SOLUTION BRIEF

Protect Your Critical IoT Infrastructure with Advanced IoT Detection, Protection, and Control Services

Executive Summary

The Internet of Things (IoT) continues to grow in capabilities and expand in applicability. We are surrounded by IoT devices that have become integral to the environments where we work, shop, learn, and play. We also live in a world where cybercriminals look to exploit technologies for financial or political gain. That's why, in addition to taking advantage of the services these devices provide, it's also essential to understand the different types of IoT devices we interact with, including their unique cyber risks, whether it's smart buildings (CIoT), Industry 4.0 sensors (IIoT), medical diagnostic and monitoring devices (MIoT), or just the smart consumer electronics (CEIoT) we have come to rely on in our daily lives.

In today's increasingly hyperconnected world, IoT devices play a valuable role in collecting, providing, and acting on data. Many devices do this by connecting to the cloud, where third parties process and analyze that information. However, these same devices often rely on overly simplistic security to protect that data—if they use anything. As a result, IoT devices create risks that increase exponentially as their numbers grow and your attack vectors expand. And because they are headless, there is usually no way to add security or even update their software.

That's why organizations that rely on IoT technologies need IoT detection and protection security services—like those provided by the FortiGuard IoT Detection Service—to bolster IoT security and mitigate IoT risk.

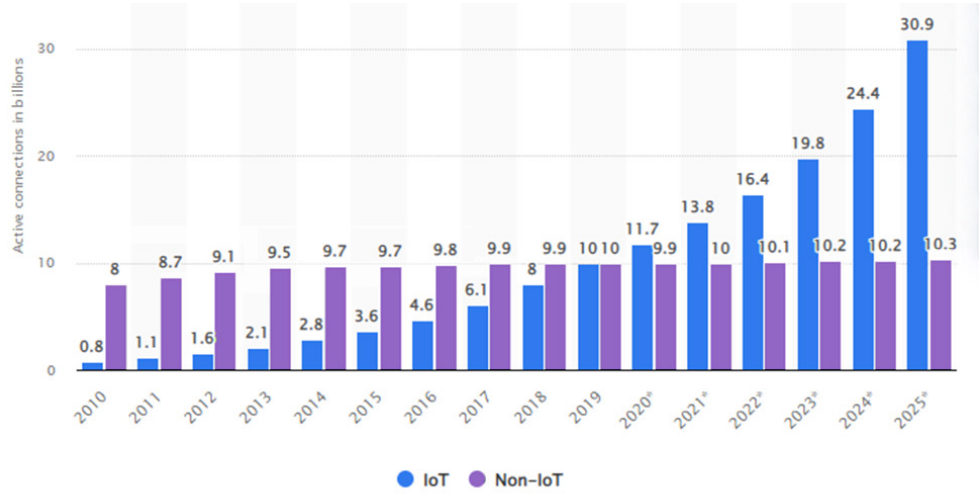

Figure 1: The dramatic rise of connected IoT devices

The number of deployed IoT devices surpassed non-IoT devices in 2020. They now represent 62% of all connected devices, and the number of IoT devices is expected to grow from 16.4 billion in 2022 to nearly 31 billion in 2025.[1]

Of the 80% of organizations that use IoT, one in five detected an IoT-based attack in the last three years.[2]

The Challenges of Securing IoT

Securing IoT devices represents a significant, and exponentially growing, set of challenges for most organizations.

Device detection

The first challenge is simply identifying all the IoT devices in use inside your organization. For many, the sheer number of vendors and devices in place makes IoT detection difficult and maintaining a current inventory next to impossible. Complicating matters further, the inherent simplicity of IoT devices can make it difficult to communicate with them. And this problem becomes even more challenging when IoT devices are deployed across your distributed environment and use the cloud to communicate with their servers.

The FortiGuard IoT Detection Service is designed to detect IoT devices connected to your network and then match them to a local library of IoT devices that is regularly updated. This helps simplify and accelerate the detection of IoT devices. And for any devices that are not part of the local library, FortiGuard provides a query service that polls FortiGuard Labs for the latest IoT device information for unknown IoT devices that the service detects. As a result, you can quickly create and maintain a robust, up-to-date inventory of all the IoT devices deployed across your network.

Powerful and finite IoT device security controls:

- Detection via local library and external query
- Vulnerability protection
- Virtual patching

Device protection

Detection is only half the battle. Once your IoT inventory is created, the next challenge is to figure out how to protect these devices, especially from new threats specifically targeting them. Unfortunately, the top priority for most IoT manufacturers is time to market. As a result, security safeguards and vulnerabilities associated with the software code or hardware they are supplying are often ignored or overlooked. As a result, IT teams need security solutions designed to prevent malicious IoT activity.

Once your IoT devices are identified, the FortiGuard IoT Detection Service uses its robust library of IoT-specific intrusion prevention system (IPS) signatures to detect malicious activity. It leverages the FortiGate Next-Generation Firewall (NGFW) and its powerful IPS engine to perform deep packet inspection (DPI) on IoT traffic to signature-match malicious exploits targeting known vulnerabilities. These known IoT IPS signatures are created and curated by FortiGuard Labs in concert with more than 200 global partners to ensure your IoT devices are protected with one of the industry's most comprehensive libraries of IoT IPS signatures.

Virtual patching

Traditionally, organizations rely on patching to combat known vulnerabilities and malicious attacks targeting devices. However, many IoT vendors see security as a secondary concern, which means that even those IoT devices that can be patched (and most can't!), those patches and updates may be a long time coming—if at all.

Fortunately, the IoT Detection Service working with a FortiGate NGFW enables an advanced security control called virtual patching. This strategy uses a FortiGuard Labs IoT IPS signature to block network traffic that matches the IPS signature, preventing an infection just as if an IoT vendor patch had been deployed. This allows unpatched IoT devices to be protected with an IPS rule until a device patch can be applied (when possible), thereby adding robust IoT security controls to the network.

The FortiGuard IoT Detection Service Is Part of the Fortinet Security Fabric

The FortiGuard IoT Detection Service, as part of the FortiGate NGFW, provides powerful IoT security. Additionally, both solutions are part of the Fortinet Security Fabric. Thus, the FortiGuard IoT Detection Service can be centrally managed, and security updates are delivered across the Security Fabric.

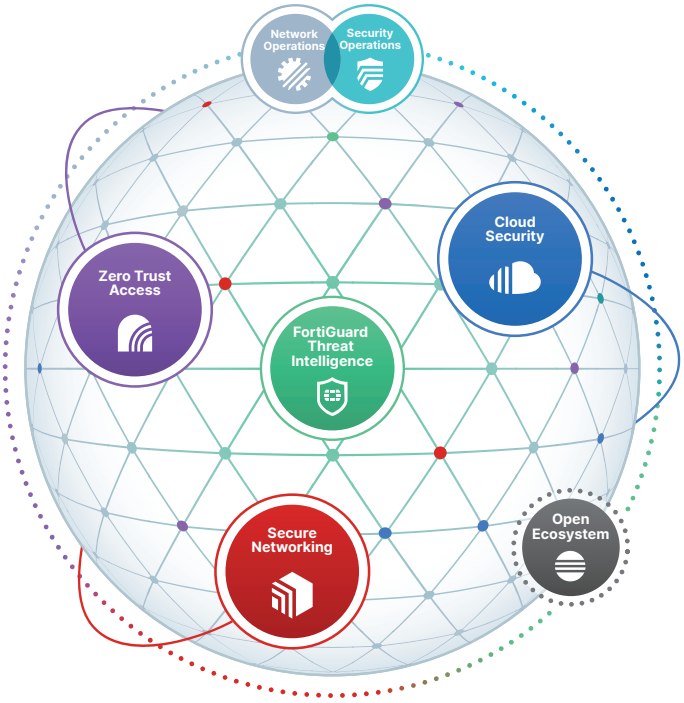

Figure 2: The Fortinet Security Fabric

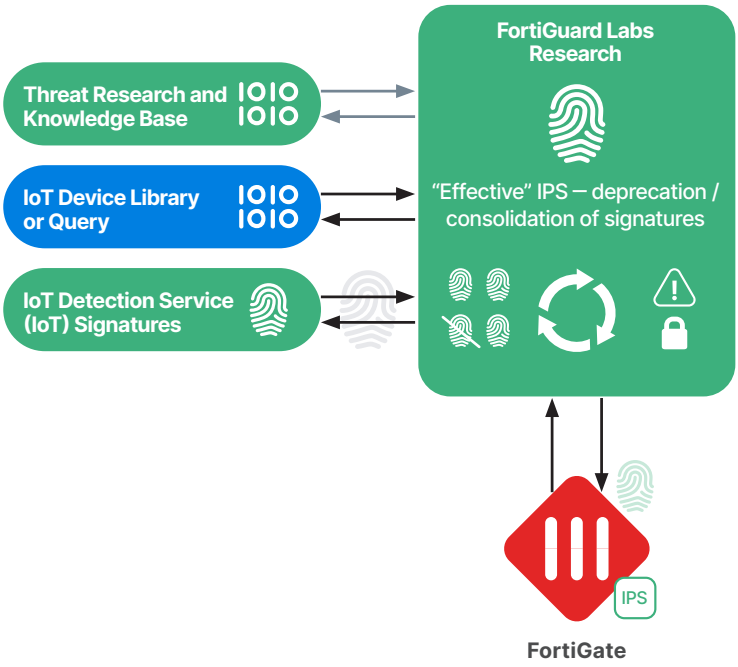

Figure 3: IPS signature development process

Enhance Your IoT Strategy with the FortiGuard IoT Detection Service

Managing and securing IoT devices is a monumental challenge for your network security team. The FortiGuard IoT Detection Service, combined with a FortiGate NGFW, is specifically designed to detect, inventory, and secure your IoT devices. It combines active IoT device detection, IoT IPS security controls, and IoT device virtual patching in a single service. And as part of the Fortinet Security Fabric, all IoT devices can be secured, centrally managed, and continuously updated across your entire distributed network.

[1] Statista, "Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025," Accessed December 16, 2022.

[2] Gartner, "IoT Security Primer: Challenges and Emerging Practices," Accessed December 16, 2022.

January 12, 2023 10:51 AM

1871821-0-0-EN