Technical Manager’s Guide- Devices Insights

May 02, 2023

Cybersecurity Research Analyst

Alex is a cyber security research analyst at Stratascale. His background in both research and practical security gives him a unique perspective on providing security with a risk-based approach. He focuses his expertise on emerging technologies, data-driven IT strategy, and tactical solutions to large security problems.

Submitted by Alex Banghart on 2, May 2023
Technical Manager’s Guide- Devices Insights

Zero trust (ZT) is an approach to cybersecurity that aligns capabilities across an organization around the defense of key assets. ZT is structured in six “pillars” — identity, devices, network, infrastructure, applications, and data. Each pillar’s security team needs to both establish ZT capabilities within their area and work effectively with other pillars to support ZT strategic objectives throughout the enterprise.

For managers responsible for device security within an organization committed to ZT (“ZT devices”), addressing both device-specific and business-wide ZT objectives is a complex endeavor. CISOs will look to ensure that ZT devices fully support organizational objectives, while ZT device and asset managers will look to use the ZT capability framework to organize and prioritize their investments and activities. ZT device managers must execute on:

- Establishing devices as a baseline for ZT.
- Facilitating relationships between internal, BYOD, and third-party devices.

- Adapting to OTwith agility.
- Operationalizing data-driven security models.
- Establishing and maintaining a device inventory.
- Understanding and reacting to business priorities.
- Ensuring real-time device visibility.
- Aligning technical controls with regulatory and compliance demands.

ZT device managers will encounter roadblocks such as:

- New remote work realities.
- Increasing pace of change in business demands.
- Shadow IT.
- Lack of standardization in device onboarding and offboarding.
- Increasing number of ephemeral devices.

Devices as a baseline for ZT

In the modern world, it’s increasingly important to prioritize the security of devices connected to networks. This is known as a "zero trust" approach, which means that we must not only trust the person accessing the network but also the device they are using. In the past, it was common to assume that a device was secure simply because it belonged to a trusted individual, such as “Joe Smith.” However, this is no longer the case — attackers can use various techniques, such as rootkits and remote access Trojans, to gain access to networks through compromised devices.

Here are some common attacks that a compromised device could execute even with a valid user:

- Eavesdropping: collecting user data when a valid user operates the device, such as usernames, passwords, and account numbers.
- Malicious applications: leading the user to install software that can take over the device or cause harm to the network.
- DDoS zombie: using device resources to execute DDoS attacks on behalf of the hacker.
- Data exfiltration: sending out copies of data to an outside source as the user operates the device.

To effectively implement a zero trust framework, it’s necessary to consider various factors related to the device being used to access the network. This includes

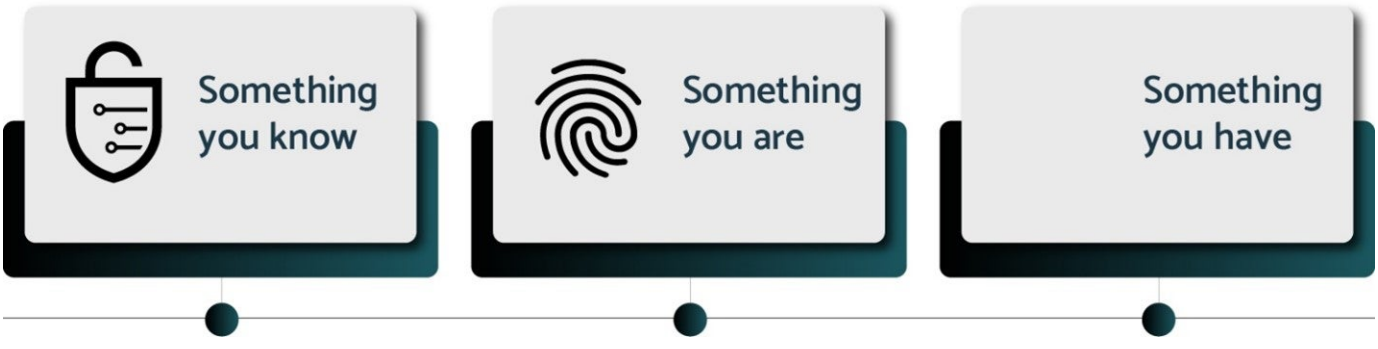
understanding the profile of the device, such as whether it’s a company-owned or personal device. It’s also important to know the device’s physical location and to keep track of its current state of patching. Having an inventory of all devices connected to the network and ensuring that they meet certain security standards is essential in maintaining the security of the network as a whole.

Devices beings used for MFA

In today's digital landscape, it’s essential to prioritize the security of devices that are used to access networks. This means going beyond simply relying on user authentication, such as a username and password, and instead implementing multi-factor authentication (MFA). MFA involves using an authorized device, such as a phone or computer, in conjunction with other forms of authentication, such as a code sent via text or email, to verify the identity of the user. Devices are the method of implementing MFA through authentication applications, yet accessing the devices themselves also requires MFA methods.

The challenge lies in maintaining the security of these authorized devices and authenticating them when a user switches from one device to another. This requires implementing a system for maintaining an inventory of devices and ensuring that they’re properly registered and verified.

In industries such as banking, it’s common to see MFA implemented, with users required to register their devices and undergo MFA the first time they log in. This may involve text or email verification and some form of device registration, such as through a cookie, Mac address, or IP address. Successful MFA programs involve a combination of something you know (like a password or pattern), something you are (thumbprint, IP address), and something you have (phone, laptop, physical access token, cookie).



A successful MFA plan requires a successful device strategy, because the most effective forms of MFA — biometrics and location data — are provided by mobile phones. The ability to utilize powerful authentication technologies on a mobile device or through physical access tokens such as a YUBI key allows for robust and simple verification.

The importance of implementing MFA and properly authenticating and verifying devices cannot be overstated. With threats from cybercriminals constantly present, it’s necessary to adopt a "zero trust" mentality and always verify the security of devices being used to access networks. The old adage of “trust but verify’ has been updated to “don’t trust anything; always verify.” By taking this approach, we can better protect ourselves and our networks from potential threats.

Device Posture and Device Posture Checks

Because compromised devices can serve as an attack vector against other resources, a zero trust strategy includes a Device Posture Check (DPC) as part of access decisions. This DPC evaluates the device’s current state and potential vulnerabilities. To support a zero trust strategy, device managers would define the elements of the device’s posture to be evaluated in the DPC. For example, DPC elements might include:

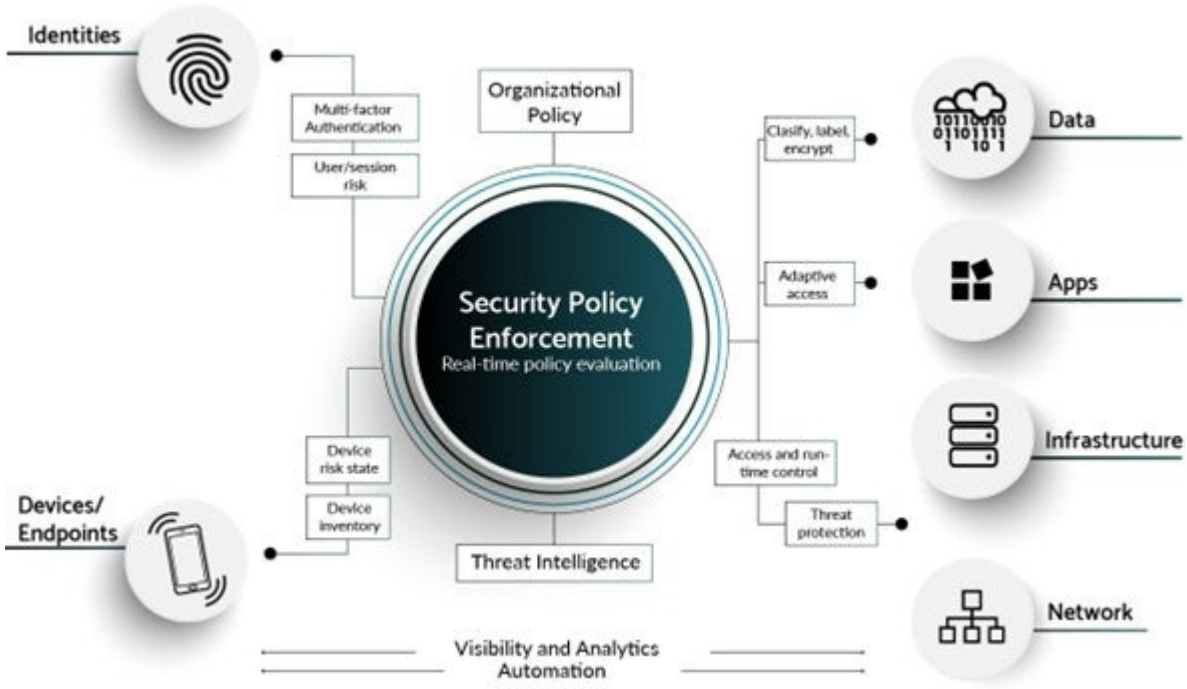
- OS version.
- Anti-malware version and status.
- Screen lock status.
- Firewall status.
- Storage encryption.
- Biometrics.
- Certificates.
- Device name and ID.
- Management software client version.
- Patch status.
- Last update time.
- Installation of specific applications.

This process of earning trust by evaluating device posture is important for all types of devices, whether corporate, personal, or owned by third parties or contractors. It’s also relevant for servers and internet of things (IoT) devices, which may have

specific purposes such as acquiring telemetry data from patients in the healthcare industry.

It’s important to ensure that both the device and the user accessing it are not compromised in any way that could put sensitive data at risk. This includes protecting the data and limiting access to only those who have a “need to know.” One way to achieve this is through device registration — storing the device fingerprint of the user in a risk-based access database. The device fingerprint contains information required for calculating a risk score, which helps to establish controls and limit the “blast radius” of potential threats such as ransomware.

Device posture supports more effective decisions for continually evaluating access, because devices provide more signals and telemetry. The decision on whether to grant access no longer hinges entirely on identity — the DPC provides a key level of input to your policy enforcement point in order to make access decisions, as shown in the following diagram:



Source: https://www.microsoft.com/en-us/security/business/zero-trust

By requiring device registration and limiting access to data on a need-to-know basis, we can better protect sensitive information and reduce the risk of data breaches.

Investment Drivers for Devices

The rise of Operational Technology

As technology has advanced, there has been a shift toward streamlining and automating processes, particularly in the convergence of operational technology (OT) and information technology (IT). This merger has resulted in a proliferation of devices that are used to access networks and perform a variety of tasks. While these devices can be incredibly useful in increasing efficiency and cost-effectiveness, they also present a significant security challenge.

In the past, OT was typically separate from the main network, preventing it from being exposed to many common threats. Today, the rise in data/analytics requirements has led many organizations to connect OT devices to their main networks. These connections provide value to the business, but with increased risk comes the need for more controls.

The security concerns for OT devices include:

1. Legacy applications.
2. Default configurations.
3. Missing encryption.
4. Poor or missing policies and procedures.
5. Legacy remote access.
6. DDoS attacks.
7. XSS attacks.
8. SQL injection.
9. Malware.
10. Parameter manipulation.

To secure OT devices, managers must consider the unique challenges of concern to OT devices as well as ensure that these devices are folded into the network in a way that keeps them secure and updated with all the other devices on the network.

Network Segmentation

Network segmentation no longer provides the level of protection it once did, because users’ devices can bridge the gap between networks. Consequently, the device manager plays a crucial role in securing the enterprises’ assets under the zero trust paradigm.

Traditionally, organizations have relied on network segmentation as a way of protecting their assets against threats. For example, a hospital might have the main network and a guest wi-fi network. The hospital's main network may be heavily restricted while the guest network allows for greater access, such as for streaming on Netflix or Facebook.

In these cases, it's common for employees to connect to the guest network using their corporate devices in order to access prohibited content or activities. This could easily lead to a corporate device becoming compromised with something like ransomware, which could then spread to other devices on the main network.

The solution to this problem is to place controls on the endpoints themselves. For example, device teams can lock down endpoints by detecting and preventing prohibited activities and/or requiring endpoints to use agents to connect to resources through a secure access service edge (SASE) platform.

When allowing remote access to the network through devices such as personal computers, security teams should limit access as much as possible and segment the network appropriately through the use of access control lists.

Security teams may encounter pushback from end users, but additional controls at the device level are usually the only practical way of addressing the risk to the organization's assets. "Segment it and forget it" may have worked in the old days of wired connections and air-gapping, but in the modern world the sprawl of devices and the ability of devices to connect to multiple networks have rendered that approach woefully inadequate to address today's threats.

Key Zero Trust Device Priorities

Establish an inventory

Developing a device inventory is an essential step in implementing a zero trust model. Without a thorough inventory of all devices, it's impossible to accurately track and monitor them or identify rogue devices, which can lead to security vulnerabilities. To quote a contributor: "[Inventory] is number one. If I don't have that, then what am I doing? Why am I doing zero trust if I don't have my hands around my devices at some point? If I'm going to do anything with devices, I better have a construct where I've got these devices tracked, flagged, fingerprinted, and

something to pull that stuff into. Otherwise, I'm going to 20 different sources, and I can't build a consistent policy or consistent anything around them."

In the past, it was all too common for IT teams to track devices manually using spreadsheets. Today, device tracking must be fully automated, including scanning and monitoring to update a single source of truth. Generating rules-based alerts for security operations teams should also be automated.

The modern-day device inventory for enabling zero trust security moves beyond traditional asset management because it needs to include many devices that the enterprise doesn't own. BYOD devices and devices owned by third-party contractors can pose just as much of a threat as any corporate-owned device. Today's security teams must establish a fully automated device inventory for **all** endpoints, including non-traditional devices such as sensors, cameras, and other IoT or OT devices.

Assess business needs and develop policies as a living document

The cybersecurity strategy that drives device policies changes with evolving technology and the threat landscape but also with the needs of the business.

Fundamentally, business requirements drive how users and applications function and determine which users and applications need access to which data and services. And while it's easy to automate technical things like the device inventory, it's impossible to automate updates with a full understanding of the business context and end users' needs and requirements.

To effectively support a zero trust program, device managers must implement regular touchpoints with business and application stakeholders to ensure that the policies and controls reflect the needs of the business logic. Technical configurations and policies need to be flexible and adaptable, using something like a "policy as code" approach, so that ZT devices' teams can quickly and easily modify functionality to accommodate changing business needs.

Ensure device access control

A zero trust approach requires not only that access be based on continuous DPC, but also that controls be established to limit the ways in which endpoints can access

services and data. Zero trust device managers have a number of different technologies and architectures at their disposal for implementing these kinds of controls:

- Installing DLP agents on devices.
- Implementing access controls through CASB.
- Implementing access through SASE.

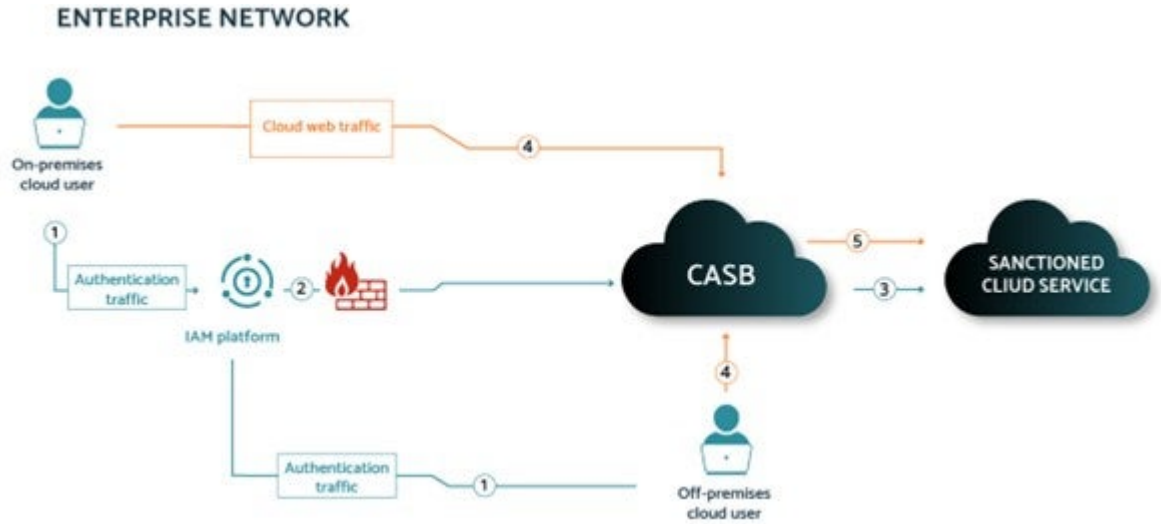
These approaches may be seen as equivalent alternatives, but they’re not. Each of these technologies and architectures have distinct technical requirements and advantages and disadvantages. ZT devices’ managers must work with several stakeholders to determine the best technologies to deploy for establishing the controls the business needs. In some cases, they may prefer to use a combination of technologies for different endpoints and/or use cases.

DLP

Through the agent, you can force users through specific gateways or only provide the device access to things based on device posture or the specific network. DLP also supports establishing processes for monitoring and responding to any potential data breaches, including notification and remediation procedures.

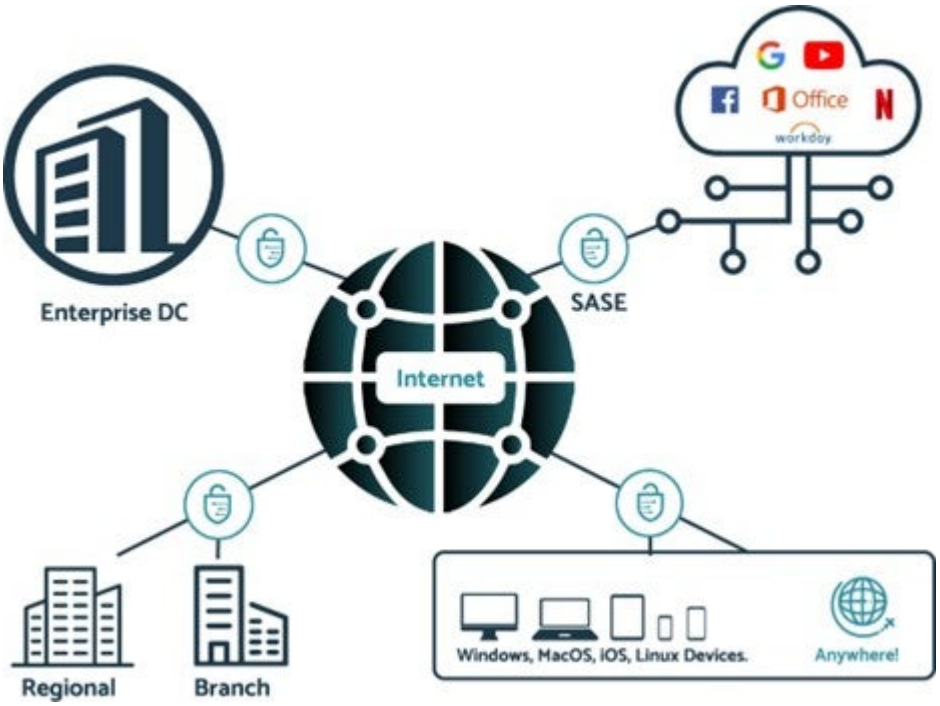
CASB

Deploying a CASB ensures that devices have to connect to your IAM platform regardless of their current posture before accessing secure SaaS or cloud services. Following is a sample of what that architecture looks like at a high level.



SASE

SASE deployments focus on ensuring that network traffic going to on-premise, cloud, and SaaS corporate locations are secured. This allows for other network traffic to flow freely. SASE deployments typically look like the architecture shown below:



Your DLP agent also needs the ability to quickly restrict the types of activities on the device based on the posture and current state of the device. It needs to be context-aware and have some form of DLP enforcement on corporate devices or personal devices. Developing a policy about what data can be accessed and how to force access through specific gateways based on device posture is an important step to establishing a ZT posture.

The ability to look into devices and deliver context continuously is important. You also don’t want to trust devices simply because they’ve been trusted before. Continuously understanding and having visibility into devices allows you to avoid potential scenarios where breaches can happen.

Overall, establishing a DLP program is a critical step in protecting sensitive data and maintaining the integrity of corporate systems. By identifying the data that needs protection, understanding how it’s being accessed, and implementing appropriate controls, organizations can effectively mitigate the risk of data loss and maintain the trust of their customers and stakeholders.

Ensure Device Visibility

“I have to think about the devices continually,” a contributor explained. “I need to do some continual evaluation of the posture.”

A contributor explains a potential scenario where an organization relies on a point-in-time assessment of a device’s posture rather than continuous assessment: “The user’s phone? It’s good. We’re letting it in to go access the data. But now it’s got a rootkit on it that I picked up 20 minutes ago — my posture’s changed and [you won’t] evaluate that until five days later because it’s inconvenient. I can’t let convenience interfere with security sometimes.” When organizations monitor devices for their status and their context through comprehensive visibility and analytics, they can ensure that devices are secured based on current data-driven context rather than static policies. The latter will always lag behind rapidly advancing threats and threat actors.

Roadmap to ZT Devices

Each document in the Technical Manager’s Guide to Zero Trust series incorporates a roadmap providing practical guidance to readers looking to implement ZT within their areas. To establish a ZT devices roadmap, our contributors recommend being able to answer the following questions in this section:

- Are your policies and priorities aligned with current business needs?
- Do security practices align consistently with these policies?

Addressing these questions means considering the current state of the business, including the remote workforce, threat landscape, and technology infrastructure. ZT device managers are not doing enough if they simply review and update policies annually based on compliance requirements; they should take a wider focus to ensure that they consider all relevant factors.

Taking this wider focus may lead ZT device managers to re-evaluate the way the business operates as well as the technologies it uses when determining how to effectively implement and enforce policies in these areas. A holistic approach to cyber security policy development enables the organization to better protect itself against threats and ensure the continued success of its business.

- Do you have visibility into all devices
- Can you onboard and offboard new devices?

ZT device managers need to establish a process flow and classification system for the various devices and for how those devices interact with each other. Some questions to ask yourself when setting up a device onboarding plan are:

- How is the device enrolled in inventory?
- Who is adding the new device?
- How is the device tracked and monitored?
- How is the device maintained?
- How does the device gain access to the networks?
- How do you perform DPC for the device?
- How do you offboard the device?
- What personas are connecting it to the network?
- Who owns this device?

Our contributors all agreed on the need to deal with onboarding all devices, even “ephemeral” devices. A contributor described these as “machines, servers, resources that come up and down.” Device managers need to understand these devices and make sure all devices are registered, even in test environments or temporary containers. These should be included in your management process.

Contributors specifically mentioned having a comprehensive offboarding plan for retiring devices, to help combat “device sprawl.” Understand when and how to dispose of the physical device as well as any access privileges that device had. Then, update your inventory to make sure that any interconnections don’t break — for example, a specific system may require input from this device.

- Do you have a tight connection between devices and data?
- How are you ensuring that devices/endpoints can access data while keeping that data off the device?

As part of the normal course of business, users must be able to access data through devices. But if data gets transferred to those endpoints, it becomes much more difficult to secure that data. Even if the data is encrypted at rest on the endpoint, there’s no way to ensure that the user didn’t etch their password on the bottom of their laptop. A good device manager realizes that “the best device security is keeping data off the device,” as one of our contributors pointed out.

An effective ZT device strategy will ensure that even if an attacker compromises the device, they won’t be able to touch the data.

- Can you ensure that protections and corporate policies evolve with changing requirements and the threat landscape?

While many organizations may have a policy in place that states they will review their policies annually, this approach often doesn’t include all the factors that need to be considered in order to effectively protect an organization’s assets.

One of the primary challenges organizations face is keeping up with new regulations and compliance requirements. For example, new PCI or HIPAA rules may have been introduced that require updates to existing policies. However, organizations must also consider broader factors such as changes in the threat landscape, including new types of cyberattacks like ransomware, and changes in the way business is conducted, such as an increase in remote work.

Another important consideration is the impact of technological advancements and changes in infrastructure, such as the shift to cloud computing. Organizations must ensure that their policies and procedures can be effectively implemented and enforced in these new technologies and environments.

Another challenge organizations face is that when they do update their policies they may not take into account all the inputs and factors that should inform those policies. For example, they may not consider the latest cyber security threats or how IT and OT are changing their operations. In addition, they may not consider how the organization is conducting business while its workforce is working and how technology changes within the infrastructure.

Your program should be reviewed regularly — at least annually. However, Stratascale also suggests to review policy in these situations:

1. Major organizational changes in leadership.
2. Any change to law or regulations.
3. Major incident or policy violation, both internally and externally.
4. Major technology changes, such as deploying new forms of devices.
5. Before any merger and acquisition activity.

To address these challenges, organizations need to ensure that they're reviewing and updating their policies regularly (annually at minimum), and that those updates take into consideration a broader spectrum of inputs. This includes not just regulations and compliance, but also best practices from a NIST cybersecurity framework as well as how the organization is conducting business and the technology changes within the infrastructure.

- Are you emphasizing the current monitoring of devices and policy as part of this zero trust device approach?

Current state monitoring is important to ensure that issues with devices are detected as soon as possible. Constant monitoring of devices provides the following benefits:

- Detecting incidents earlier.
- Setting performance benchmarks.
- Setting cost expectations.
- Enabling managers to be proactive.
- Detecting misconfigurations.
- Detecting unauthorized logons.

When a device is compromised, it's important to have a plan of action for responding swiftly and with minimal disruptions to the business as a whole. It's important to be able to segregate devices from the network to help limit the blast radius of any attacks.

In case of a device breach, any plan should also cover the following:

- What is happening to the data — is it being encrypted, deleted, exfiltrated?
- What is the plan for conditional or adaptive access?
- What to do with the compromised device?

Roadblocks and Challenges

Implementing a zero trust model for devices can present organizations with several roadblocks. One of the main challenges is the speed of business and the constant influx of new devices and services coming online. With the move toward a more ephemeral state of devices, where servers, laptops, and other devices are brought up and taken down regularly, it can be difficult to keep an accurate inventory and

maintain an up-to-date record of all devices on the network.

Another roadblock is the proliferation of shadow IT, where users or lines of business may bring new devices and services online without informing IT or going through the proper channels. This can lead to a lack of visibility and control over these devices, making it difficult to enroll, track, and monitor them.

To effectively implement a zero trust model for devices, organizations need to take a holistic approach that is structured to overcome these roadblocks. This includes regularly reviewing and updating policies and procedures, standardizing the way that new devices and services are brought online, and implementing a robust device management system that can accurately track and monitor all devices on the network. Additionally, it’s essential for organizations to address the rising shadow IT and ensure that all devices are brought online and managed through the proper channels.

ZT Device Metrics

As part of its zero trust research program, the Stratascale team has developed the Stratascale Zero Trust Metrics in Context and Action (Stratascale ZT-MICA) tool. Its robust, embedded set of metrics combine to provide strategic insights to executives, operational perspectives to IT and security management, and tactical data to managers responsible for ZT within each of the six pillars mentioned above.

The metrics contained within Stratascale ZT-MICA for ZT Device include:

# of corporate devices integrated into Zero Trust Program

# of IoT/IOTM devices integrated into Zero Trust Program

# of BYOD devices integrated into Zero Trust Program

% of devices enrolled in MDR/XDR

% of devices utilizing certificates

% of devices enrolled in DLP

# of unpatched medium/high vulnerabilities

Collectively, these measurements help device security managers assess readiness and progress over time and identify and respond to areas of need before they're exploited.

Important ZT Devices Technologies

As part of its Executive Guide to Zero Trust research series, Stratascale published Key Zero Trust Technologies and Management Imperatives. The ZT Devices section of this report highlights the technologies that managers should understand as they plot their ZT device strategies:

Devices are a complex category in a ZT framework. Most businesspeople intuitively include corporate-issued PCs, tablets, and smartphones under the "devices" heading, but security professionals also need to consider third-party user devices—both bring your own device (BYOD) and units used by customers or supply chain partners to interact with corporate assets—as well as company-owned and third-party access points, IoT devices, and infrastructure components, such as servers, switches, and even software. In the ZT world, a device is any entity that is looking for access to resources. Each represents a potential point of vulnerability, and each needs to be wrapped in the ZT framework.

Stratascale's SMEs emphasized the need to build sound management capabilities: device inventories/device asset management, device hygiene and posture, and endpoint protection.

Device inventories/device asset management

The first step in ZT devices is to understand which devices need to be protected. "Device inventories, device asset management, unified device management (UDM), enterprise device management (EDM), IT asset management (ITAM), or whatever you want to call it"—there are multiple terms used to describe the ability to track and manage devices. Fundamentally, ZT requires that the security function be able

to identify each device that might access corporate resources and answer questions, such as:

- What user devices do we have in use today—company-owned, BYOD, and other human-controlled devices that access our network and resources?
- What IoT or other devices that are not assigned to a human user have access to our network?
- What BYOD devices are we supporting?
- Where is each of these devices?
- Which devices have we retired?
- Do we have proof that they've been destroyed?

The important thing is to be as comprehensive as possible: include both corporate and personal devices and maintain currency over time via proactive additions and deletions from the inventory/register.

Device hygiene and posture

Device hygiene refers to the ability to understand the current status of a device and whether basic security steps have been taken to protect it. The phrase covers a range of factors, including:

- Core device attributes — company-owned or personal device? Locked down or "jailbroken"?
- Status — properly patched?
- Accessing the environment via a virtual private network (VPN)?
- The ability to receive and analyze signals and telemetry that support analyzing risk associated with the device.

At a higher level, device hygiene means referencing the core attributes that comprise device compliance and risk state—ensuring that the device meets defined corporate standards and policies.

Endpoint protection

Endpoint protection goes by several names, including endpoint detection and response (EDR) and endpoint protection platform (EPP). Although some differences can be debated across these terms, the general sense of securing the device is common to each—an essential component of a ZT devices strategy.

Endpoint protection hardens connected devices against attack by connecting related capabilities:

- Predicting when an endpoint might be compromised, based on threat intelligence and pattern analysis.
- Preventing compromise, if possible.
- Detecting and responding to compromises when they occur.

These systems are often delivered via cloud-based platforms that support ubiquitous connections and real-time updates. Effective endpoint protection should connect seamlessly with other ZT pillars—for example, ZT network technologies—to enable anytime/anywhere user access while enforcing ZT access standards consistently across human-controlled and non-human devices.