SEPIO

EMBRACING A ZERO TRUST HARDWARE ACCESS SECURITY MODEL

A Sepio white paper

INTRODUCTION

The concept of Zero Trust (ZT) is primarily a security model but also a mindset. ZT is based on the idea that threat exists everywhere, both inside and outside traditional network boundaries. Essentially, anyone and anything can be a security risk.

Hence, by assuming that a breach is inevitable, ZT eliminates the automatic trust given to enterprise users and devices. Instead, users' and devices' access to an enterprise's resources is based on a dynamic policy that attempts to reduce the attack surface by providing access based on the principle-of-least-privileged (PLP).

PLP is applied for every access decision, and access is constantly under review, requiring continuous verification through real-time information from various sources that detect anomalies and suspicious activities.

ZT is a data-based security model that relies on different sources of input to make real-time access decisions. In doing so, ZT aims to increase the enterprise's security posture by improving its ability to address the existing threats. Transitioning to a ZTA is a complex process that requires planning and patience. For optimum efficacy, ZT must be included in most, if not all, aspects of the enterprise's network and have the support of the entire organization, from c-level executives to entry-level employees and everything in between.

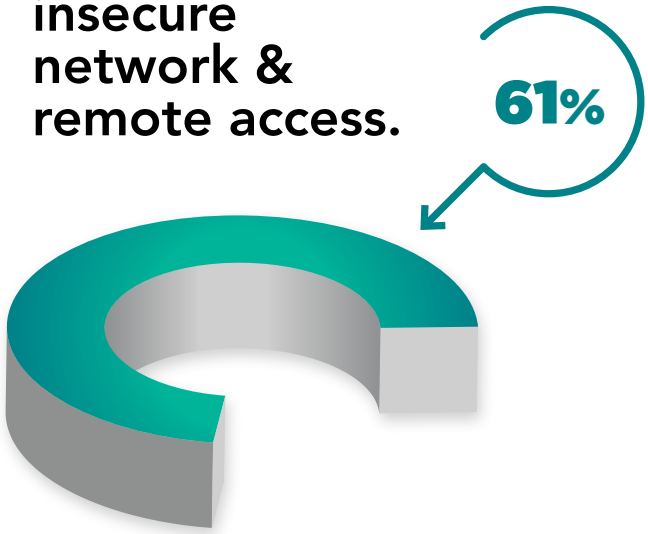
> ***"ZT is a data-based security model that relies on different sources of input to make real-time access decisions"***

TODAY'S THREAT LANDSCAPE IS DESPERATE FOR ZERO TRUST

As the world becomes increasingly connected, it also becomes less secure. Today, enterprises benefit from a wealth of devices that assist in operational capabilities. However, while this benefits the enterprise, it also benefits attackers seeking to exploit such devices. The volume of data possessed by organizations has grown exponentially to enable connectivity and has done so in an increasingly mobile environment. Hence, data is no longer tied to a specific location, and it is both endpoints and networks which facilitate remote data access.

Endpoints make attractive targets not only because of the data stored on them, but also the network access that they can provide an attacker with. This includes IoT devices which are often used as an attack vector. According to a 2020 report on Zero Trust Endpoint and IoT Security by Cybersecurity Insiders, there is a concern among 61% of organizations regarding endpoints and IoT devices gaining insecure network access and remote access.

61% of organizations are concerned about endpoints & IoT devices gaining insecure network & remote access.

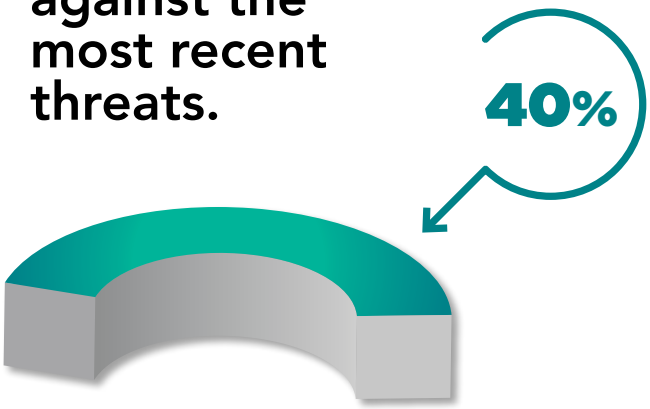


Even more worrisome is that attackers' tactics, techniques, and procedures (TTP) improve as security solutions become stronger. Malicious actors are finding increasingly innovative and deceptive ways to exploit the blind spots that security solutions do not cover.

40% of organizations claim that they have insufficient protection against the newest threats, according to the Cybersecurity Insiders report. Traditional perimeter-based network and endpoint detection and response solutions prove ineffective as cybercriminals have repeatedly demonstrated their ability to bypass many of these defense measures.

Malicious actors exploit the trust given to internal users and devices, resulting in successful attacks. By removing the concept of trust, ZT minimizes organizations' susceptibility to network infiltration stemming from unauthorized devices and their users.

40% of organizations cannot defend themselves against the most recent threats.



ZERO TRUST

While it is still necessary for enterprises to implement traditional security solutions as a form of tactical response, ZT provides a strategic framework that enables a shift to proactive security. As such, organizations can benefit from a hybrid environment that is both proactive and reactive, thus increasing the overall cybersecurity posture. With ZT, the concept of trust is eliminated from the organization's network architecture, thus providing more opportunities to identify threats and take subsequent action to avoid an attack. Importantly, ZT protects the enterprise outside its typical perimeters, which is especially relevant as telework, Bring Your Own Device (BYOD), and Internet of Things (IoT) devices become increasingly common "within" organizations. The ZT model ensures that network access is granted based on who, what, when, where, and how. However, to answer such questions, the enterprise must have complete device visibility.

ZT is based on the following three guiding principles:

1. Never trust, always verify

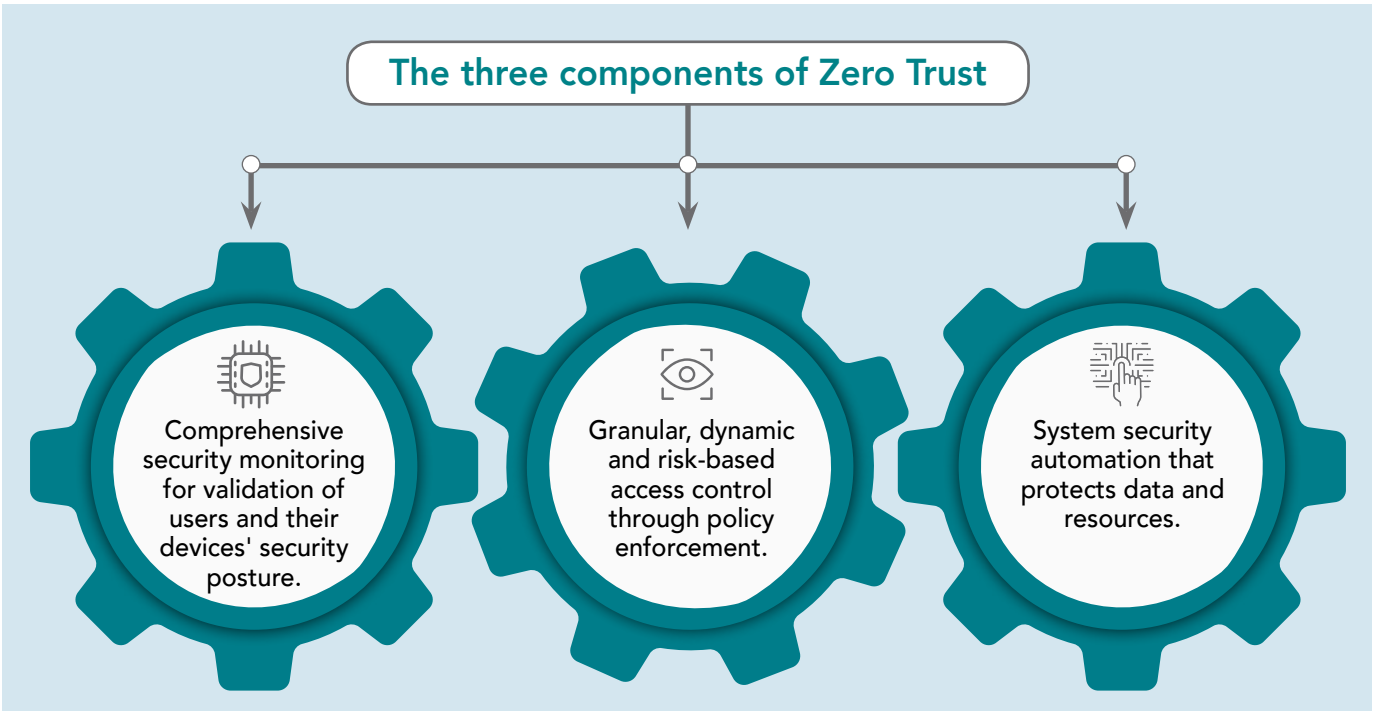
Enterprise network devices, and users, are typically assumed to be fully trusted as they are internal. However, both the device and the user's identity can be spoofed by a malicious actor. Furthermore, unmanaged and remote assets cannot be assumed as trusted since they are out of the enterprise's control, even though they are considered "internal". To eliminate the risks that come with trust, ZT eliminates the trust component itself; every user, device and application/workload must be treated as untrusted – every single time.

2. Verify explicitly

Access to resources is determined by a dynamic policy that relies on identity management and other data sources. Authentication and authorization should always be based on all data points, including user identity, location, device health, data classification, and more, to comprehensively evaluate the device and user's identity. The evaluation should continue for as long as the session lasts to ensure maximum protection.

3. Assume breach

Under the ZT model, resources are defended by the assumption that there has already been a breach, meaning that devices and users are denied network access by default. Access can be blocked several ways, depending on the ZTA the organization decides to implement. An architecture based on identity means that the characteristics of all users, devices, data flows, and requests for access must be heavily scrutinized. Access to data is controlled, minimized, and monitored based on the principle of least privilege, meaning that users' network access is limited to the lowest level required to perform the task. An architecture based on micro-segmentation significantly reduces the user's ability to move laterally throughout the network by isolating workloads through granular segmentation policies. Essentially, the network splits into smaller parts, each of which requires separate access. Micro-segmentation is an effective ZT approach as, often, a perpetrator's point of infiltration is not the target of attack. Micro-segmentation prevents the lateral network movement that facilitates the actual attack. A strong ZTA will incorporate numerous aspects from various approaches to enhance the Assume Breach principle. Finally, all configuration changes, resource access and network traffic should be logged, inspected, and constantly monitored for suspicious activity.



CHALLENGES

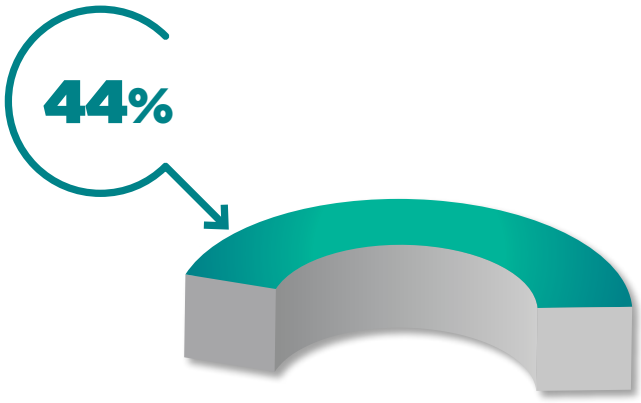
Adopting the mindset

Implementing ZT is a long process that requires integration across all departments and processes. For ZT to be effective, the entire organization must adopt the mindset of "never trust, always verify". Leaders must be willing to put in the necessary investments that ZT adoption requires, while staff and users need to make an effort to understand the concept and why is it necessary for cybersecurity, in an attempt to avoid security fatigue.

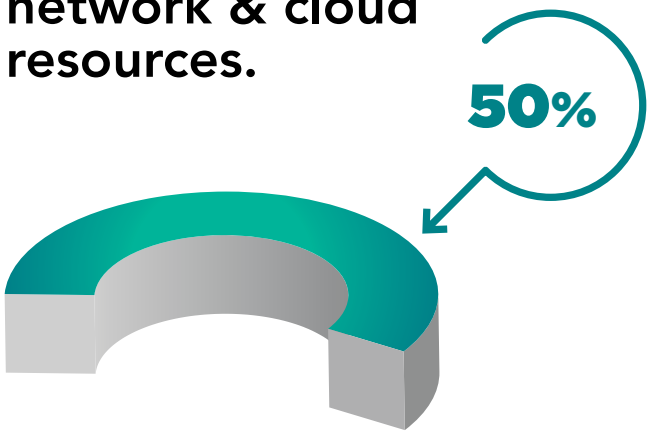
Visibility

A ZTA relies on a strong Continuous Diagnostic and Mitigation system (CDM) to identify and manage devices, and to log network activity. As such, the enterprise must have complete asset and network visibility to accurately evaluate the access requests. However, the charts below demonstrate the difficulties that many enterprises face when it comes to device visibility.

Organizations most concerned about unknown/ unmanaged devices operating within its infrastructure.



Organizations have moderate means to discover, identify & respond to unknown, unmanaged, or insecure devices accessing network & cloud resources.



A lack of visibility presents a substantial risk to the ZT model, which relies on device characteristics and device monitoring to evaluate access requests. A compromised device can bypass ZT security policy measures and gain network access by spoofing a legitimate, trusted device. Spoofing devices sit on the Physical Layer and run completely passively with no inbound traffic manipulation, operating under the radar of existing security software solutions, including NAC and IDS.

As such, network access might be granted based on an inaccurate evaluation due to a lack of visibility. More worrying is that, by going undetected, Rogue Devices can bypass micro-segmentation and enable the attacker to move laterally throughout the network. Network access can facilitate harmful attacks and, since Spoofed Devices go undetected, the attacks can persist for long periods of time. Furthermore, as ZT is specific to network access, IoT cybersecurity is at risk since IoT devices are also vulnerable to Physical Layer manipulation.

IoT cybersecurity covers a broad spectrum as the number of IoT devices in use has increased by astonishing amounts and now includes everyday devices that are not typically deemed a security risk. And, since such devices require network access, they are an attractive target to hardware attackers.

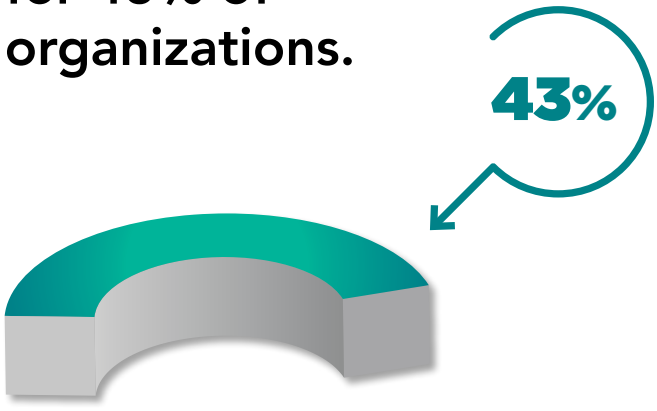
The risk of a compromised device is a serious concern for many organizations and is deemed the greatest endpoint and IoT threat for more than half of organizations.

Access policies

A ZTA uses data access policies as a source of information when evaluating access requests. Policy creation is based on asset and network traffic data, yet the visibility challenges mentioned above will have a knock-on effect on effective policy creation. A lack of asset and network visibility will result in policies that have been developed without complete information, negatively impacting the validity and reliability of such policies.

Endpoint and IoT policies are relevant to ZT as these devices will make access requests, and the Policy Engine (PE) will depend on such policies to determine the access decision. Furthermore, since ZT expands outside the enterprise's perimeters, endpoint and IoT policies are essential in ensuring that such devices maintain their security posture when operating in a non-enterprise-owned environment. However, 43% of organizations' greatest security challenge is the inability to enforce access policies on endpoint and IoT devices, harming the efficacy of the overall ZTA. And, more importantly, any policies that are in place will not be enforceable on assets that are not visible.

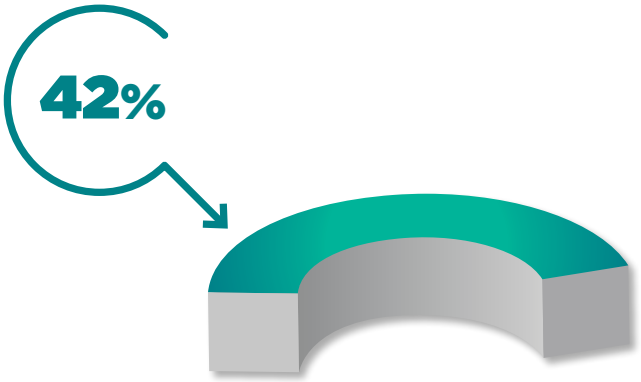
Enforcing endpoint & IoT access policies is the greatest challenge for 43% of organizations.



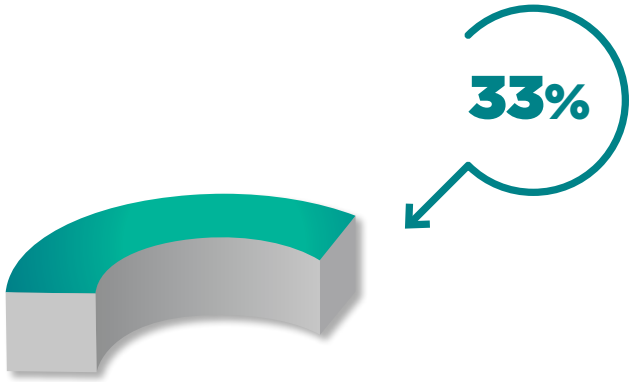
ZERO TRUST HARDWARE ACCESS WITH HAC-1

With a lack of device visibility limiting the ZTA's efficacy, enterprises are beginning to focus on applying ZT to the hardware level. Starting at the first layer of defense ensures that a more comprehensive ZTA is in place to provide a stronger overall ZT approach.

Organizations adopting a ZT approach on the hardware level due to an inability to identify, classify & monitory endpoint and IoT devices.



Organizations adopting a ZT approach on the hardware level due to insufficient visibility into endpoint & IoT activity.



The ZT model grants access based on who, what, when, where, and how. If the organization cannot answer these questions accurately, then the ZTA is essentially ineffective. To answer such questions and have a strong ZTA, enterprises must have complete asset visibility. With Zero Trust Hardware Access, the focus is on all hardware assets operating within the enterprise's infrastructure – including remote assets – as this is where access requests originate from, as well as being able to answer the critical questions of "who, what, when, where, and how".

Concentrating on hardware improves the overall efficacy of the enterprise's ZTA, especially micro-segmentation efforts, as the PE can make accurate access decisions through deep visibility into a device's characteristics. Furthermore, enabling Hardware Access Control through policy enforcement stops a hardware attacker at the first hurdle, not even giving them the opportunity to cause damage or infiltrate the network.

Sepio's Hardware Access Control solution (HAC-1) enables Zero Trust Hardware Access through a comprehensive approach to Hardware Access Control. HAC-1 provides enterprises with complete device visibility by using Physical Layer fingerprinting technology and Machine Learning to calculate a digital fingerprint from the electrical characteristics of all devices. By validating devices' Physical Layer information, HAC-1 verifies the device's true identity – not simply what it claims to be. Comparing a device's digital fingerprint with the extensive built-in threat intelligence database for known-to-be vulnerable devices allows HAC-1 to instantly detect when a vulnerable or malicious device is present within the organization's infrastructure.

The comprehensive policy enforcement mechanism of HAC-1 allows the system administrator to define a strict, or more granular, set of rules for the system to enforce that controls hardware access based on device characteristics. As such, Hardware Access Control policies support PLP, which is integral to ZT. More importantly, when breached, HAC-1 automatically instigates a mitigation process to instantly block unapproved or Rogue hardware. Hardware Access Control policies provide actionable support to Zero Trust Hardware Access and prevent malicious devices from bypassing traditional ZT security policy measures, such as identity-based approval and micro-segmentation.

The three components of Zero Trust enhanced by HAC-1

Comprehensive security monitoring for validation of users and their devices' security posture.

HAC-1's ultimate visibility capabilities enable the most comprehensive approach to device monitoring.

Granular, dynamic and risk-based access control through policy enforcement.

HAC-1 allows organizations to implement strict, or more granular, hardware access control rules.

System security automation that protects data and resources.

HAC-1 allows organizations to implement strict, or more granular, hardware access control rules.

CONCLUSION

As it can no longer be assumed that internal users and devices can be trusted, ZT is an attractive security model being adopted by many organizations. Based on the principle of "never trust, always verify", organizations adopt ZT to enhance their security by treating every user and device – internal or external – as a potential threat and eliminating any automatic trust given to those requesting network access. Additionally, with ZT, users and devices are only provided with the necessary network access to perform the task, reducing the possibility of malicious lateral movement.

However, a ZTA relies on numerous data sources for the PE to make an accurate decision. The lack of visibility and access policy challenges put the efficacy of the ZTA at risk. Such challenges allow Rogue Devices to bypass identity-based authentication and micro-segmentation, providing an attacker with unauthorized network access – without the enterprise even knowing. To mitigate the risk, organizations must focus on Zero Trust Hardware Access. Doing so means that ZT applies to the first layer of defense and can therefore better protect the organization from intruders.

With HAC-1, a Zero Trust Hardware Access approach can be achieved through complete device visibility and a policy enforcement mechanism that, when combined, also enable Rogue Device mitigation. As a result, the enterprise benefits from a stronger overall ZTA as hardware attack tools can no longer bypass the ZT model.

HAC-1 - Visibility & Security of Hardware Assets

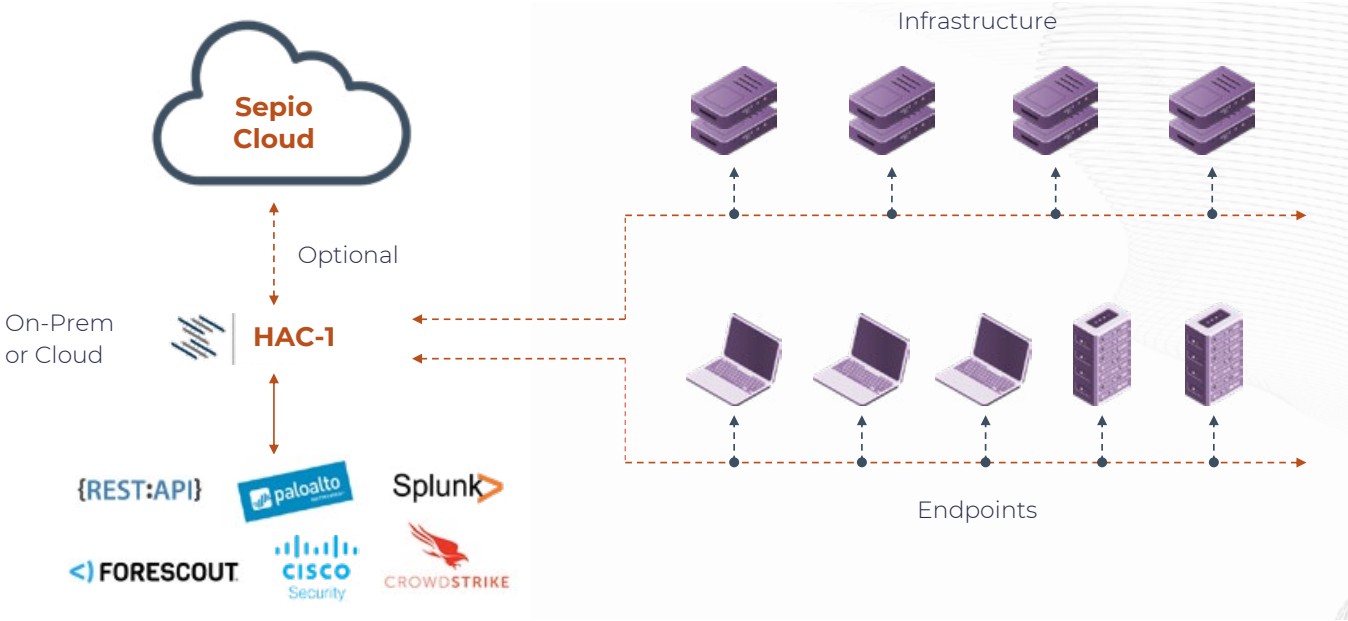
Main Benefits

Complete Visibility of AI Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE


IOT
access denied
210.95
149.16
23.26
1.41%