

Cost/benefit analysis is still a clear challenge with managed services of intrusion detection (IDS) and intrusion prevention systems (IPS), says **Peter Stephenson**.

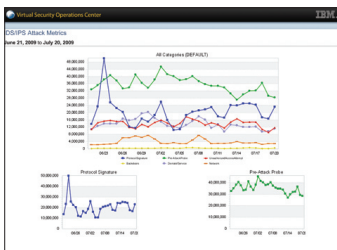
There are several aspects to managed security services that have evolved over the past 10 years. A decade ago, managed security services were restricted to applying the output of sensors to some sort of collection and display device. Usually this took the form – in the beginning, anyway – of a homoge-

neous system allowing only a single sensor type. The first evolution of that approach was the use of Snort sensors to overcome the problem of feeding the collector.

It was not long, though, before we began to see the development of translators that could take many of the most popular data sources and

feed them into the collector. This forced the collector to become a correlator, taking the pressure off of the human operators and placing it on machines. When that happened, the race for the market was on. Today's refinements are a direct result of the development of compact, high performance log correlators.

Managed Protection Service



Vendor IBM ISS
Price starts at \$575/month
Contact www.ibm.com

The IBM Managed Protection Service combines a full security monitoring staff with security monitoring devices to manage, monitor and respond to



security threats on a customer's network. This service includes management and monitoring of features, such as firewall, IPS, anti-virus, anti-spam, content management and VPN.

The service, based on IBM ISS Proventia, is solid, as is the underlying technology. The collection of events from security operations centers (SOCs) around the world helps IBM correlate global and regional events, as well as improving reliability of its customer-level services.

While the service is totally managed and monitored, users can access a web-based management dashboard where they can easily find information on events, as well as reports and logs from various security devices on the network. Users can also view real-time information on device status via this dashboard. We found the dashboard to be intuitive and easy to navigate.

All the log and event data from a customer's security appliances are sent securely across the internet to one of IBM's SOCs where both automated and human correlation techniques are applied by analysts to detect and respond to threats facing the customer's entire network.

A portal user guide is provided. This PDF includes many screen shots and information on how to use the web-based portal, as well as a walkthrough of the various menus available.

IBM Managed Protection Services are provided 24/7 with client access to the eight global SOCs and customer portal. The service is offered at three levels: standard, select and premium. Each of these

levels offer various response times and access to features, such as onsite support, access to an engineer and update services.

At a cost of \$575 per month, we find this service to be an excellent value for the money. The service combines all the capability of the IBM ISS Proventia appliance into a managed security service that can be completely managed and monitored with little need for customer intervention.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★
Strengths Full-scale UTM capability in a managed service with good analyst involvement.	
Weaknesses None that we found.	
Verdict A top-notch services suite based on proven technology and infrastructure. We make this one our Best Buy.	



A top-notch services suite based on proven technology and infrastructure. We make this one our Best Buy.

Peter Stephenson

www.ibm.com/services/us/iss