

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

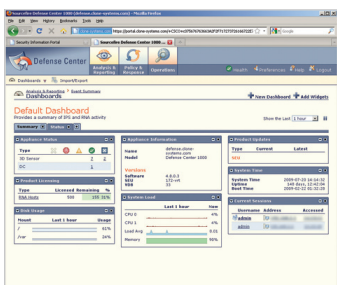
There are several aspects to managed security services that have evolved over the past 10 years. A decade ago, managed security services were restricted to applying the output of sensors to some sort of collection and display device. Usually this took the form – in the beginning, anyway – of a homoge-

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.

Clone Guard Managed IDS/IPS



Vendor Clone Systems
Price \$525/month
Contact www.clone-systems.com

The Clone Systems Clone Guard Managed Security Suite provides protection from malicious threats against VoIP, web or customized applications. This service detects, logs, prevents and reports suspicious, malicious or unauthorized access to critical network resources.



Deployment is done by installing a managed appliance at the customer site. This uses Sourcefire as its backbone and can be integrated with other network devices. Once deployed and configured, administrators can access the web-based

portal to manage the appliance or view and print reports. Both the portal and the web GUI are intuitive and easy to navigate. Customers also have access to the Clone Systems Enterprise Vulnerability Scanning Service, which they can use to run full-scale real-time remote vulnerability scans against network assets.

The Clone Guard service provides experts who monitor data-networking environments from the Network Operations Security Center. The use of advanced monitoring tools allows them to reliably separate actual security threats from false positives.

Documentation is a PDF installation guide, which includes step-by-step instructions on installing the preconfigured sensor into the network, as well as a custom network diagram for easy reference.

All Clone Guard Managed Security Services include 24/7/365 phone and email technical and alert support as part of the service via an SLA. The SLA includes four-hour hardware replacement on complete failure, notification of IDS hardware/software failure within 15 minutes of detection,

and notification of major events within 15 minutes of detection. There is also a short FAQ section available on the vendor website.

At a cost starting at about \$525 per month for hardware, software and monitoring, we find this product to be an excellent value for the money. With this service, not only do customers have their network monitored 24/7, but they also have access to vulnerability scanning tools and various dashboards full of monitoring data.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★
Strengths	Full-scale managed IPS service with included vulnerability scanning.
Weaknesses	None that we found.
Verdict	Excellent service with a lot of capabilities. We rate this one Recommended.



“Clone Guard Managed IDS/IPS offers excellent service with a lot of capabilities. We rate this one Recommended.”

Peter Stephenson



Clone Systems, Inc.
 US: Corporate Office
 1835 Market Street, Suite 535,
 Philadelphia, PA 19103, USA
 Tel: +1.800.610.2833
www.clone-systems.com