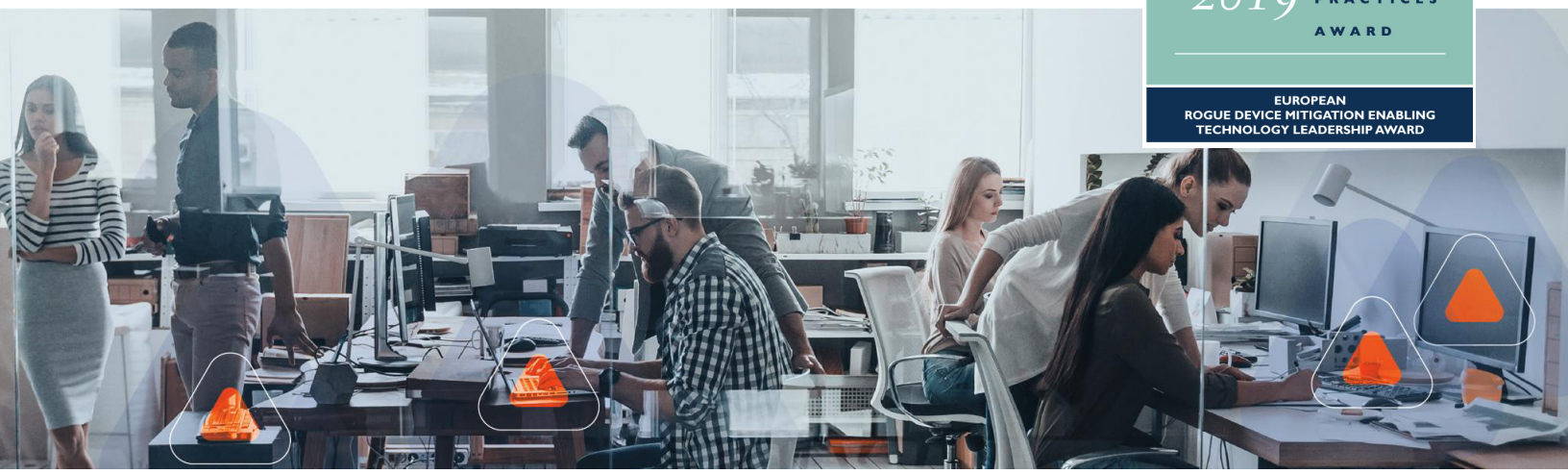
SEPIO SYSTEMS

FROST & SULLIVAN

2019 BEST PRACTICES AWARD

EUROPEAN ROGUE DEVICE MITIGATION ENABLING TECHNOLOGY LEADERSHIP AWARD



ROGUE DEVICE MITIGATION

They're Coming For Your Data. Stop Them Before It's Too Late.

A data heist can be easy: The attacker plugs a rogue device called a Packet Squirrel or a Plunder Bug into a wired network or connects a Rubber Ducky or USBNinja to a network workstation's USB port. Never heard of them? Hackers have, and such devices are easy to find or build. The rogue device then listens… hacks… gains access… and siphons critical business information right out of your network.

> *"Infected hardware devices constitute both an information technology and cybersecurity issue. The network visibility created by Sepio's solution is a critical component of any effective rogue device management solution."*
>
> *- Eli Grach, Aerospace & Defense Research Analyst, Frost & Sullivan*

The Problem With Rogue Devices

These vulnerabilities extend to any network where an adversary can gain access long enough to plug in the rogue hardware: Banks, schools, government offices, businesses, retail establishments, all can be compromised through an unlocked door. An unsecured jack in a reception area. An Ethernet switch in the data center.

Attacks also come from within: Nearly any malicious employee, partner, supplier or customer with access to your facility could surreptitiously plug malicious hardware into an unsecured port and launch supply chain attacks or succumb to inside threats.

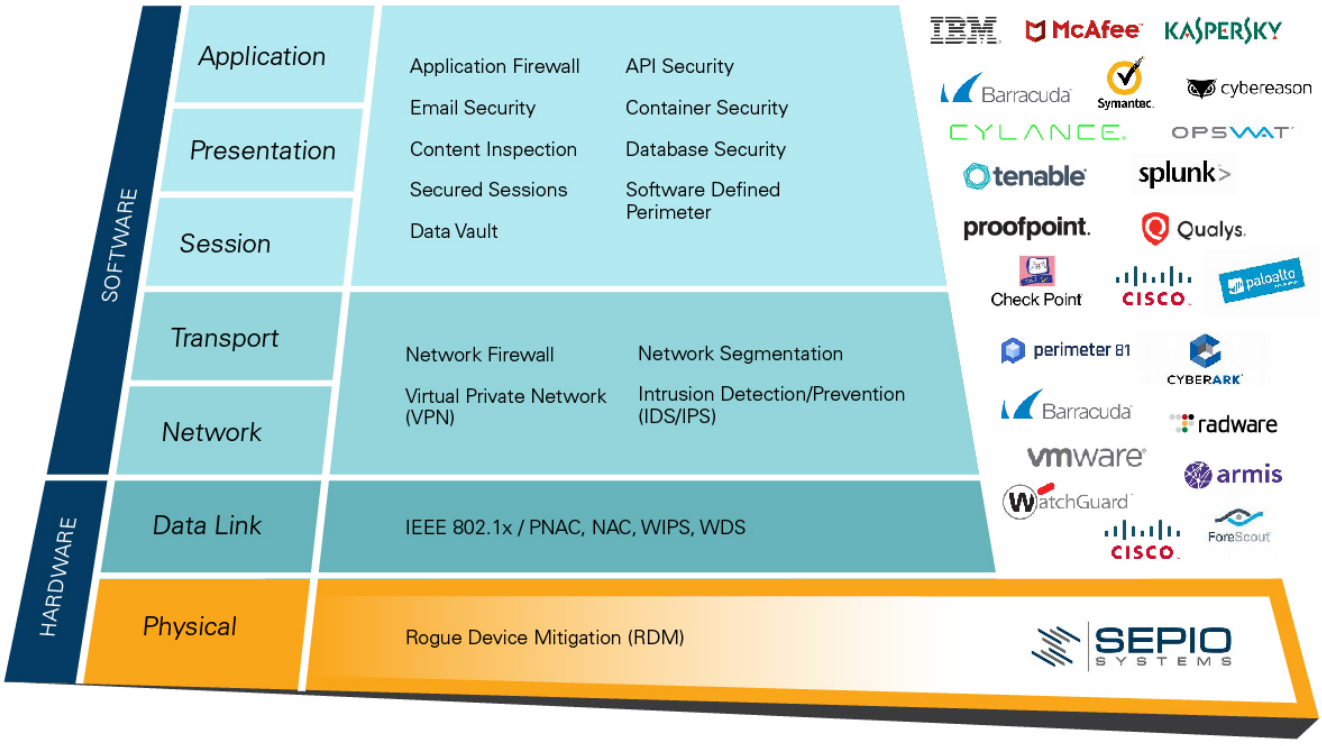
The good news: Many organizations have excellent network-protection and intrusion-detection systems, as well as network firewalls (operating at OSI Layers 3 and 4) and application firewalls (operating at Layer 7) with deep packet inspection.

The bad news: Such protections won't guard against rogue hardware, which taps into network traffic at Layer 1 – the Physical Layer – thereby flying under the radar of traditional security systems.

Mitigate Rogue Device Attacks

That's where Sepio Systems comes in, with three unique solutions that work together to stop attacks using rogue hardware.

- Sepio Network Security works at the Physical Layer, polling switches to analyze what's happening at that layer and detecting all rogue devices plugged into the Ethernet network.
- Sepio Endpoint Protection guards against rogue devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices.
- Sepio Prime orchestrates Sepio's solution, alerts or security threats, enforces policies and delivers risk insights and best practices recommendations.



Sepio discovers and inventories invisible hardware, analyzes hardware behavior and automatically block attacks. The software is augmented by real-time cloud-based intelligence that provides early warning of the latest malicious hardware and threat patterns. Sepio's SaaS-based security suite can be deployed on any physical or virtual environment in any combination of on-premises, private and public cloud.

Bad Actors Are Coming

Block rogue device attacks and stop the hardware-based data heist, with Sepio Systems. Request a demo at www.sepio.systems/schedule-a-demo.