IoT Security

Proposition Overview

The influx of IoT devices presents huge opportunity but also poses a new set of challenges, particularly for security teams

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, and this number is only likely to grow. Organisations need these devices to enable more efficient operations, yet they cannot trust them. IoT devices pose immense cybersecurity risks as they are largely unregulated.

Block's IoT security solution, powered by Palo Alto, allows you to stop threats and control the risk of IoT, IoMT, OT, and Bluetooth devices on your network.

At a glance

- ✓ We'll give you complete device visibility with Machine Learning (ML) based discovery, helping you to accurately identify and classify all IoT and OT devices in your network, including those never seen before.
- ✓ We'll stop all threats headed for your IoT devices with the industry's leading intrusion prevention system (IPS), malware analysis, web, and DNS prevention technology.
- ✓ We'll help you to find all the information you need to quickly evaluate vulnerable devices, assess security compliance and initiate the next steps.

Problem solved

Combined with a ML-Powered Next-Generation Firewall (NGFW) platform, this IoT Security service 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.

Benefits

Turn unmanaged devices into managed devices and control the largest contributor to risk: unknown devices.

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

Improve operational efficiency with integrations across ITAM, SIEM, NAC, and more