SECURONIX™ | ARMIS™

SOLUTION BRIEF

Detect and Respond to IoT Security Threats With Securonix and Armis

Corporate networks have an increasing number of internet of things (IoT) devices on their network, even as the security team struggles to gain visibility into those devices.

Visibility into IoT devices is important because most IoT devices use outdated operating systems and security protocols with weak passwords, making them prime targets for attackers. Healthcare and manufacturing are especially vulnerable to IoT-based attacks. The variety of devices that can be exploited but which cannot be monitored using an agent is massive, and includes security cameras, printers, HVAC devices, smart TVs, Wi-Fi routers, and more.

Integrating Securonix Next-Gen SIEM with the Armis® Agentless Device Security Platform provides you with end-to-end visibility into your enterprise network, across IT, IoT, and unmanaged devices. Armis provides an agentless approach to monitoring and provides baseline device profiles for over 11 million distinct devices. Securonix leverages the asset inventory and alert data from the Armis platform for IoT analytics, compliance reporting, and adding contextual data for investigations.

The Securonix-Armis Solution

Armis is agentless and passive. The platform uses information from the Armis Device Knowledgebase – the world's largest cloud-based device knowledgebase - to evaluate the configuration and behavior of unmanaged/IoT devices on the network. This includes key asset information such as known vulnerabilities, configuration issues, and anomalous activities such as traffic on unusual ports, or excessive data transfer activity over the network.

Securonix ingests this configuration and behavioral data and correlates it with related data from other sources such as firewalls, endpoint detection and response (EDR), and email gateways. Securonix then utilizes advanced behavior analytics to detect threats and provide risk scoring. Threats are prioritized using the Securonix risk scoring algorithm, and data is retained for further analysis, forensics, and compliance.

Integrated response capabilities enable remediation actions for devices with detected threats, such as device shutdown or disconnecting from the network.

The combined solution enables a complete, holistic view of threats to the enterprise – including IoT and unmanaged devices – for end-to-end threat identification and response in a single solution.

Solution Benefits

- **Improve Threat Detection**
  Combine event telemetry from unmanaged devices with the rest of your network data to provide a holistic view and improve threat detection.
- **Decrease Overall Response Time**
  Respond quickly to threats using integrated SOAR, enabling automatic device quarantine for faster remediation.
- **Faster Search and Threat Hunting**
  Securonix analyzes IoT and unmanaged device events together with managed device data in order to provide historical search capabilities for threat hunting and fast live search for active threats.

Context-Driven Threat Modelling

The Securonix platform adds critical contextual data to ingested events such as MAC addresses (from Armis), user information (from the HR system), IP attributes, and multiple other data points. By correlating Armis asset data with data from other sources, Securonix enables you to take appropriate actions across the network, such as blocking beaconing traffic from infected IoT devices. Securonix's highly scalable and economical storage also enables the retention of Armis data for compliance and threat hunting.

Fast Threat Hunting for IoT and Unmanaged Device-Based Threats

Threat hunting on integrated Armis data is possible using Securonix SearchMore for fast search on historical data. This can help you find threats that already have a foothold in your network. Built-in live data feeds and searching capabilities enable you to also find new, active threats to your enterprise.

Conclusion

A stray digital camera with an exposed operating system on the network, or an executive's iPad that is running malware – both threats on unmanaged devices, and just as dangerous as any other threat. The Securonix-Armis joint solution helps you find such threats and act on them immediately. Compromised printers, vulnerable tablets, and poorly configured Wi-Fi routers – they can all be managed as part of your overall IT infrastructure using this joint solution.

Extend your cybersecurity perimeter to comprehensively include your unmanaged device footprint with Securonix and Armis.

Key Use Cases

- Ransomware detection
- Network recon/snooping detection
- Circumvention of controls detection
- Compromised asset detection
- Infrastructure abuse detection
- Covert channel data egress detection
- Anomalous network activity detection
- Account misuse/compromise detection
- Zero-day attack detection

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000