Secureworks

DATA SHEET

Managed iSensor with Advanced Malware Protection and Detection Technology

Protect Critical Assets with a Network Sandbox Enhanced IPS Solution

Network IPS can identify and block threats before they impact endpoints and users. Boost protection and enhance IPS with Advanced Malware Protection and Detection (AMPD) Technology. Network sandbox technology identifies more threats – even ones with little or no malware, or threats too new for IPS signatures to identify.

True Value Goes Beyond the Initial Purchase

An intrusion prevention system (IPS) is a critical component of your security defense, but achieving maximum value and effectiveness goes far beyond simply purchasing a product. IPS appliances must be managed and maintained with patches and upgrades. Alerts generated by an IPS device have to be monitored and analyzed. Rules must be assessed and adjusted to meet the ever-evolving threat landscape. In some cases, the best way to validate an alert is to detonate a suspicious file to confirm whether the intent is malicious or benign. These demands can burden your IT personnel, who may lack the time or expertise to maintain optimized IPS devices.

How Secureworks Helps

Our Secureworks iSensor™ IPS removes the burden of device or signature management, while helping clients eliminate malicious inbound and outbound traffic. This fully managed solution enables regulatory compliance, protection from the latest threats and vulnerabilities, and comprehensive reporting. As a 24x7 service, Secureworks augments your existing security team, eliminating increased in-house headcount. Our iSensor includes thousands of unique countermeasures developed by The Secureworks Counter Threat Unit™ (CTU™) Research Team, and unmetered support from our elite team of researchers, engineers, analysts and consultants working in our global Security Operations Centers (SOCs).

Client Benefits

- Expert management and support for administrative and maintenance activities
- 24x7 monitoring and alerting of security events
- Intelligence-enhanced threat protection, including thousands of unique countermeasures
- Identify threats in email and web traffic not easily identified via IDS/IPS signatures
- Reduce time spent investigating false positives
- On-demand security and compliance reporting
- Availability for advanced throughput and virtual environments

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Powerful Defensive and Blocking Capabilities

Our iSensor IPS allows you to detect, respond to and prevent security incidents on your critical assets. iSensor performs in-line deep packet inspection of inbound and outbound network traffic, using multiple integrated defense technologies to identify and block real security events requiring attention. Our iSensor provides:

- Scaling from 100–500 Mbps without replacing hardware, even as your performance needs increase
- An additional hardware unit that scales from 100 Mbps – 3 Gbps
- The ability to interconnect 10 Gbps networks on our 1 Gbps, 2 Gbps and 3 Gbps service offerings (maximum performance with a 10 Gbps interface is 3 Gbps

Optional Network Sandbox Capabilities

iSensor also offers unique, integrated, Deep Content Inspection™ network sandbox technology via our Advanced Malware Protection and Detection (AMPD) technology. With AMPD technology, suspicious files are detonated and analyzed in a Secureworks-hosted AMPD instance. Detonation clarifies intent, thus enhancing your ability to identify malicious activity. Deep Content Inspection looks more like a real endpoint, which thwarts many sandbox evasion techniques that are often built into malware. AMPD technology:

- Detects advanced and evasive threats in web and email traffic that may be overlooked by traditional IDS/IPS signatures
- Identifies new threats before IDS signatures are defined
- Reduces time spent investigating false positives
- Provides faster detection of new and emerging threats

The AMPD technology option is an elite layer of defense that can be added to iSensor.

Why it Matters

Extensive intelligence: iSensor uses countermeasures researched and created by our CTU team. Deploying this suite of countermeasures allows us to deliver protection quickly when a new threat is identified.

Increased efficiency: iSensor with AMPD Technology delivers unique network sandboxing technology without adding hardware or software.

Security expertise: Our elite team of security experts manage and monitor deployed iSensors on a 24x7 basis, freeing up your security personnel to focus on their business priorities. There is no need for you to hire, train and retain security personnel to monitor the device or to deal with management and maintenance.

For organizations with an existing VMware ESXi infrastructure, Secureworks provides a virtual iSensor that scales from 100 Mbps–1 Gbps by allocating more processing and memory utilization. This preserves rackspace for other critical assets, or deployment of additional iSensors.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.