Reducing Risk from the IoT in Our Increasingly Connected World

How you can use network monitoring to identify and mitigate cyberthreats and operational problems in IoT devices

There will be more than

75 billion

connected IoT devices by 2025.

With the rise of automation, remote access, and the ever-expanding Internet of Things (IoT), IT and OT teams are collaborating at an unprecedented rate to strengthen organizational network security. Business operations that rely on machinery and physical processes are no longer disconnected from the world.

With a staggering majority of devices – expected to reach more than **75 billion by 2025** [1] – connected to vast networks and the internet, cybersecurity becomes a critical focal point for the age of IoT.

New Risks from IoT Devices

Today's countless Internet-connected devices offer many enhancements to our lives, but they also introduce new threats. These devices are mostly unmanaged, come from a multitude of vendors, use non-standard operating systems, support a diversity of – often insecure – protocols and may dynamically connect to other devices inside or outside of an organization's network.

Additionally, bad security practices like default or simple credentials, unencrypted traffic and lack of network segmentation remain common. Because many organizations lack visibility into their networks, it's almost impossible to identify and isolate an IoT device being attacked, or even one that was simply misconfigured during installation.

Detecting Threats in IoT Devices

If something bad or unexpected is detected in an IoT device, SilentDefense immediately notifies the operator and provides them with detailed threat intelligence to respond to the event.

This includes information about the:

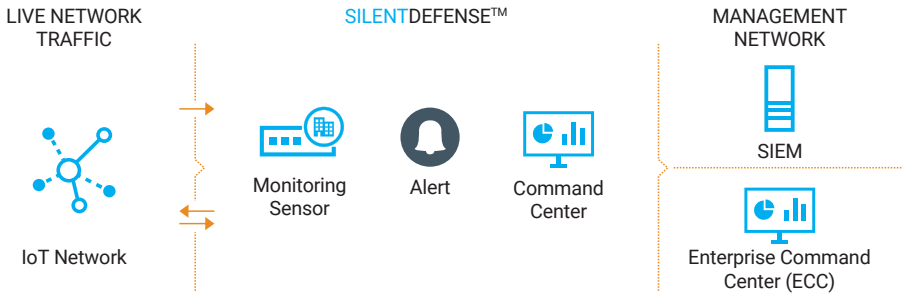
- Source of the problem
- Targeted device(s)
- Nature of the problem
- Packet capture (PCAP) of the traffic related to the event

This traffic capture can become critical information to have if advanced threats, such as a zero-day attack, occur. This key data can then be forwarded to specialized security vendors and organizations for further analysis.

The IoT Cyber Resilience Platform: SilentDefense

SilentDefense identifies vulnerabilities in IoT devices, and helps mitigate potential consequences of an attack. It protects these devices from a wide range of threats with patented deep packet inspection (DPI) and anomaly detection technology, combined with a library of over 2,400 threat indicators and over 3,500 IoCs for advanced cyberattacks, network misconfigurations and operational errors. Our IoT protocol coverage is the most extensive on the market, with over 130 protocols supported, and counting.

By continuously monitoring and analyzing network communications and comparing them with a baseline of legitimate/desired operations and with the "known bad" defined in a collection of checks, SilentDefense spots cyber and operational risks in the network in real time.



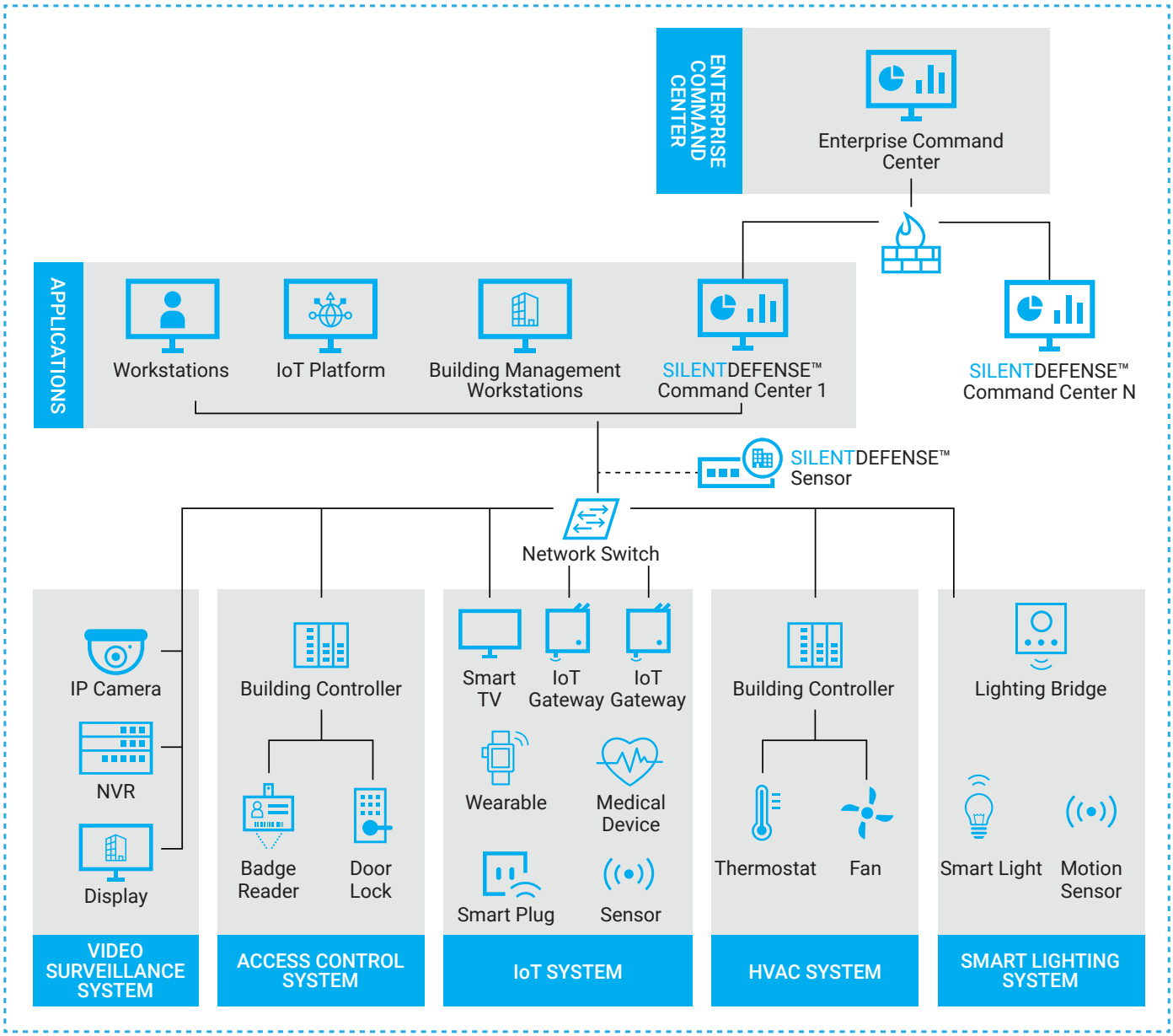
Basic SilentDefense Deployment Model

The optional Enterprise Command Center (ECC) provides global device visibility and risk management for geo-distributed, multi-site IoT systems from a single pane of glass. The ECC transmits relevant data from the field up to the enterprise level to analyze any incident in detail, including the devices involved and context of the alert.

Complete IoT Visibility

SilentDefense can identify and help remediate a full range of both cyber and operational threats, including, but not limited to:

- Cyberattacks (DDoS, MITM & Scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior / policy changes
- Device malfunction misconfiguration
- New and non-responsive assets
- Corrupted messages
- Unauthorized firmware downloads
- Insecure protocols
- Default credentials and insecure authentications
- Logic changes Default credentials and insecure authentications
- Logic changes



IoT Architecture with SilentDefense

SilentDefense Use Cases for IoT

Device Visibility and Monitoring

SilentDefense provides continuous asset visibility across the entire IoT network. It automatically builds a detailed network map with extensive device details and automatic grouping by network and/or role, provided in multiple formats, including Purdue level and communication relationship. Users can also proactively identify vulnerable IoT devices and protocols to prioritize mitigation strategies with the Asset Risk Framework, the first centrally available 'impact-based' risk tool for IoT networks.

SilentDefense uses a wide range of threat discovery capabilities that include:

- Patented deep packet inspection (DPI) of 130+ protocols.
- Continuous, configurable policy and behavior monitoring.
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems.

Device Configuration Management

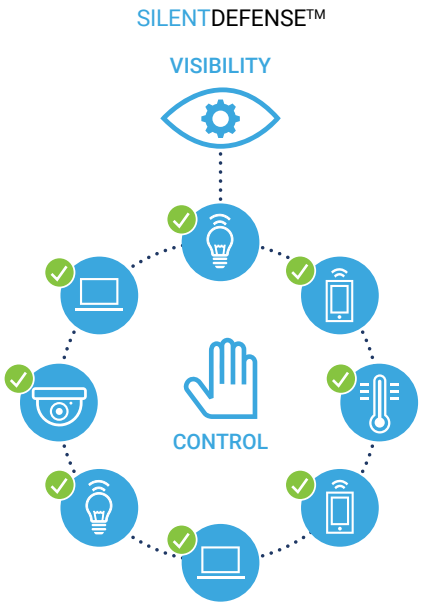
SilentDefense automatically collects a wide range of IoT device information, logging all configuration changes for security analysis and operational forensics. Discoverable details include:

- Network address
- Host name
- Vendor and model
- Serial number
- OS version
- Firmware version
- Hardware version
- Device modules' information

Threat Detection & Incident Response

Automate threat detection, containment and remediation with SilentDefense's alert investigation and response tools. Dashboards and widgets enhance user collaboration. Our interactive map identifies the source and spread of an incident. The rich data provided in our packet captures (PCAPs) supports root cause analysis and expedites effective, efficient response. The Enterprise Command Center (ECC) lets users zoom in on alerts from any of their multi-site or geo-distributed networks to analyze an incident in detail, including devices involved and context of the alert.

The IoT device visibility and control offered by SilentDefense are the cornerstones of a robust cybersecurity strategy, and our cyber resilience platform is used by enterprises worldwide to reduce business and operational risk with continuous, unified visibility and control of all IP-connected devices.



[1] Statista, 2016 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Ready to Empower Yourself with Complete IoT Visibility?

Schedule a demo to see how SilentDefense can help secure the IoT in your enterprise.

REQUEST A DEMO

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com