Secure Your IoT Investments While Keeping Business As Usual

By: Xu Zou
Vice President of Products, IoT Security, Palo Alto Networks

The Internet of Things (IoT) is a significant driver of enterprise transformation. But to bring about this transformation, businesses need powerful cybersecurity that safeguards IoT investments from the threat of attacks. As reported by McKinsey, 75% of businesses say IoT security is a top priority—landing it at the top of every enterprise CISO's security agenda. But, the key question is "how difficult is this endeavor?"

IoT Is Here to Stay But Not Without Security Challenges

Out of all the respondents surveyed by McKinsey, only 16% feel prepared to tackle the challenges that come with securing IoT. The fact is IoT devices enter enterprises in large numbers with staggering diversity and mostly without involving IT, making them difficult to find, monitor, and therefore secure. Moreover, not all IoT devices are created for the same purpose.

Enterprise IoT devices, from surveillance cameras to IP phones, point-of-sale systems, conference room technology, and many others are brought in because they are essential to business operations. On the other hand, a number of fly-by consumer IoT devices are starting to enter and leave the network. These include everything from connected toys, wearables, and vehicles—see the most common at risk devices in your industry or region here.

Needless to say that IoT device proliferation is a matter of grave concern for security chiefs. When these devices connect to the network and communicate freely with each other, their concerns over the ever-widening attack surface grow even more. From an IT perspective, the 'untraceable' IoT devices become "shadow devices" or unmanaged devices, thereby exposing serious cybersecurity concerns. The conundrum makes one fact clear—as IoT continues to become integral to the enterprise, so should a well-planned and well-implemented IoT security strategy.

IoT Security Done Right Does Not Upset the IT Apple Cart

In the midst of seeing the IoT security problem grow, CIOs and CISOs have a mistaken impression about the approach needed to address and solve the problem. Many assume that they are required to purchase separate point solutions, build a separate and dedicated IoT security team, and radically change existing network security and security operational processes to bring it all together. At Palo Alto Networks, we have the opposite view and believe in taking a turn-key approach to IoT security—one that leverages existing talents, security infrastructure investment, and cybersecurity processes while utilizing the latest technology breakthroughs like machine learning to improve productivity, simplify processess and take full control of IoT Security.

Securing IoT Is a Highly Distributed Function

Security chiefs are not at fault for assuming securing IoT is a complex undertaking. As a matter of fact, early stage IoT security solutions were quite disparate, requiring dedicated security teams and significant investments in new infrastructure. But at Palo Alto Networks, we've figured out

a way that aligns all elements of securing IoT by leveraging existing IT resources, and without disrupting existing processes and best practices.

Here's our take—we think implementing IoT security is a highly distributed function calling for collective responsibility across **network infrastructure**, **network security** and **information security** teams. From our point of view, all three teams are functionally equipped to naturally extend their expertise to cover IoT security—what is required is just a functional alignment with each other and the individual **IoT device business owners** that introduced these devices into the organization. This is easily achieved by means of a single, centralized IoT security platform.

Once all teams have user access to the IoT security platform, the cross-functional role matrix required to implement IoT security would start with the **IoT device business owner** alerting Network infrastructure team of a new purchase to then secure the entire IoT security lifecycle with existing resources and best practices:

Network engineers, handling enterprise networking infrastructure, would use the IoT security platform to automatically discover existing and new IoT devices in real-time to onboard them into the network with proper VLANs and access policies. In tandem, the information security engineer would use the same IoT security platform to conduct all initial risk checks, making sure patch levels are up-to-date and device passwords are reset. The IoT business owner will be kept informed of the onboarding actions because proactive risk and vulnerability management of IoT devices is flanked as a joint responsibility between the IoT device business owner and information security.

Network security engineers, who manage policies on the Next-Generation firewall which is now "IoT-enabled", would be responsible for enforcing device-level security policies consistent with segmentation and Zero Trust to ensure that IoT devices are allowed to run trusted applications, communicate with allowed destinations, and accessed by verified users.

Additionally, they would manage prevention alerts delivered via the firewall to block known and unknown threats—keeping information security informed of both these activities. Because IoT device proliferation is constant in the current enterprise landscape, they would also oversee discovery of random new IoT devices coming onto the network and proactively manage IoT devices vulnerabilities, with help from information security.

The **information security engineers** will own anomaly detection, incident analysis, and response. They would use the IoT security platform to respond to unknown or zero day attacks on IoT devices taking advantage of device and incidence context to come up with a playbook-based approach to automate the incidence response process.

Additionally, they would integrate the IoT security platform with other tools to proactively address any IoT-related vulnerabilities working closely with IoT device business owners to address security and business risks.

A model IoT security solution connects all stages of the IoT security lifecycle by retaining on-going processes and functions of network and security teams, while leveraging machine learning to deliver leading-edge protections to unmanaged IoT assets on your Next-Generation firewall.

IoT Security by Palo Alto Networks is designed to accomplish exactly that—the cloud-delivered solution goes beyond providing baseline network traffic visibility by offering comprehensive IoT device identification, threat prevention and security enforcement for any enterprise environment. Designed to integrate with a customer's current network security infrastructure and processes, it eliminates spend on costly point solutions and the need to continuously fill security gaps with single-purpose infrastructure to help CISOs achieve the best return on investment. To learn more, visit us here.