Best IoT Security Solutions

Internet of Things (IoT) solutions have revolutionized today's workplace. These devices offer predominantly positive ROI for organizations, from location tracking and remote asset monitoring to process automation and asset performance optimization.

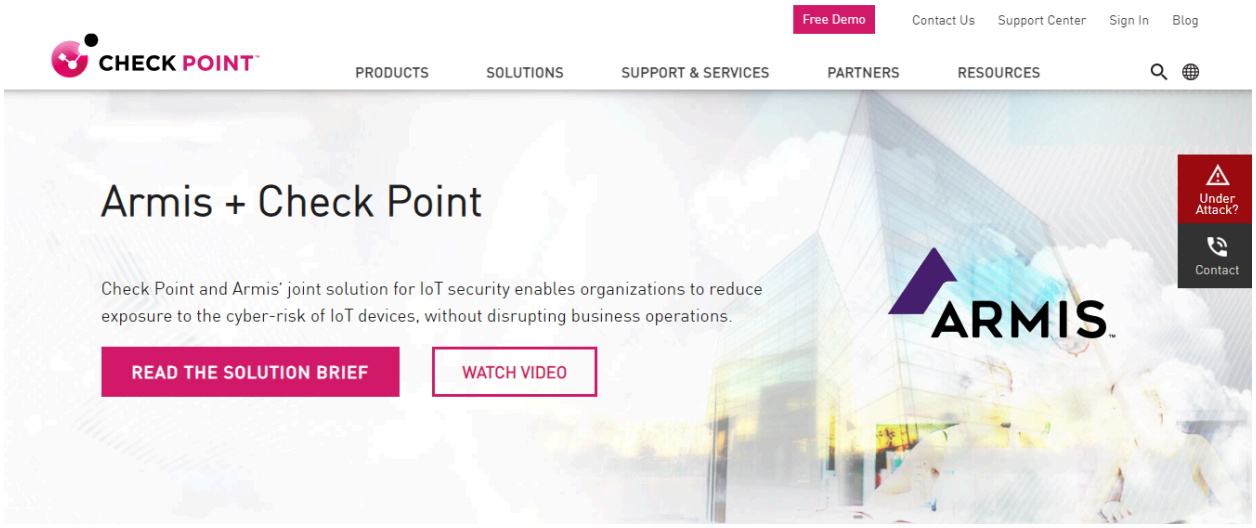
These devices also serve just about every market, including commercial, industrial, and consumer applications. And IoT adoption is only expected to rise in the coming years. According to Statistica, there will be 38.6 billion connected devices worldwide by 2025.

IoT devices also present unique security challenges over traditional devices like desktops and laptops. For instance, IoT devices typically have low memory, compute, and storage capabilities. This design makes it difficult, if not impossible, to implement security directly on the hardware.

Furthermore, IoT software and hardware components are often sourced and assembled by different manufacturers. This reality leads to disparate security elements ownership, making it difficult to unify device security.

Nevertheless, Internet of Things (IoT) security solutions propose countermeasures for these security challenges and optimize device performance and usage. Below are the five best IoT security solutions on the market today.

Armis + Check Point



Armis + Check Point is a joint platform that combines the disparate capabilities of Armis and those of Check Point into a unified IoT security solution. Armis offers asset discovery, continuous vulnerability assessment, and device behavior tracking capabilities. Checkpoint, for its part, brings security gateways and security policy management to the fold.

Firstly, Armis + Check Point is an agentless solution. Instead of installing software on your devices, the platform relies on your existing infrastructure to discover, monitor, track, and secure IoT and unmanaged devices. This setup means that you don’t have to worry about devices crashing or similar disruptions during scanning.

Secondly, the solution offers continuous monitoring with real-time device behavior updates in the IoT Security Manager Console. Security managers can then use this information to create informed policies. Alternately, Armis also recommends security policies based on the platform's data.

Admins also get granular control of policy management. For example, admins can prevent devices from using prohibited applications or unapproved protocols.

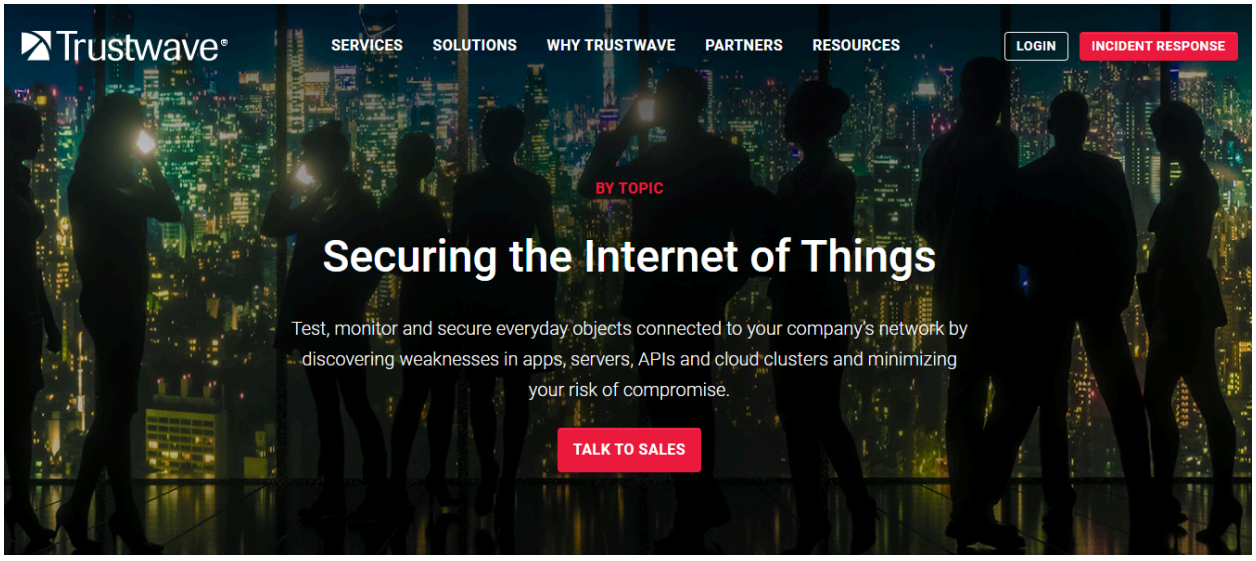
Other notable Armis + Check Point features include:

- Automatic IoT discovery
- Automated security protections
- Dedicated IoT event reports
- Contextual risk analysis
- Zero-trust segmentation
- Armis Device Knowledgebase and other premium threat intelligence feeds

On the downside, Armis + Check Point is a fully web-based solution. This renders the solution ineffective in the absence of an internet connection. The platform also doesn’t support mobile access such as iOS and Android, which puts field teams at a disadvantage.

Still, Armis + Check Point is an effective IoT security solution for various environments, including industrial, medical, enterprise, and more. You’ll need to contact sales to learn about pricing.

Trustwave Managed IoT Security

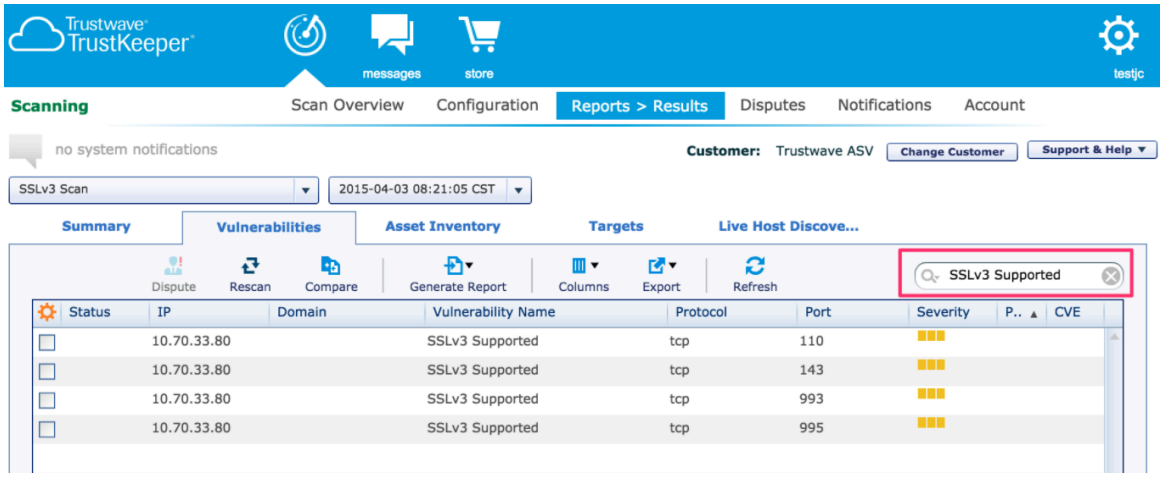


Trustwave Managed IoT Security is an extended IoT security service primarily targeting IoT product manufacturers, developers, and providers. The platform takes a two-fold approach to secure IoT devices.

Firstly, Trustwave secures endpoints, including physical devices and the associated infrastructure. Secondly, the platform monitors the edge where these devices interact with your network. This step includes continuously monitoring mobile and web applications, networks, servers, databases, and cloud servers supporting IoT devices.

Trustwave also offers a comprehensive list of managed security services, including SSL Certificates, managed SIEM, managed DDoS protection, managed IDS/IPS, and firewall management. All this happens with the help of the SpiderLabs team, a group of expert security researchers, forensic investigators, incident responders, penetration testers, and malware researchers.

Trustwave equally supports IoT implementers and deployers. Implementers can outsource critical IoT security measures, including IoT security testing, monitoring, and management, to the platform's security operations center.



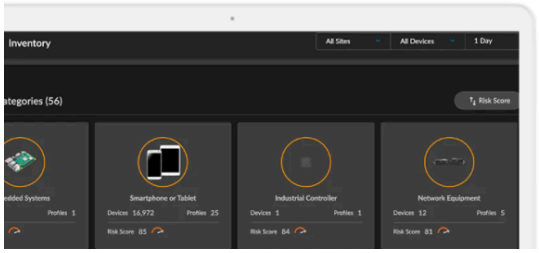
Users also can access the Trustwave TrustKeeper portal for complete visibility and control over network security. The cloud-based portal is intuitive and easy to use. For example, admins get access to various apps spanning managed security services, vulnerability scanning, penetration testing, and compliance management. The portal also offers easily digestible snapshots of your security and compliance posture in real-time.

The TrustKeeper portal also allows admins to view and manage security events, trends and reports, and alerts. Finally, admins can communicate directly with Trustwave security analysts right from the portal.

On the downside, Trustwave is expensive for small businesses and startups. In addition, you need to get into a licensing contract. This situation can make it difficult to switch vendors if you're unhappy with the service.

Trustwave offers custom pricing depending on the managed security services you require.

Palo Alto Networks IoT Security



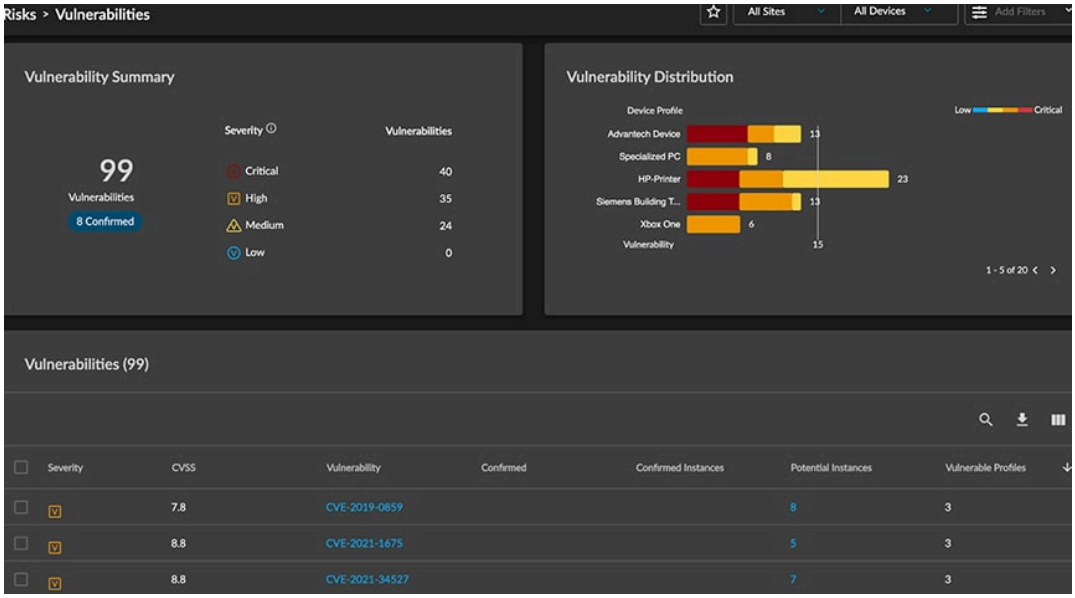
Palo Alto Networks IoT security provides a smart, machine learning-based solution for securing enterprise networks. The platform leverages machine learning to continually assess risk, identify anomalous activity, and provide actionable policy recommendations to secure your network. Additionally, the platform automatically discovers and identifies all IoT devices in your network in real-time. It is a cloud-delivered platform with no additional infrastructure requirements.

The platform also includes a next-generation firewall (NGFW) to proactively block vulnerabilities, prevent threats, and enforce policies automatically. Your operations team also gets deep insights into all IoT devices on the network, down to the physical location, firmware, port usage, access point, and up to 40+ other unique device attributes.

Other noteworthy Palo Alto Networks IoT Security features include:

- SaaS Security
- Enterprise Data Loss Prevention (DLP)
- Malware Prevention
- Advanced Threat Prevention
- DNS Security
- Advanced URL Filtering

Furthermore, the platform offers several automations to make things easier for your security team. For example, the platform automatically generates policy recommendations that you can instantly integrate into your existing firewall policies.

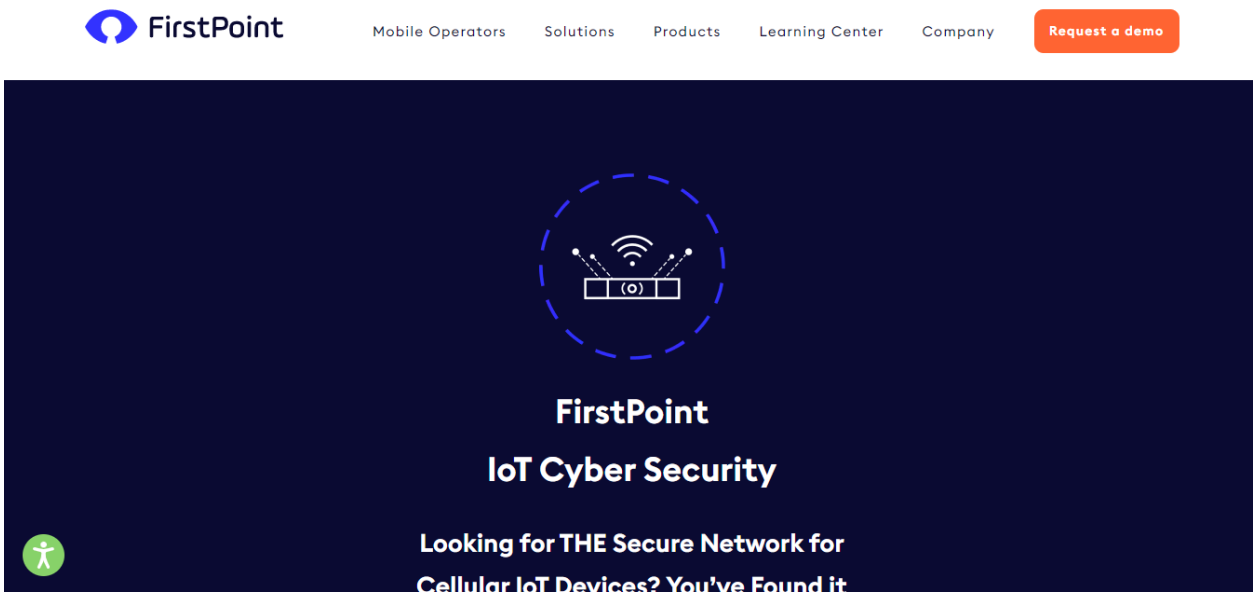


Finally, administrators can manage all the devices on the network from the intuitive IoT Security portal. You'll find the most commonly used pages such as Dashboards, Devices, and Profiles conveniently grouped. Similarly, visibility-related pages such as Applications, Networks, and Reports are all grouped for easy navigation.

On the downside, Palo Alto Networks IoT security offers a complex licensing structure. As a result, it can be difficult to know exactly how much you need to pay for the service until you are well into enrollment.

You'll need to contact sales to request a quote for the service.

FirstPoint



FirstPoint IoT security solution is designed explicitly for SIM or eSIM-based cellular IoT devices. Cellular devices are notoriously difficult to protect from location tracking, hacking, malicious exploitation, and eavesdropping. This reality is particularly concerning when using public networks. FirstPoint offers organizations complete control of cellular devices, regardless of their physical location.

FirstPoint relies on its SIM applet Over-The-Air (OTA) installed on devices to communicate with the SIM card. Additionally, the OTA technology updates, changes data, and builds security functionality on the SIM card independent of the original carrier's features and offerings. Alternatively, users can switch to FirstPoint SIM cards with built-in security features.

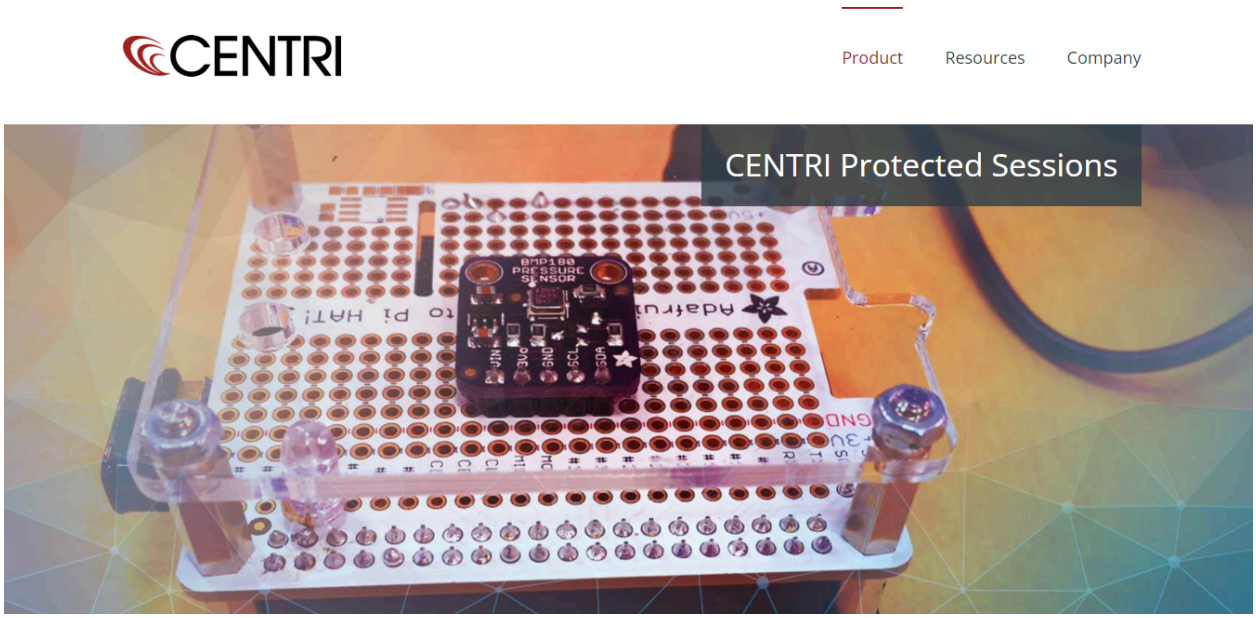
The solution takes a three-step approach to protect cellular devices. Firstly, FirstPoint creates a secure overlay network on top of your regular mobile network operator (MNO). This secured layer doesn't affect your regular MNO operations. Secondly, the solution secures the physical cellular device with its SIM applet. Finally, FirstPoint routes all signaling and data traffic through a secure network. ‘

FirstPoint also offers a central dashboard to manage all cellular IoT devices. Administrators can view all managed devices on the network, including defining devices, and set policies based on a group, type, user, or scenario. The dashboard also integrates existing mobile security features, including private APN, Mobile Device Management technology, and VPN. This way, you don't need to refer to separate consoles for all your on-device hardware solutions.

The obvious downside is that FirstPoint's security solution is protection is limited to cellular devices. So you'll still need another solution to cover other IoT devices like printers or biometric cybersecurity scanners.

FirstPoint doesn’t share its pricing publicly, so you’ll need to contact them for a quote.

CENTRI Protected Sessions



CENTRI Protected Sessions offers robust every-mile security from the moment your IoT devices create data to when the data is consumed. In addition, the solution is optimized for lightweight devices to counter common IoT security problems like intermittent network access or low-power microcontroller units (MCU).

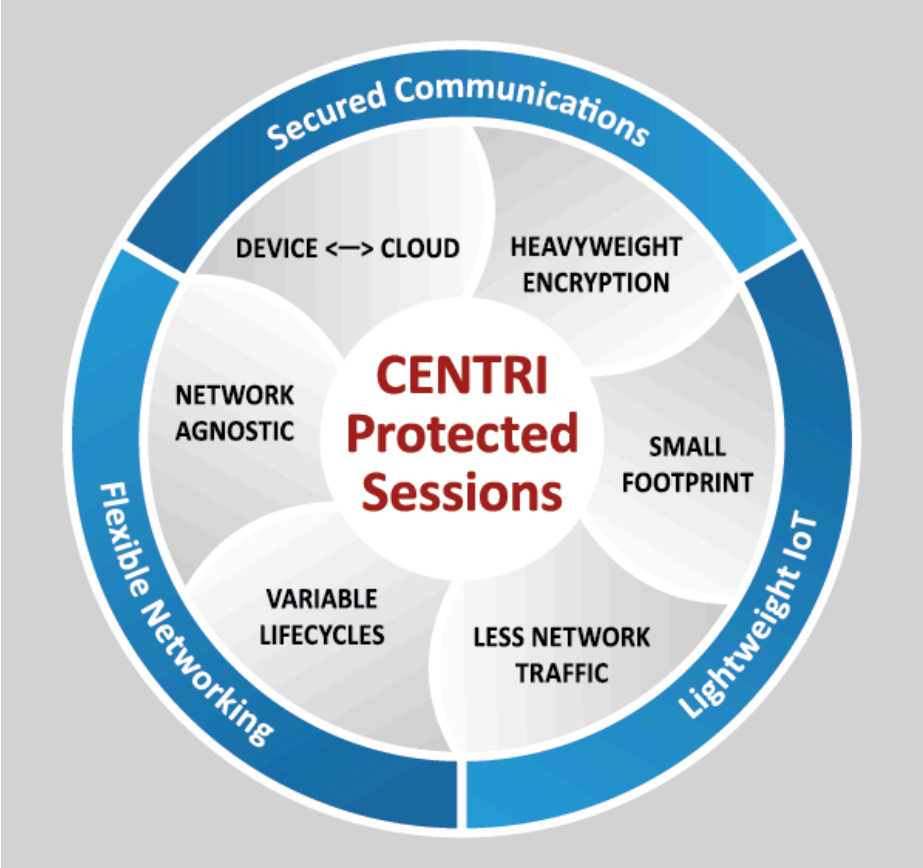
The solution is highly versatile by design. You only need to integrate it on the application server and the device. This setup allows it to run on virtually any network or mishmash of networks and protocols. You also don’t need to re-code your CENTRI Protected Sessions instance when you change network topologies.

The platform’s main features include:

True First-Mile Security – CENTRI Protect Sessions protects data right from the beginning before it is even introduced to the network. The solution extends this capability to all devices, including those without TCP-IP stacks, small devices, and low-power devices.

True Last-Mile Security – The CENTRI library lives inside your application server. Here, data is encrypted and decompressed, meaning that no unencrypted data ever travels through any of your network links.

Every-Mile Security – CENTRI protects your data at every point between the IoT device and application data. This includes data transfer between mid-points, compute engines, or gateways.



On the downside, CENTRI Protected Sessions can have a steep learning curve. It is primarily designed for IoT developers creating devices from scratch. As a result, the platform isn't as intuitive for users outside this domain. Otherwise, it's a tremendous every-mile IoT security solution for many industries.

Reach out to CENTRI directly to learn more about prices.

How to Pick Your IoT Security Solution

Choosing the right IoT security solution largely depends on your IoT security strategy. Leading with the most critical features will help you narrow down the options to find your organization's best IoT security solution.

Step 1 - Prioritize Visibility

If nothing else, an IoT security solution should offer total visibility of all the devices on your network. Ideally, the solution should automatically discover managed and unmanaged IoT devices. Additionally, it should provide high-fidelity information about all these devices, including make, serial number, classification, operating system, location, and so on.

All the solutions we reviewed here offer this capability to some extent. However, Palo Alto Networks IoT Security aggregates more than 50 device attributes, in addition to automatically discovering your assets.

You may also want to consider additional assets aside from IoT. These assets may include IT, OT, and IIoT devices. This way, you can manage *all* your network devices from a single platform. Here, Armis + Checkpoint satisfies this requirement. So you might not even need a separate security tool for your traditional IT hardware like laptops and desktops.

Step 2 - Look for Insights into Device Behaviors

It's one thing to have a visual of all the devices in your network. However, it's not always clear what these devices are doing in your network. The IoT landscape is ever-expanding, and you can't always stay on top of everything that's happening in the network.

Having a baseline for how devices communicate is central to proper IoT security. However, this isn't always possible or practical from a human perspective. Therefore, try to focus on solutions that integrate machine learning. These solutions can instantly detect anomalous behavior since they have access to vast data about how devices should be behaving in the first place.

Palo Alto Networks IoT Security is an excellent option in this regard. It incorporates machine learning to track and update each device's identifiable patterns. It then uses this information to flag unusual behavior that may indicate a possible cyberattack or breach.

Alternatively, a managed solution like Trustwave Managed IoT Security lets you outsource this task. The platform's security team is in charge of continuously monitoring your devices for strange behaviors and remedying detected issues as necessary.

Step 3 – Think about Centralized Management

You certainly need a single dashboard to track and investigate at-risk devices. The dashboard is a standard offering with IoT security solutions. But these dashboards aren't created equal. Ideally, you want an intuitive dashboard that's easy to navigate.

You may not immediately tell the quality of the dashboard until you get to the free trial in the last step. But a solution like Palo Alto Networks IoT Security immediately comes to mind with its intelligently structured portal dashboard.

Step 4 – Consider Segmentation Capabilities

Onboarding new IoT devices can be cumbersome, especially in a large organization. In addition, each device category probably has its own policy. So an IoT solution that automates segmentation based on device attributes is a must-have for enterprises.

Again, Palo Alto Networks IoT Security stands out. The platform offers segmentation based on policy enforcement, deep profiling, and assessment of your IoT devices.

Step 5 – Test Two or Three IoT Solutions

You should have a good picture of the IoT solution that might fit your organization's security needs. Don't forget to add a few of your own must-have features, such as agentless scanning or cellular network protection.

Most of these solutions offer a free trial with just a few details. Next, get a few IT team members to test two or three solutions and compare their feedback. Be sure to prioritize the steps we've outlined so far when evaluating the software. Other areas to assess during the free trial include data volume handling, scalability, user-friendliness, and pricing. Finally, you should identify the best IoT security solution for your needs.