

Managed IDS/IPS

Bolster Your Security With Indispensable, Fully Managed Tools for Monitoring and Threat Remediation

Managing Constant Changes

Intrusion detection and intrusion prevention appliances are a critical component of a company's security environment, but buying a device is just the first step. Getting the most out of an IDS/IPS investment goes beyond just purchasing a product, given the level of work required to keep devices updated as the global threat landscape changes. An organization's needs change, requiring adjustments of configurations and signatures. Organizations without the staff expertise to keep IDS/IPS devices updated often struggle to get the most value out of their cybersecurity investments.

How Secureworks Helps

The Secureworks IDS/IPS solution provides 24x7 operational administration, monitoring, and maintenance of intrusion detection and intrusion prevention devices. Our Managed IDS/IPS service uses proven practices to ensure appropriate network access, while preserving the availability, integrity and privacy of information. Our security experts monitor IDS/IPS health events and traffic logs in real time, identifying and responding to threats before they impact critical assets.

Secureworks supports the traditional model – where clients have limited or no administrative privileges for the managed IDS/IPS – and a co-managed services model. In the co-managed model, clients retain ownership and administrative rights to IDS/IPS devices to the extent they prefer.

Accelerate Your IDS/IPS Investment with Expertise and Threat Visibility

An effective intrusion detection and intrusion prevention solution monitors the activity in your network, identifies events that may pose a security risk, stops the events and alerts an organization that something has happened. Secureworks Managed IDS/IPS solution provides administration and monitoring of a client's intrusion detection and intrusion prevention infrastructure on a 24x7 basis. Backed by the power of The Counter Threat Platform™ (CTP), which uses predictive technology, holistic threat intelligence, and automated action, Secureworks is able to detect events of interest and perform further investigation to determine if the event represents a valid security threat.

Client Benefits

- Device provisioning and deployment
- Performance, availability and policy management, upgrades and patch management
- Real-time security and health monitoring, and expert response to threats and health issues
- Secureworks Counter Threat Unit™ (CTU™) intelligence-enhanced threat protection where supported by the device

Our global threat visibility comes from monitoring more than 4,400 clients, and our powerful correlation technology and machine-learning capabilities provide Secureworks with impactful, immediate analysis. Secureworks partners with leading IDS/IPS vendors to evaluate features and software before general release to the public.

The Secureworks Managed IDS/IPS solution includes policy management, device and policy troubleshooting, security event monitoring and alerting, device availability monitoring and alerting, and device software maintenance. As vendors release policies and make recommendations on signatures, Secureworks updates devices we are managing. Secureworks also performs regular device availability checks, begins troubleshooting activities if a device does not respond, and implements IDS/IPS change requests.

Our Client Portal gives clients full visibility into their security environment, helping to identify and determine risk and demonstrate compliance. The Client Portal allows clients to drill down into specific events, generate standard and custom reports, schedule reports in advance, and engage the security analysts in our SOCs through a powerful ticketing system. The Client Portal's mobile app provides this information on the go.

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.™

Why it Matters

Reduce management and monitoring costs: Our Secureworks solution removes the burden of the administrative tasks of updating and maintaining a client's IDS/IPS devices, freeing up resources to focus on other business objectives.

Protect systems and data 24x7 without increasing in-house headcount: Secureworks provides around-the-clock monitoring and management of your IDS/IPS environment, eliminating the need for clients to hire, train and retain qualified security personnel.

Satisfy compliance regulations: Clients easily can generate reports from The Secureworks Client Portal for technical audiences, management and auditors. Consolidated reports can be generated, providing audit trail documentation.

Flexible management approach: Secureworks delivers its Managed IDS/IPS solution in either a co-managed or fully managed fashion.

Impactful intelligence: Our CTP processes more than 250 billion events daily across our client base, and our Counter Threat Unit research team scours the Internet to produce a globalized view of the rapidly changing threat landscape.

Solution Features

- 24x7 real-time security event and device health monitoring
- Unmetered support from our certified security and Tier 1 product support from device management experts
- Configuration and implementation support; policies available for review in The Secureworks Client Portal – Powered by the Counter Threat Platform™ (CTP)
- Upgrade, change and patch management
- Intelligence-enhanced threat protection via the CTU
- Custom IPS signatures and countermeasure feeds where available



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