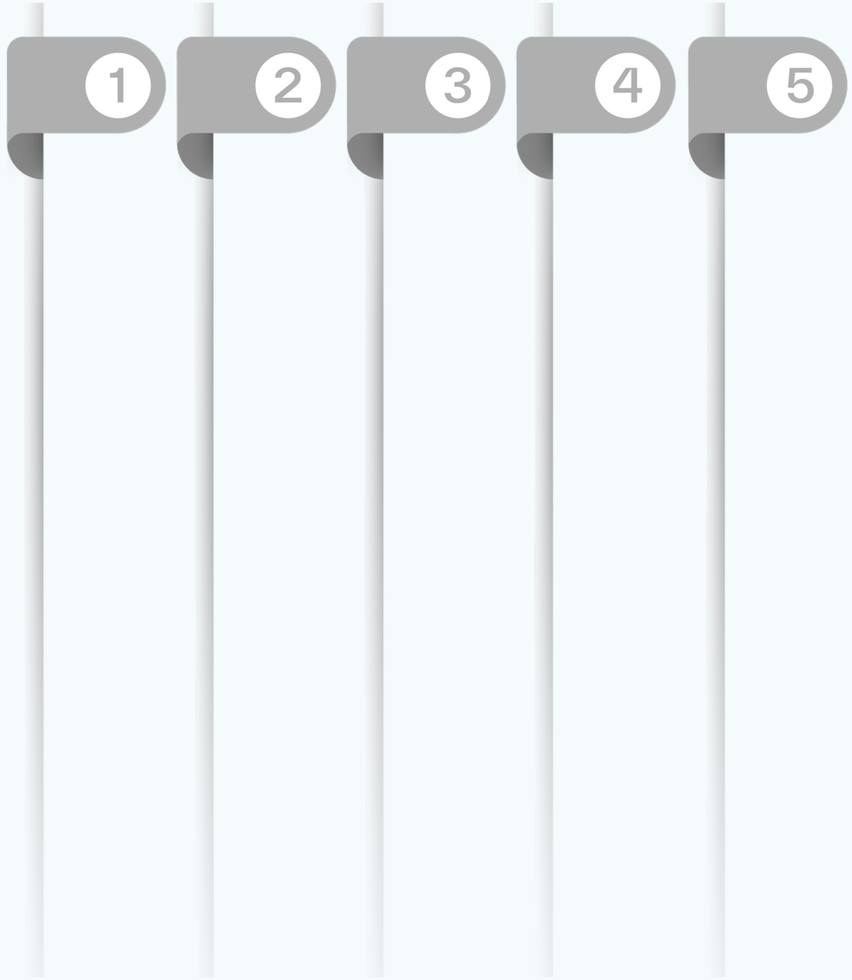
- **Progress Flowmon Probe –** Generate data down to the application level for more granular user experience monitoring, network troubleshooting, and threat detection—plus, choose virtual, cloud, or hardware appliance for anywhere use.
- **Progress Flowmon ADS –** Leverage behavioral analysis algorithms—via an intelligent detection engine—to detect anomalies hidden within network traffic and expose malicious behaviors, attacks against mission-critical applications, data breaches and indicators of compromise.

VMware

- **VMware Carbon Black –** Get real-time threat intelligence and proactive threat hunting capabilities with a comprehensive endpoint security platform that applies behavioral analytics and machine learning to detect and respond to advanced threats.
- **VMware Workspace ONE Intelligence –** Proactively identify and remediate potential threats across the enterprise with a unified digital workspace platform that combines endpoint management with threat analytics, providing insights into user behavior and device security posture.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:



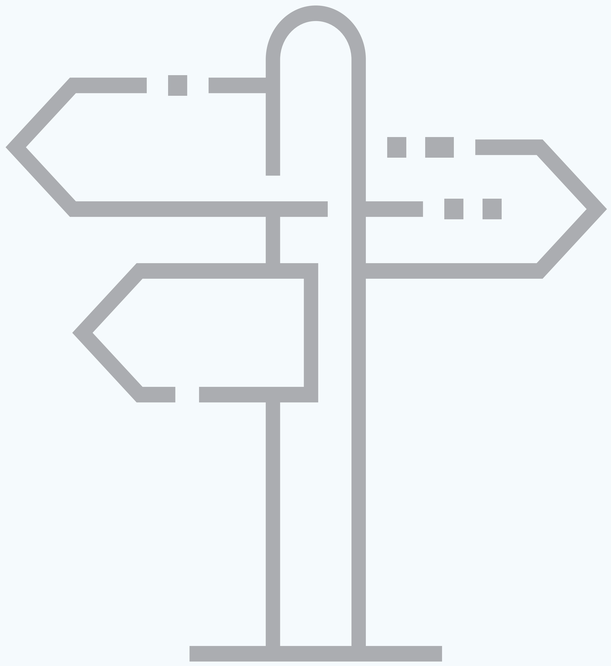
Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 Build a zero-trust roadmap

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer's zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester or others. TD SYNNEX can help you select the right vendors to help you craft a zero-trust vision.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.



2 3 4 5

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 | 3 | 4 | 5

2 Refine the business continuity plan

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems and their criticality to make it easy to prioritize actions in case there's a threat or attack. Create playbooks, conduct tabletop exercises, and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 **3 Assess their environment** 4 5

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments and many others.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 **4 Offer comprehensive services** 5

Help customers focus on their core business by leveraging our advanced managed and other security services.

- **Incident Response Services –** Comprehensive incident response (IR) services—including plan development, readiness review and emergency response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA, HITRUST, PCI-DSS, NIST 800-171, ISO 27001, NERC-CIP, SOC 1&2, GDPR and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations and staff augmentations to help you design the best solution for them.
- **Managed Security Services –** These managed services help you maximize limited resources:
  - **SOC as a Service :** Have a bench of cyber experts who can monitor, analyze, manage and act on threats across your customer's business.
  - **Firewall Services :** Help your customer focus on their core business while you administer, monitor and maintain their firewall infrastructure.
  - **ISAO Threat Feed :** Join a very large community of companies, local governments, and security professionals to collaborate, share intelligence, and participate in training and conferences and leverage competent collaborative analysis.

Consider these solutions:

Dell

- **Dell Incident Recovery (IRR) –** Proactively evaluate your customer's existing incident response plan with our 40-hour service—and, if an incident does occur, Dell experts will quickly assess the situation, determine the best course of action, and take the necessary steps for recovery (an additional 120 or 240 hours).

Veritas

- **Veritas Alta Recovery Vault –** Ensure the lowest TCO for your customer's cloud storage requirements with this fully managed, cloud-based data retention service—featuring award-winning NetBackup's end-to-end deduplication, ransomware protection with immutability, predictable monthly costs, and the industry's broadest workload support.

Opportunities for MSPs & MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4

5 Engage through training & engagement experiences

Finally, engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor, and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses, and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment. leverage competent collaborative analysis.

Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Common Service Recommendations[41]

- Email security
- Network security
- Managed firewalls
- Ransomware backup services
- Identity and access management (IAM)
- Managed detection and response (MDR)
- Extended detection and response (XDR)
- Incident response services
- Security awareness training

[41] "Top Managed Security Services for SMBs," ChannelInsider.com, 04/04/2022.

We're Here to Help...

If your team is short on time, budget, or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help to address most critical cybersecurity needs.

Our sponsors are listed on the next page, along with an email address to reach a TD SYNNEX security professional. Contact us...we're here to help.

Organizations that reported a mature implementation of zero trust were 2X more likely to report excelling across desired outcomes such as:

Greater executive confidence
47%

Peer buy-in
45%

Keeping up with the business
47%

Creating a security culture

Thank You to Our Sponsors!

For more information on any one of these security solutions or services, please contact the security professionals below:

ActZero®

Contact Us

DELL Technologies AUTHORIZED DISTRIBUTOR

Contact Us

FORTINET®

Contact Us

Progress®

Contact Us

SONICWALL™

Contact Us

VERITAS™

Contact Us

vmware®

Contact Us

WatchGuard™

Contact Us

You can also reach out to CyberSolv@tdsynnex.com for more information on our other cybersecurity solutions and services.