StormWatch ROI:
A Single Intrusion Prevention Deployment for Desktops and Servers.
Avoiding the Signature Update Race

Substituting Multiple, Redundant Technologies on Servers and Desktops

StormWatch is a host-based intrusion prevention solution that provides protection for both servers and desktops. Being able to protect both sets of hosts from their specific attacks as well as blended or multi-faceted attacks (like Nimda which targets both servers and desktops), obviates the need for distinct and redundant technologies that are being considered or are currently deployed.

The StormWatch solution allows corporations to consolidate many security functions or solution into one product, from one vendor. These solutions include: host-based intrusion detection and prevention, file integrity monitoring, NT event auditing, distributed or personal firewall, and malicious mobile code protection.

Deploying StormWatch allows an enterprise to simplify its security strategy, alleviate the management burden of multiple products and reduce the annual software and maintenance license fees associated with these products

Escaping the Signature Update Race

Signatures and virus definitions are the lynch pins of Intrusion Detection and AV systems. Inherent in this reliance not only is the reality that you're basing your security controls on only known vulnerabilities but also the administrative and financial burden of implementing and maintaining these signatures on a regular basis. The only way to avoid this 'update race' is to proactively secure your applications so intrusions are prevented not just detected, even if they aren't known today.

IDS and AV products are entirely dependent on signature updates. These signature updates are delivered by vendors either on a periodic basis, or as and when the new exploit is discovered. For example, an 8-hour turn around time is the standard for intrusion signature updates. Some vendors send out updates only on a monthly basis. Whether a company needs its users or administrators to download updates, or they utilize a 'live update' technology to an internal signature server, great reliance is placed upon the system user (even 'live update' requires a user to log into a machine while it is connected to the network).

While the live update architecture lessens the time lag between a vulnerability and the availability of its fix from the vendor, most security conscious companies thoroughly test any new signature within their labs before deploying it on critical production systems. This testing can take on average 1-2 days to ensure compatibility with critical systems and that the fix for a specific attack does not inadvertently block good activity from executing. There is an administrative cost associated with these tests, not to mention the exposure while systems remain 'un-updated'.

Managing Alerts and False Positives

Pattern and signature matching technologies are prone to a high number of false positives and false negatives. In other words, the signatures that they deploy generate false alarms that indicate possible malicious activity when, in fact, appropriate host and network behavior is taking place. These false

positives crowd administrative consoles, reduce the effectiveness of the product and the administrator and force the admin to respond to unwarranted security alerts.

Because StormWatch does not deploy signatures but focuses on actual application behavior it is not subject to a false positive rate. Furthermore, correlation is deployed at both the agent and enterprise levels for industry-leading accuracy in prevention decisions. Events are still sent to the console, however they are far fewer and reflect legitimate events that the administrator has elected to be notified on.

> *"In addition, IT managers at companies of this size would have to manage more than 500,000 log file entries every day. Each firewall generates an average of 200,000 to 300,000 log entries and 20 alerts per day, according to the Activis study. Likewise, each network sensor will generate between 20 and 50 console alerts per day, and each server sensor will generate between one and 20 console alerts per day, the study found."*
>
> ***ComputerWorld, November 30th 2001***

Security for applications in between service packs

As recent attacks like Code Red and Nimda have shown, applications remain vulnerable even when security patches have been released (sometimes months before). These recent intrusions show the inability of even the most dedicated admins to keep pace with the hot fixes and patches that are released on all their servers (There were 14 IIS patches in 2000).

> *"There are a lot of problems with penetrate and patch. One is that the patches are put together so quickly that they have their own security holes. They introduce more problems than they fix. The other is that most systems administrators ignore patches and don't apply them. The reason is that their stuff just barely works, and they don't want it to screw up."*
> ***CNET News, November 28th 2001***

An application-centric approach to security like StormWatch does not absolve admins from ever having to install patches on their servers but does allow them to protect their hosts until a well–tested vendor server pack is released that aggregates all the hot-fixes for a period of time. The release of service packs is done on a more measured, less frequent and less reactive basis.

> *"The number of required security patches and updates to security products during the past 12 months has so overwhelmed IT managers at most companies that the process now places network security at greater risk, a new study concludes.*
>
> *The study, conducted by U.K.-based managed security service provider Activis, a subsidiary of Germany-based Articon-Integralis AG, found that security managers at a company with an IT infrastructure consisting of only eight firewalls and nine servers would have had to make 1,315 updates to those systems in the past nine months alone, equal to five updates per working day. That number is based on the total number of updates and patches released during that time frame by some of the major software and security vendors."*
>
> ***ComputerWorld, November 30th 2001***

The ROI of Preventing Intrusions and Subsequent Losses

What can't be assigned a cost until it is too late is the cost of damage caused by the new and unknown attack that signatures do not prevent against. If historical precedence can be trusted, vulnerabilities such as those recently reported on IIS Web servers or the proliferation of viruses such as ILOVEYOU and Anna Kournikova have resulted in billions of dollars of losses associated with user downtime, loss of proprietary information, loss of reputation, and the cost of rebuilding systems.

This is not idle use of Fear Uncertainty and Doubt over security risks because the CSI survey bears witness that 85% of companies who responded reported some sort of intrusion in the past year, despite deployment of traditional security solutions. The costs of these intrusions will vary from company to company but the following facts are worth considering when evaluating your level of exposure:

- The Computer Economics Survey of 2001 found that the following attacks wreaked the following estimated worldwide damage:
  - Nimda $635 Million
  - Code Red $2.62 Billion
  - SirCam $1.15 Billion
- Fortune 1,000 companies lost more than $45 billion from the theft of proprietary information in 1999, according to a study released by the American Society for Industrial Security and consulting firm PricewaterhouseCoopers.
- "2000 Computer Virus Prevalence Survey", ICSA.net
  - Including hard and soft dollar figures, the true cost of virus disasters is between $100,000 and $1 Million per company
- 186 companies in the CSI/FBI survey 2001 reported losses of $377,828,700. An average of $2,031,000.

Conclusion

Implementing a proactive security solution like StormWatch provides a quantifiable return on investment because:

- Redundant, duplicate technologies can be substituted or replaced on the server and desktop
- No signature update burden
- No exposure between signature updates
- No false positives and event management burden
- Less downtime

Your systems are protected against the new and unknown attacks that signature-based products can't defend against; these attacks being the most damaging in terms of system down time, loss of reputation and proprietary information.

To assess the ROI that StormWatch can bring to your environment, request the StormWatch ROI calculator from your OKENA representative

71 Second Avenue, Waltham, MA 02451
Tel: 781-209-3200 Fax: 781-209-3199
E-mail:info@okena.com

www.okena.com

6905 Rockledge Drive, Suite 600
Bethesda, MD 20817
301-896-9388