Secureworks

SOLUTION BRIEF

Detect & Prevent Solution

The Challenge

As technology transforms the marketplace, thriving organizations are exposed to increased cyber threats. It's difficult to retain experienced personnel to investigate the mountain of alerts produced by today's security products and their assorted vendors. As the complexity of threats grows and threat actor behavior becomes more sophisticated, many organizations chase the latest threat trends, instead of achieving proactive security.

The Solution

The right mix of technology, human intelligence and processes provide organizations with the right solution: one that bolsters visibility throughout the environment, uses threat intelligence and correlation for the right context, and provides the elements of foundational security backed by vast security expertise.

Foundational security is a fundamental aspect of protecting data and devices. Secureworks Detect & Prevent solution establishes the foundation your organization needs. Accelerate your detection and prevention capabilities by combining Secureworks iSensor™ proprietary IPS and advanced security monitoring. Fulfill basic compliance requirements and establish a solid security posture to produce unified security visibility across your environment.

Finding the Right Fit

Organizations have plenty of options when it comes to security, but it's not always easy to determine which is the best fit for the unique needs and customer base of the organization. This especially is true for companies who have little or no security expertise on staff. These organizations are challenged to find a complete solution that delivers basic foundational security. The marketplace is full of all kinds of point security products and services, but it can be difficult to determine what comes out of the box and what remains to be customized or managed by your limited resources.

A Holistic Solution

Secureworks Detect & Prevent solution boosts protection of your data and devices by providing our iSensor IPS technology. iSensor monitors across your infrastructure — including your existing firewalls, next generation firewalls and any third-party IDS/IPS products — plus server monitoring and advanced analytics on your Windows servers. This holistic solution brings together several of our foundational services to form a comprehensive security offering for organizations who do not have the skills and resources to do so effectively.

Secureworks provides nearly two decades of experience in helping protect clients of all sizes in a digitally connected world with a constantly evolving global threat landscape. We understand how threat actors operate and how best to protect our clients, producing the better visibility, decreased noise and complexity, and speedier defenses needed to stay ahead of emerging threats.

Better Visibility

Secureworks Detect & Prevent solution helps you eliminate blind spots by increasing the level of visibility throughout your environment. The elements of our solution not only refine your view inward to internal operations, but outward to the threat landscape. We understand threat behaviors, and the who, what, why, when, where and how of potential attackers, so we can outsmart and outwit them.

The Detect & Prevent solution is flexible as you change devices and scales to grow with your organization as it expands.

Client benefits include:

- Maximizes your ROI on existing security investments (e.g., NGFWs)
- Fills the gap for hard-to-find security expertise
- Instant time-to-value
- Provides updated threat intelligence with actionable remediation guidance
- Automates event analysis through correlation and machine learning

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

Decrease Noise and Complexity

Secureworks helps you pinpoint malicious and suspicious activity in the sea of data that often overloads security teams. This context helps prioritize what activity represents a true threat and what represents just harmless noise. You can learn from the collective knowledge of past and current threat activities worldwide, given the network effect of Secureworks serving 4,400 clients in every major industry.

Faster Defense

The combination of our machine learning and human expertise provides you with the needed perspective to decide quickly what needs attention first. We update our iSensor with countermeasures from the Secureworks Counter Threat Unit™ (CTU™) and from threat activity observed across our client base. We provide the recommended course of action as soon as you open a ticket, based on our vast experience in serving clients of all sizes.

Taking the Next Step

The Secureworks Detect & Prevent solution delivers the next step for you: expanded security capabilities across your environment, bolstered visibility throughout your network and out to the endpoint, additional threat intelligence to more places, more correlated events for better outcomes, and advanced user behavior analytics that delve beyond basic server monitoring.

The Secureworks Detect & Prevent Solution Includes:

- **iSensor:** The iSensor includes thousands of countermeasures developed by the CTU, and unmetered support from our elite team of researchers, engineers, analysts and consultants working in our Security Operations Centers (SOCs).
- **Security Monitoring:** The Detect & Prevent solution extends security monitoring to your existing firewall, next generation firewall and third-party IDS/IPS devices. This enhances your level of visibility and casts a wider lens on potential entry points adversaries may use to enter your environment.
- **Server Monitoring:** Secureworks proprietary Red Cloak endpoint sensor protects your Windows servers, while native logs are reviewed for malicious traffic.
- **Secureworks Counter Threat Platform™ (CTP) and Counter Threat Appliance (CTA):** The CTA resides in your environment and connects to our CTP. Events of interest undergo initial analysis on the CTA. Those events remaining in question or known to represent a threat then are sent to CTP – which resides in our SOCs – for more advanced correlation and, if needed, investigation by our security analysts.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the 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.™

Secureworks®