November 19, 2001

Technology Migration to Intrusion Protection Systems

Michael Rasmussen

Catalyst

Analyst research

Question

There appears to be a new breed of intrusion detection technologies aimed at protecting the host and/or application itself — what is Giga's analysis on these technologies?

Answer

There has been a lot of hype around intrusion detection systems (IDS) during the past few years. Many organizations adopted these technologies not understanding how they work or the management overhead they require. One of the most flawed assumptions has been that they are protection devices — in the past this has been false or they offered only a rudimentary level of protection.

This appears to be evolving as new technologies are being purchased that offer intrusion protection as well as detection capabilities. In reality, a new market segment is opening up for intrusion protection systems that protect the host operating system and/or application.

Intrusion protection technology is more closely related to host IDS as opposed to network IDS, and in many ways it can be seen as a submarket in the overall host security market. While network IDS remains fairly stagnant in development — most development is in management capabilities and developing fast appliances — technologies to secure host operating systems and applications are abounding.

The two basic approaches to host intrusion protection involve:

1. **Operating system protection** — This involves shim technology at the kernel level that basically puts a software firewall around the operating system kernel to detect and prevent security incidents. Vendors in this space include **Entercept** and **Okena StormWatch**.
2. **Application protection** — This protects an application residing on a host by placing a very specific application firewall in front of the application itself on the host. Vendor offerings in this space include **Sanctum**'s AppShield, Entercept's Web Server Edition and **eEye Digital Security**'s SecureIIS.

Intrusion protection applications offer more value by protecting a host as opposed to pure detection capabilities. Why only detect when you can provide protection as well? Vendors in this space are providing products that protect systems and applications beyond the standard detection capabilities of the past.

Deployment of intrusion protection technologies comes at the cost of complexity. Organizations deploying them need to have a high level of understanding of the issues surrounding application and operating system protection to get the most value out of them. Improperly configured systems can become unstable and not function properly, while the properly configured system can represent a nearly impenetrable secured fortress.

Organizations looking at the adoption of intrusion protection technologies should selectively deploy them on critical hosts in their environment that have a high susceptibility to vulnerability and/or compromise. Only after these hosts have been adequately secured, with an understanding of the technology gained, should these solutions be moved to other systems within an organization.