EXIUM

CATEGORY: Solutions Brief

See, Know, and Secure IoT Devices for Enterprise, Industrial and Healthcare

Solution: Secure Things Access (STA) ▪ **Industry**: Enterprise, Industrial, Healthcare, more ▪ **Use Case**: Securing IoT/ OT devices

Exium Secure Things Access (STA) ensures IoT and OT devices connecting to your network are secure and protected against cyberattacks that can infect your extended business. Applies protections to any IoT or OT device across smart-office, smart-building, medical and industrial environments.

With 63% of enterprises, 92% of industrial organizations and 82% of health care organizations using IoT, almost every company is exposed to cyber-attacks. IoT devices make life easier for businesses. Unfortunately, connecting IoT devices to the network extends the attack surface which provides more entry points for hackers. Many of the IoT devices currently deployed are running on unpatched software, are misconfigured, or use unsecured communication protocols, which makes them extremely vulnerable and easy to hack. Organizations require these devices to enable their business, yet they cannot trust them. IoT devices pose immense cybersecurity risks as they are largely unregulated. In fact, majority of these devices, which often ship with their own vulnerabilities, are susceptible to medium- or high-severity attacks. It is especially concerning when they are network-connected with unfettered access.

Security teams, rarely involved in purchasing, find it extremely challenging to secure these devices due to their incredibly diverse types, long lifecycles, and lack of coverage from traditional security controls.

Most traditional security products can't see these devices and the ones that can often don't know what to do with them because they can't identify them accurately. You need more than just an IP address to tackle threats in a way that's effective but not disruptive to critical equipment like medical and manufacturing devices.

Current IoT security solutions limit their visibility to manually updated databases of known devices, require single-purpose sensors, lack consistent prevention, don't help with policy creation, and can only provide enforcement through integrations. All this leaves security teams with heavy lifting, blind to unknown devices, and unable to scale their operations, prioritize efforts, or minimize risk.

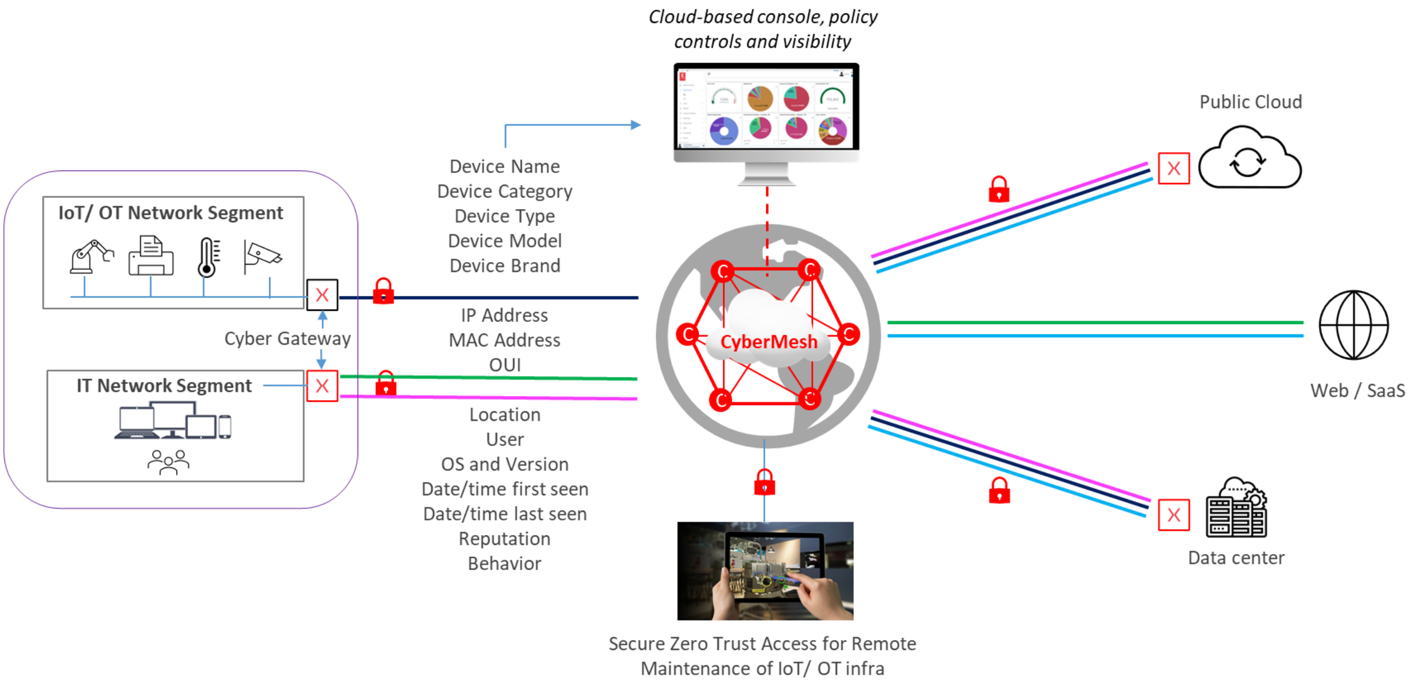
Protect Every Device on Your Network

As an integral part of Exium's CyberMesh platform, Exium Secure Things Access (STA) ensures IoT and OT devices connecting to your network are secure and protected against cyberattacks that can infect your extended business.

Without any agents or additional hardware, the Exium platform uses the existing infrastructure to discover and identify every device in any environment—enterprise, medical, industrial, and more. The platform analyzes device behavior to identify risks and threats and provides continuous device risk assessments.

With its market-proven hardware Root-of-Trust (RoT) design, STA ensures the highest level of protection for all connected devices with end-to-end encryption and zero trust authorization.

To overcome IoT device limitations, the Cyber Gateway (CGW) connector runs on a client's existing IoT gateway or any other standard x86 hardware and acts as an intermediary between IoT devices and the CyberMesh, extending a highly secure Zero Trust Path for end-to-end protection and performance.



Identify & classify devices in any environment.

Exium automatically discovers every connected device and collects comprehensive data on each. See granular details, such as manufacturer, model, version, operating system, location, applications, IP and MAC address, reputation, username, software, behavior, connections, risk factors, and more. View devices by type, such as all physical security devices or all network cameras. Drill down to view specific devices by model and version. Or view devices on specific VLANs or subnets. Exium also decodes more than 100 device and industry-specific protocols for analyzing the application-level behavior of each device. Our machine learning engine classifies each device based on its type and business function.

The platform also performs application-based discovery by looking at the software applications that use IoT devices as sensors, then following the path from the application to the specific devices. This provides additional information about configuration, usage, performance, and device relationships.

Automate microsegmentation

The Exium platform reveals specific communication flows that each device requires to perform its function. Exium can dynamically generate microsegmentation policies, to ensure that devices can only interact with other necessary devices. For example, an HVAC system can communicate with a trusted smart-building controller using approved protocols while being blocked from communicating to the Internet or another HVAC system.

Create policies for any unmanaged & IoT device

As the Exium platform discovers devices in the environment, it provides the Admin console granular device attributes like the manufacturer, model, operating system, MAC address, and more. It also provides a risk analysis based on contextual understanding of a device's behavior in your environment.

In the Admin console, you can configure policies based on these attributes, and you can enable policy recommendations made by the Exium platform. This allows you to reduce your risk exposure proactively by ensuring your security gateway has policies for any device in your environment— policies that can react to changes in device attributes, behavior, and risk level.

For example, you can set granular rules that restrict devices from using unapproved protocols, applications, and communication patterns. You can also set policies to alert on anomalies in device behavior or communication patterns. And to avoid confusion or conflicts, Exium keeps policies for unmanaged and IoT devices separated from policies for your entire network.

> “
>
> *Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices make up more than 30% of the devices on enterprise networks. Organizations require these devices to enable their business, yet they cannot trust them. IoT devices pose immense cybersecurity risks as they are largely unregulated.”*

Detect and respond quickly to threats and vulnerabilities

Exium IoT security solution uses continuous device analysis to detect threats and vulnerabilities associated with unmanaged and IoT devices (i.e., CVE's, unsupported operating systems, etc.). This analysis is based on information from Exium Device Knowledgebase and from premium, globally-shared threat intelligence feeds.

When the Exium platform identifies a vulnerable device, it can activate security protections automatically, either through virtual patching (by installing the appropriate IPS signatures on the gateways) or through policy enforcement that isolates affected devices. This provides effective protection against unpatched devices, or devices running on unpatchable operating systems and software, all without disrupting critical processes and business operations.

Provide security teams comprehensive device information

Each device also is analyzed for potential risk to the organization. Exium identifies high-value devices, as well as those with vulnerabilities, recall notices, weak or open passwords, and indicators of compromise. Device behavior is analyzed to understand normal communication patterns. We can detect device interaction with known malicious IP addresses or domains. Anomalous device behaviors can be identified based on observed device and network baselines.

Security teams also can see the wealth of information the platform provides about each device directly in the admin console. With rich log records and dedicated IoT event reports, Exium gives security teams a contextual understanding of device behavior and forensics for event investigation. That helps make security teams more well-informed when responding to threats without impacting critical devices, and without ever leaving the admin console.

Discover and learn	Zero-Trust segmentation	Monitor and control	Detect and respond
The Exium platform discovers and classifies every managed and unmanaged device in any environment—enterprise, manufacturing, healthcare, retail, and more.	Once the enterprise understands its IoT attack surface, IoT devices can be segmented into policy-driven groups based on their risk profiles.	See and profile every device on the network, to understand what IoT devices are being deployed.	The Exium platform continuously analyzes device activity for abnormal behavior. Whether a device is misconfigured or is the target of an attack, the platform can alert your security team and trigger automated actions to help stop an attack.
It works with your existing IT/security tools and network infrastructure to identify every device, including off-network devices that use Wi-Fi, Bluetooth, and other IoT protocols.	The policy driven IoT groups and internal network segmentation enable monitoring, inspection, and policy enforcement based on the activity at various points within the infrastructure.	Control access to the network, both connecting to the network and determining where devices can access.	Automatically detect policy violations, restrict access or quarantine suspicious or malicious devices.
This comprehensive device inventory includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, connections made over time, and individual risk assessment scores.	Enforce zero trust policies to prevent unauthorized access and lateral movement	Monitor the devices on the network to ensure that they are not compromised and to take automatic and immediate action if they are.	This automation provides peace of mind that an attack on any device—managed or unmanaged—can be stopped, even if your security team is busy with other priorities.

Exium IoT Security Business Benefits

Businesses of all types are moving rapidly to take advantage of IoT and industrial IoT technology to streamline operations and automate processes. However, every connected device on the factory floor or in the field introduces a host of vulnerabilities and expands the attack surface.

With billions of these devices connecting to corporate and industrial control systems, cybercriminals are finding new ways to launch attacks, steal sensitive data and disrupt public works and government services we rely on everyday. And with their limited processing power and memory, these connected devices often lack the security controls to keep them secure.

Exium offers the industry's most innovative IoT security solution, allowing you to stop threats and control the risk of IoT, IoMT, OT, and Bluetooth devices on your network. Leveraging a machine learning-based approach, our cloud-delivered IoT Security service quickly and accurately discovers and identifies all IoT devices in real time, including those never seen before. IoT Security uses crowdsourced data to identify anomalous activity, continually assess risk, and offer trust-based policy recommendations to improve your security posture.

Combined with our industry-leading Extended Detection and Response (XDR) solution, IoT Security can prevent threats, block vulnerabilities, and automatically enforce policies either directly or through integrations, reducing the strain on your operations team and keeping devices safe. IoT Security deploys effortlessly from the cloud and requires no additional infrastructure.

> *“Exium automatically discovers all managed and unmanaged devices and delivers insight through the real-time dashboard. Exium also generates policies by type and enforces them to support micro segmentation, zero trust and other network access controls.”*
>
> **IT Technical Manager, Healthcare provider**

Exium platform’s advanced device visibility and monitoring with Zero-Trust policy management reduces your exposure to the risks of unmanaged and IoT devices and provides security teams with deeper device insights—all without disrupting business operations.

Turn unmanaged devices into managed devices. Gain visibility into all IT, IoT, IoMT, OT and Bluetooth devices, and control the largest contributor to risk: unknown devices.

Enjoy complete IoT security. Gain ML-powered visibility, prevention, trust-based policy recommendations and enforcement for every device in your network from a single platform.

Reduce the strain downstream with prevention. Built-in prevention stops threats as they arrive, eliminating the deluge of alerts on your security team.

Leverage your existing talent. Empower your existing security and operations teams to secure IoT without changing their practices, policies, or procedures.

Improve operational efficiency with integrations. Optimize cross-product operations and new security use cases across ITAM, SIEM, NAC, and more.

Use predictable and simplified licensing. Avoid exhausting device true-up models and get simple licensing based on network coverage.

Don’t get caught with single-purpose sensors. Every IoT solution requires its own visibility sensor. Only with Exium can you prevent threats, segment, and enforce policy as well.

Get security built for enterprise use cases. Secure IoT in any industry: healthcare, finance, retail, government, education, manufacturing, and more.

Frictionless Deployment and Integration that delivers immediate time-to-value. Getting started with the Exium is fast and easy. It’s agentless and requires no additional hardware. With just a few clicks, you can connect your existing IT/security tools with our out-of-the box integrations to start seeing value immediately.

Ready to secure your IoT/ OT devices?

Test Drive Here