SYXSENSE®

Embracing the Zero Trust Mindset for Endpoints

Written by

Charles Kolodgy
Security Mindsets LLC

Charles J. Kolodgy

Security Mindsets LLC

Charles J Kolodgy is a security strategist, visionary, forecaster, educator, historian, and advisor.

He has been involved in the cyber security field for decades. He identifies market trends, specifically he defined the Unified Threat Management (UTM) market. He has been deeply engaged in advancing application security, encryption, and the human element of security.

Presently he is Principal at Security Mindsets LLC and an Adjunct Professor at Rivier University.

Table of Contents

What This Is All About..... 4
Endpoints Are the Destination..... 6
Zero Trust..... 9
- Origins of Zero Trust..... 9
- The Zero Trust Mindset..... 10

Moving to a Zero Trust Architecture..... 12
- Design It..... 12
- Implementation Journey..... 13
- How to Implement Zero Trust in Your Environment..... 14
- Zero Trust Maturity Model..... 16

How Zero Trust and Endpoint Security are Compatible..... 17
The Urgency to “Shift-Left”..... 20
Zero Trust with Syxsense..... 21
- How Syxsense Supports Zero Trust..... 22
- Syxsense Zero Trust Evaluation Engine..... 23

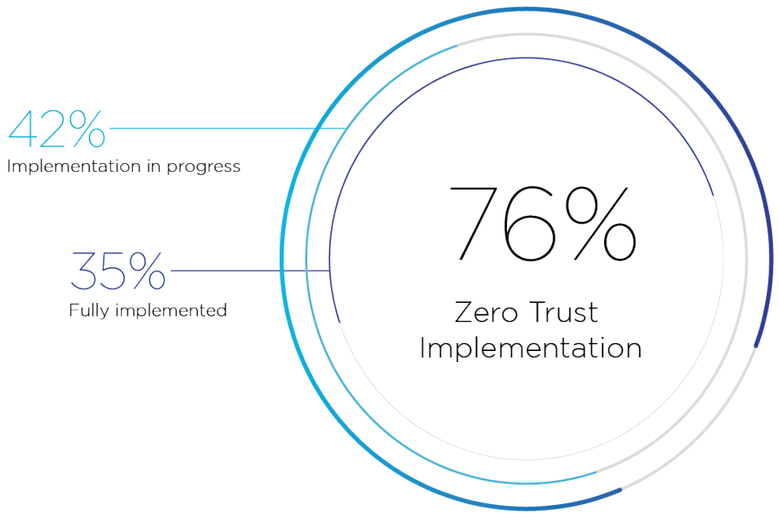
Final Comments..... 24

What This Is All About

Information technology (IT) has drastically improved business operations. It changes the nature of work. It elevates productivity, expands communications and data sharing, and frees people to work from anywhere. However, IT can also be abused by attackers and criminals. Every positive innovation is offset by new threats and dangers.

Cybersecurity professionals and the gamut of attackers are engaged in a constant struggle. Security technologies and frameworks are developed to address each new security challenge. Security strategies and game plans continue to be honed and improved.

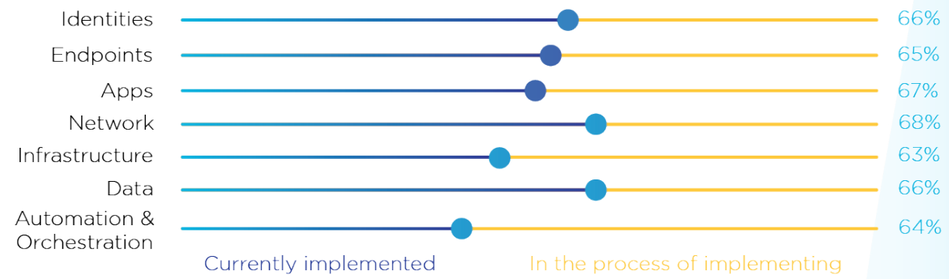
The “Zero Trust” security framework is being embraced as a solution best suited to address the most pressing cybersecurity concerns. Nearly three out of four organizations have begun to implement some aspects of a Zero Trust strategy.



Source: Microsoft Security's Zero Trust Adoption Report, July 2021

Zero Trust, introduced as a call to change the security archetype, is a strategic security mindset modernizing cyber security by encouraging the interweaving of multiple security disciplines into a comprehensive solution which fosters business transformation while expanding overall protection.

Zero Trust initially focused on networks and identity but has morphed into a comprehensive strategy which requires close interaction between all types of security solutions, including Unified Endpoint Management, security automation, analytics, and threat intelligence.



Source: Microsoft Security's Zero Trust Adoption Report, July 2021

This paper will explain the Zero Trust mindset, how it has evolved from concept to implementation, and explain some basics around implementing a Zero Trust framework. The specific focus is explaining how a Zero Trust architecture and Unified Endpoint Management are compatible and how the integration of a comprehensive solution for device hygiene fits within Zero Trust and how it can be achieved.

Endpoints Are the Destination

In simple terms, an organization's IT infrastructure consists of two components — networks and endpoints. Both are needed and both must be protected from misuse but ultimately of those two, attackers focus on gaining undetected privileged access to endpoints. The network is the attack avenue, but endpoints are the destination.

Endpoints, be they servers, virtual machines, workstations, desktops, laptops, tablets, or mobile devices, are where work takes place. They run multiple applications that create, store, and manipulate data. They connect to data sources and other devices.

Today's mobile work environment means endpoints can live anywhere and go everywhere. Infiltrators recognize that to ultimately succeed they must live on an endpoint, which explains why cyber criminals strive to control endpoints.

Compromising an endpoint provides attackers a starting point for a deeper infiltration into an enterprise's network, or in some cases direct access to valuable data. Living on an endpoint, or multiple endpoints, allows the attacker to operate with the appearance of authenticity.

"The network is the attack avenue, but endpoints are the destination."

They leverage their new position to gather intelligence about company operations and system behavior which strengthens their cover of legitimacy.

The endpoint becomes a safe haven from which they can further their incursion by gaining additional credentials, moving laterally within the enterprise environment, maintaining persistence, and eventually exfiltrating data.

Once they become entrenched it can be difficult to root them out because ensuring that all traces of the intruders are removed is difficult and there is also some reluctance to intervene on some devices for fear of negatively impacting business operations.

Knowing endpoints are prized targets doesn't prevent them from being compromised. One reason is that endpoints are constantly in use, making it difficult to lock them down. The growing number and types of devices constantly connecting and disconnecting to the network creates a tremendous attack surface.

Attack Surface Management (ASM)

ASM involves a combination of people, processes, technologies and services deployed to continuously discover, inventory and manage an organization's assets. These assets can be both internal and external, and they pose digital risks. This visibility can help reduce exposure that could be exploited by malicious threat actors.

Gartner, 2022

Attackers also have a huge toolbox of attack techniques — the specific steps or behaviors that cascade into a string of activities required to install malware and to gain operational control of endpoints. A comprehensive inventory of attack techniques is contained within the MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework.

Q1 2022
Incident Response Insights

57%

of total incidents were caused by the exploitation of external vulnerabilities

Tetra Defense

As of July 2022, there are 191 techniques and 385 sub-techniques on how attackers can penetrate an enterprise network. Attack methods specifically geared to endpoint compromise number around 200 techniques and sub-techniques.

The specific methods attackers use is important but of potentially greater concern is attackers getting an assist from targeted devices. Many attack methods only work against systems vulnerable to the specific attack. Ultimately successful incursions result from the exploitation of vulnerabilities.

Given there are over 176,000 vulnerabilities identified in the United States (US) government's National Vulnerability Database (NVD) Common Vulnerabilities and Exposures (CVE) system and it is growing by over 20,000 annually, it is not surprising that patching of vulnerabilities is difficult.

Endpoint avenues of attack are not limited to software vulnerabilities but are also made possible by misconfigurations. Analyst firm ESG has reported that endpoint misconfigurations — covering such items as incorrectly applied privileges, browser settings, open ports, and active un-needed services — are the entry point in a fourth of all endpoint compromises.

The bottom line is that securing the enterprise against attacks, especially those targeting endpoints, is hard. Cybersecurity professionals work at protecting the environment and this requires a holistic security framework aimed at closing all attack paths.

Zero Trust

Protecting the IT infrastructure has been a concern from the beginning. Cybersecurity philosophy, tactics, and capabilities grow with technology changes and attacker capabilities. Studying and understanding the ways an environment can be breached leads to the development of defensive strategy models.

The Zero Trust security model has emerged as the process of choice for a wide swath of the community. Depending on the survey, between 60 to 80% of organizations are involved in some type of Zero Trust project. Executive Order 14028 Improving the Nation's Cybersecurity commits the US federal government to a Zero Trust approach to cybersecurity.

The Origins of Zero Trust

From the beginning, IT infrastructures attempted to prevent unwanted intrusions using a strong, well-defined, and protected perimeter. Activities occurring behind the gates are assumed to be trusted. It was thought this encouraged productivity.

This castle model is possible with limited entry points and all devices and operations occurring behind the hard outer shell. The obvious drawback is once the perimeter is breached, unauthorized attackers or malicious insiders have unfettered access to resources and few restrictions on the actions they perform. It is recognized that additional controls are necessary.

In the early 2000s, security managers and professionals formed an organization called the Jericho Forum which promoted the de-perimeterization of the network. They advocated for the protection of assets (primarily data) where they reside and as they flow within and between enterprise network boundaries and components.

A number of years later, Forrester Research analyst John Kindervag crystallized the de-perimeterization security model in a paper entitled "*No More Chewy Centers: Introducing the Zero Trust Model of Information Security*" (2009). This essay advocated a concept that assumed all network activities should be considered as untrusted until "it is verified that the traffic is authorized, inspected, and secured." In his Zero Trust model it is assumed that unauthorized actors exist within the organization's network.

Initially, Zero Trust was an item of discussion and investigation but high-profile breaches, a growing belief in "assume breach", and the explosion of software-as-a-service (SaaS) deployments forced cybersecurity professionals to consider new security paradigms.

The Zero Trust Mindset

Security leaders understand the days of the hard outer shell are long gone. A new, different, and proactive security strategy able to adapt quickly to changes in IT is required. Many have come to the belief that Zero Trust provides a comprehensive concept that can manage cyber risks for a distributed architecture powered by the cloud, mobile devices, and SaaS.

The Zero Trust mindset supplements the gates and guard philosophy with one where each individual asset (user, application, and device) is considered untrusted so they must be constantly checked to verify trust. The consensus is that by controlling access by users and devices it is possible to contain threats while maintaining business operations.

"Zero Trust is the world's cybersecurity strategy."

John Kindervag

To address the Zero Trust mindset requires adoption of the mantra "assume breach, never trust, always verify". The top-line actions associated with these principles can be summed up as:

- **Continuous verification**: All resource requests must be authorized, authenticated, and secured. Trust is not implied but must be validated each time.
- **Least privilege enforcement**: Access is restricted to the minimum level required. This limits the attack surface and makes it difficult to access resources not explicitly authorized.
- **Constant vigilance**: The IT environment must be continuously inspected, logged, and analyzed in order to discover strange behavior and actions. Quick detection allows for swift remediation, thus limiting the window of opportunity for attackers.

Accepting the Zero Trust concept that assumes attackers exist within the network does not require the wholesale replacement of the existing security fixtures. Instead, it leverages existing security investments in ways that support a Zero Trust strategy. What is required is the development of new processes and workflows, thus allowing those foundational security elements to support Zero Trust goals.

Moving to a Zero Trust Architecture

Chief Information Security Officers (CISOs) and security professionals have bought into the Zero Trust concept. However, deciding you are going to follow a strategy doesn't make it happen. It takes work to implement a functioning Zero Trust architecture that balances business needs with security demands.

Deciding to adopt Zero Trust is the beginning of a long journey. It isn't possible to sprinkle magic dust on the existing environment to incorporate Zero Trust requirements. The good news is this journey does not require the scrapping of existing security components and controls. Instead, the Zero Trust architecture leverages existing solutions to allow for a consistent progression that is less painful and costly.

Design It

A Zero Trust architecture must be applied across the complete infrastructure. The Zero Trust philosophy changes the focus from assumed trust to verified trust.

This does not require the wholesale replacement of the existing security fixtures. There may be a need to supplement the infrastructure with Zero Trust optimized components but, in most cases, the existing products remain valuable tools within a Zero Trust framework.

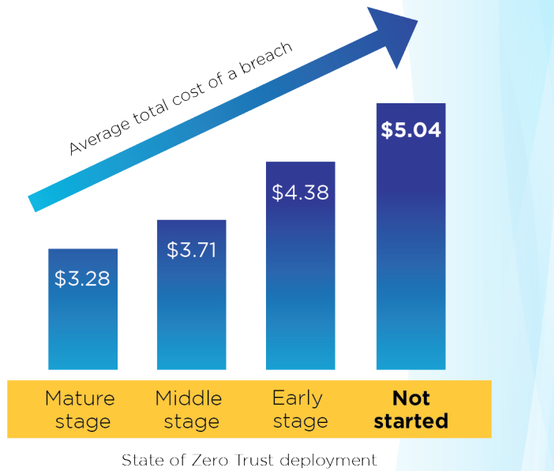
Implementation Journey

Transitioning to a Zero Trust architecture is non-trivial and it will take time, possibly years. How this is accomplished will be based on particulars associated with each organization.

Various paths can ultimately result in a successful Zero Trust architecture, but:

1. Is there an optimal route towards Zero Trust?

2. What specific steps should be taken when building a Zero Trust architecture?



State of Zero Trust deployment

Source: IBM's Cost of a Data Breach Report 2021

The first step is to change the organization's strategy and culture around cybersecurity. The next step is to look at frameworks and recommendations from others on building a Zero Trust architecture. Advice on how organizations should proceed is widespread.

Many experts and entities offer guidance on how to transform from a perimeter stratagem to Zero Trust. The most unbiased and comprehensive information is available from the US government (NIST, CISA, NSA, and DoD).

This guidance provides considerable detail about nearly every component of a Zero Trust architecture, but there are a number of recommendations and themes articulated across multiple documents.

How to Implement Zero Trust in Your Environment

- **Create a Road Map**: Implementing Zero Trust must be methodically planned out using a continually maturing roadmap. All aspects of the business, operations, and security considerations must be part of the plan. A defined plan focuses on the most pressing needs and most practical solutions. Transitioning to Zero Trust will take time so efforts should not be rushed.

- **Architect from the Inside Out**: Historically, security initiatives focused on looking at threats from the outside to design security controls. In Zero Trust, you first start by looking at the inside. Focus on protecting the data, assets, applications and services contained within the environment. Strive to protect them first, then tackle the paths to assess them. The inside out approach is why Zero Trust begins by identifying critical components and ensuring that only authenticated and authorized users, devices, and systems can access them.

- **Take a Holistic Approach**: The fragmented approach to cybersecurity technologies has made it difficult for solutions to work well together and has led to excessive technical complexity. In a Zero Trust architecture, all components of the security stack need to support each other. Do not focus too much on identity or network components without also considering how endpoint and data protection offerings can work in tandem to achieve a much deeper level of defense-in-depth.

Granting access to an endpoint isn't solely dependent on an identity check — compliance to a security policy must also be demonstrated.

- **Produce Consistent Policy**: To deliver trust on the network, the security policy must be consistently applied across environments. Too many times waivers or exceptions to the rules are made for short-term operational needs, thus leading to vulnerabilities.

For maximum effectiveness, no communication between enterprise resources occurs unless it is approved under policy.

- **Expand Visibility**: Zero Trust relies on having knowledge of what exists within the environment. **To assign trust it is critical that an inventory of all assets (applications, devices, and systems) be created and maintained.** Visibility on workflows is also essential. Visibility into the inter-working of the environment allows for intelligent response to changes and allows for the observation of threats. **Continuous monitoring and reporting within a Zero Trust enabled infrastructure is also critical to effective incident response.**

- **Orchestration and Automation**: **A Zero Trust architecture is only going to be made possible with automated security monitoring and enforcement that immediately responds to policy-based controls.** An example is isolating and remediating an endpoint that is out of compliance. Systems must be able to automatically share policy-based decisions. Automating processes by the incorporation of security orchestration, automation, and response (SOAR) results in coordinated, instantaneous responses to threats.

> Security orchestration, automation and response tools enable organizations that have an appropriate level of preparation in their security operations processes to increase efficiency and consistency. Security and risk management leaders must prepare adequately to ensure value from such tools.
>
> *Gartner, 2022*

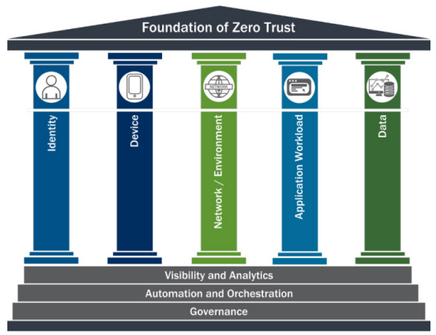
Irrespective of the path organizations take towards realizing Zero Trust, they need to avoid the trap of viewing Zero Trust as a zero-sum game. Zero Trust is a web of connected policies, practices, software, and hardware that create a Zero Trust ecosystem. However, it can and will coexist with other security models.

It is expected that most organizations will operate in a hybrid security environment. Zero Trust does not eliminate the need for layered defenses, such as endpoint security and vulnerability management. It improves on the layered security approach by encouraging greater integration and visibility among security components in order to offer better protection from threats.

Zero Trust Maturity Model

Maturity models are widely used. They provide a metric for organizations to measure how well they are performing and improving. This measurement tool, usually manifested in scales, describes the set of capabilities required for a specific maturity level.

For Zero Trust, the Cybersecurity and Infrastructure Security Agency (CISA) has published a maturity model. In keeping with the understanding that Zero Trust is a comprehensive security model encompassing the total environment, their Zero Trust Maturity Model has five pillars. These include Identity, Device, Network, Application Workload, and Data. Running across all of the columns is Visibility and Analytics, Automation and Orchestration, and Governance.



CISA Zero Trust Maturity Model June 2021

As organizations become more mature they will increasingly rely on automated processes and systems which improve integration across the pillars.

How Zero Trust & Endpoint Security are Compatible

The Zero Trust concept initially was concerned with deeper control of network traffic and access and the verification of identities. However, it was quickly realized that the endpoint has an equal, or arguably a greater, impact on Zero Trust than any other asset. Enterprises realize the need to improve endpoint security in order to support Zero Trust initiatives.

The Zero Trust assumption is that everything is assumed to be breached, so it's required for endpoints to explicitly prove otherwise for the protection offered by Zero Trust to be effective. The integrity of the endpoint must be constantly verified because once compromised an attacker has the opportunity to sidestep authentication controls.

Integrating endpoint security fully into the Zero Trust ecosystem provides the means to identify, monitor, isolate, secure, control, and remove any endpoint from the network at any time. The endpoint Zero Trust components begin with an inventory of devices.

Following discovery requires assessment of the endpoint's security posture against policy, accepting or denying access based on this assessment, bringing denied devices into compliance, ensuring endpoints are protected, and providing detailed information to the analytics and orchestration layer. The devices must be continuously re-assessed for vulnerabilities and indicators of compromise while on the network and with each access request.

Fully incorporating endpoint security and visibility into the Zero Trust architecture places trust verification as close to the user as possible. In Zero Trust, both the user and the endpoint must be assessed as trusted for authentication to be validated.

Endpoints are not just a source of trust verification information.

They are effective Zero Trust policy enforcement points.

This works by requiring users to respond to authentication requests on a specific device that meets access policy requirements. Endpoints are not just a source of trust verification information but also become effective Zero Trust policy enforcement points.

Endpoint support for Zero Trust leverages existing endpoint monitoring, protection, and risk mitigation solutions by adding Zero Trust capabilities, especially coordination with identity and SOAR components. The various US government guidance documents call out the need to use security products such as Endpoint Detection and Response (EDR), Mobile Device Management (MDM), and Unified Endpoint Management (UEM).

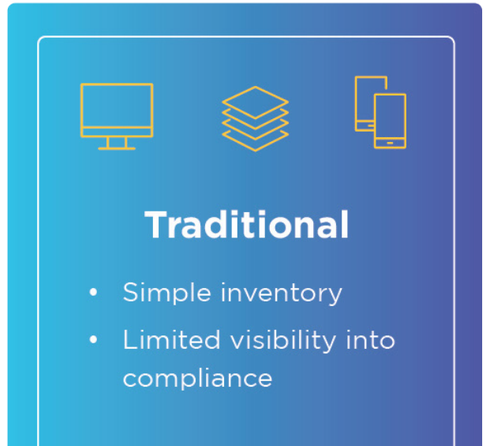
EDR is important because it scans endpoints, identifies threats, and takes appropriate action to protect the endpoint. The DoD document

specifically calls out the need to enforce patching and configuration hardening and these need to be continuously updated. The UEM component is used for centralized management of the compliance verification status of multiple endpoints.

Finally, supporting visibility, analytics, automation, and orchestration requires all actions to be logged, analyzed using an analytics engine, and deployed via a SOAR to provide real-time policy access decisions.

All of these capabilities and components are reiterated in maturity models. The CISA Zero Trust Maturity Model illustrates the maturity status for devices. As can be seen, optimal maturity is measured as "constant device security monitor and validation" and "data access depends on real-time risk analytics".

Zero Trust can be a true end-to-end security solution when organizations commit to ensuring their endpoints are continuously trusted. It is an old cliché, but security it only as strong as its weakest link. This applies to Zero Trust, but by having solutions work tightly together, including strong endpoint protection mechanisms, the risks are greatly reduced.



The Urgency to “Shift-Left”

The term “shift-left” has been adopted by the software industry to indicate they are working to remove flaws during development. There is another way of looking at shift-left. The term is an out shoot of being on the left or right of the “boom” or event.

Many security technologies are designed to stop an event at boom stage. Activities on the right of the incident are designed to respond post-attack to figure out how it happened in order to prevent it from happening again. To the left of the activity are tools and processes designed to prevent the incident from being possible in the first place.

The original shift-left is proactively taking actions to stop an attack well before it progresses by reducing vulnerabilities, limiting the time of exposure, and reducing the attack surface.

Endpoints are the destination, so it is critical to deal with configuration and software vulnerabilities by discovering and remediating those vulnerabilities as quickly as possible. Closing the avenue of attack well before an attacker can utilize it is the ultimate preventive mechanism.

Zero Trust in many cases can be considered as a shift-left mechanism. Verifying trust by the policy enforcement of identities, devices, applications, and connections is a proactive activity designed to prevent attackers from gaining a position which allows them to execute a breach.

Zero Trust With Syxsense

The vision for Zero Trust is to interlace endpoint, network, data, and identity into a comprehensive cybersecurity strategy. Each element has control over its specific domain but shares some responsibilities to make it harder for attackers to by-pass any singular component.

The complete Zero Trust cybersecurity architecture is held together by expanding visibility, automation, and orchestration. In theory, the interconnections between elements will simplify overall management and lead to improved threat mitigation.

To make this work requires utilizing products that already handle multiple workloads and can seamlessly support Zero Trust enabled capabilities by quickly reducing an attacker’s window of opportunity and integrating with a SOAR solution that allows full visibility and enforcement. For the device security, control, and management component of a Zero Trust architecture, organizations should look to Syxsense, a leader in Unified Security and Endpoint Management (USEM).

Unified Security and Endpoint Management (USEM)

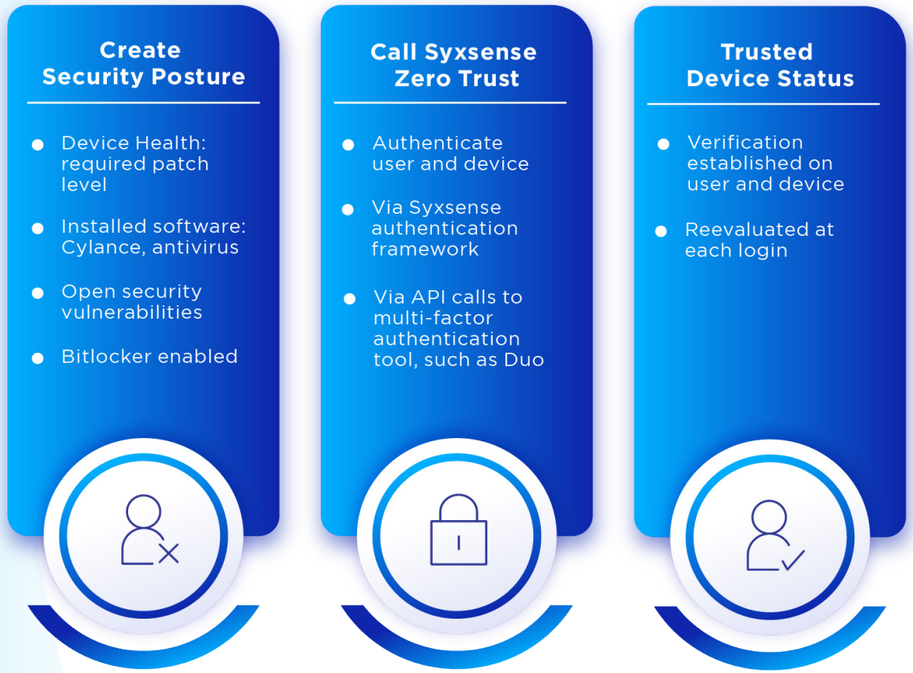
USEM enables organizations to manage, detect, and secure all endpoints across a network. This consolidation reduces an organization’s exposure to threats by scanning all the endpoints for threats, alerting and facilitating for any patching needs, enabling devices to be easily quarantined, and ensuring compliance is documented.

The consolidation of tools and streamlined workflows coupled with SOAR capability supports a Zero Trust architecture by allowing teams to remediate and fix issues in real-time.

How Syxsense Supports Zero Trust

Drawing on its leading USEM capabilities, Syxsense Enterprise takes a practical and proactive approach to broadening endpoint security with the Zero Trust approach. The solution ensures secure access to critical infrastructure through the consistent discovery, monitoring, and management of the security posture of each endpoint on the network, quarantine of out of compliance devices, and automatic remediation of vulnerabilities.

The Syxsense Cortex™ workflow automation engine works in collaboration with the Syxsense Zero Trust Evaluation Engine to establish a device's identity, health, and compliance status and bring devices into trusted status before allowing network access.



Syxsense Zero Trust Evaluation Engine

The Syxsense Zero Trust Evaluation Engine offers unparalleled visibility and control over network access policies and enables security teams to build sophisticated access policies and remediation workflows to ensure Zero Trust Network Access (ZTNA) compliance.

With the ability to evaluate endpoint access for ZTNA based on policies and to block and apply fixes for non-compliant endpoints, Syxsense Zero Trust allows organizations to have full control of endpoints through an automated end-to-end process.

The power of Syxsense Zero Trust lies in three key areas:

1. The granularity of hundreds of parameters IT can use to report and act on device compliance, such as IP address, location, anti-virus status, hours of operation, and many more, and the ability to block devices that are out of compliance from accessing the network and corporate resources.
2. The ability to enforce compliance with Zero Trust policies prior to granting access on an asset-by-asset basis.
3. The ability to automatically remediate non-compliant endpoints, including patching the system, enabling an anti-virus tool, emailing IT about unauthorized access, and more.

Final Comments

Zero Trust changes the cybersecurity mindset from intrinsic trust to verified trust. Constant vigilance is required to combat attackers who patiently and methodically infiltrate enterprise environments.

The need for Zero Trust has accelerated with the exponential growth of cloud, mobile devices, and SaaS applications. Zero Trust is all about the interweaving of multiple security disciplines into a comprehensive solution which fosters business transformation while expanding overall protection.

Zero Trust doesn't change the cybersecurity rules, but clarifies the rules. Nothing associated with Zero Trust is revolutionary. The holistic application of the components (network, identity, endpoint, workload, data) creates the strong security framework.

Endpoints are the ultimate destination for attackers. From there, they infiltrate networks and exfiltrate data. Endpoints bear some or all responsibility for their own security, but in a Zero Trust environment, the security status of endpoints is shared across the environment to improve security enforcement.

To make this endpoint security functionality work requires a security solution that offers a wide range of functionality, but that also integrates with the other Zero Trust components via the Visibility and Analytics, Automation and Orchestration, and Governance layers of the Zero Trust Maturity Model.

Syxsense offers a complete USEM solution with a Zero Trust approach to real-time vulnerability monitoring, detection, and intelligent automation for IT management, patch management and security remediation in a single console.

Organizations looking to improve their overall device security, control, and management now and as part of a Zero Trust architecture should turn to Syxsense.

SYXSENSE®

www.syxsense.com