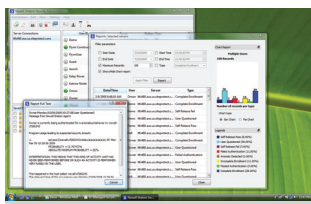


Shalom Security Platform v3.0



Vendor Nowell
Price \$4.99 per user per month
Contact www.nowellgroup.com

Nowell Shalom Security Platform is a cloud-based security as a service (SaaS) offering that is intended to protect against malicious insiders and impostors stealing information and committing fraud inside the corporate network. The offering is geared to defend against insider threats, identity theft and internal fraud.

The tool is an anomaly detection system that looks out for suspicious activity by computer users. It offers an intelligent authentication mechanism that looks for a user who exhibits suspicious behavior. It detects suspicious activity on the network by monitoring user accessed remote hosts and ports. Shalom also detects user anomalies with respect to hardware-specific variables, such as processor architecture, processor level, processor mask, OEM I.D., minimum/maximum application address and memory page size.

Once identified as suspicious, a user is reported to the central console and then presented a set of challenge questions to validate their identity. If the challenge questions are answered correctly, the installed agent will allow the user to continue to reside on the network. If

the challenge questions are answered incorrectly, the user is logged off the network.

The management and monitoring is provided as a cloud solution. There is an agent that is loaded on the individual hosts. Automated deployment options are available for attended or unattended agent installation. The agent is required to communicate with the hosted servers. This communication appeared to work well without noticeable latency.

We found the reporting to be somewhat lacking compared to the other solutions we reviewed. Email alerting on events is supported and was easy to configure.

This offering can provide an additional level of user identity management. We liked the concept and, properly managed, it can provide an additional level of protection. As with all anomaly detection systems, it has to rely on a good baseline of "normal" behavior.

SC MAGAZINE RATING	
Features	★★★★☆
Ease of use	★★★★☆
Performance	★★★★☆
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★☆
OVERALL RATING	★★★★☆
Strengths	Provides an extra layer of user identity management.
Weaknesses	Reporting; relies completely on anomaly detection of learned environment.
Verdict	Nice addition to a layered identity management program or as a standalone identity management solution.

IDS/IPS



Vendor SecureWorks
Price \$1,000 per month
Contact www.secureworks.com

SecureWorks provides real-time, 24/7 monitoring and analysis of host logs, leveraging its proprietary Sherlock Security Management Platform. The company's log monitoring service can capture, correlate and analyze log data from virtually any critical information asset.

The offering falls into the log monitoring and security event management (SEM) segment. Using its proprietary filtering and advanced correlation and logic engine rules, the Sherlock Platform analyzes all logs and alerts in real time and presents events of interest for assessment and response to a team of SANS GIAC-certified intrusion analysts in the company's counter-threat unit. The analysts attempt to identify malicious activity or policy violations. There are no agents to load on client-side equipment. Logs and event data can be transferred to the SecureWorks servers via several supported methods.

Events are reported via the portal in real time, providing clients with full visibility into security issues and policy violations within their environment. A full-ticket tracking system is available

for managing client requests and monitoring progress on various monitored situations. The portal also features asset-based reporting allowing users to easily view the security and compliance activity across their environment, as well as demonstrate compliance with various regulatory requirements.

As with most managed log monitoring solutions, client data is stored in a shared repository. SecureWorks can provide log detail back to clients in XML format for use in other analysis tools or for incident response.

We were impressed with both the canned and custom reporting capabilities. The user dashboard is fully customizable and easy to use. Alerting is very granular and based on a per asset basis, i.e., set a phone alert for a critical asset versus send email for a less critical asset. There is also an option for keeping the assets up-to-date by conducting user-configured network scans. We liked what we saw.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★☆
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★
Strengths	Mature log management offering; skilled analyst reviewing logs and event data.
Weaknesses	Not many. If we have to pick something, it would be support for a larger array of native log formats.
Verdict	If you're like most companies and don't review your log data in real time, you should consider this solution.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.