

Cool Vendors in Infrastructure Protection, 2008

Gartner RAS Core Research Note G00156078, Ray Wagner, Peter Firstbrook, Arabella Hallawell, Lawrence Orans, Greg Young, Neil MacDonald, John Pescatore, 4 April 2008, R2705 10102008

Chief information security officers (CISOs) and other security decision makers should be prepared to consider innovative, new infrastructure protection vendors. Their products will not necessarily be appropriate for every enterprise, but they point to new directions in their market spaces.

Key Findings

- Significant changes in the enterprise technology and threat environments, including the growing use of IP telephony and consumer devices, are driving innovative new approaches to infrastructure protection.
- Endpoint protection – offered in platforms and by point solutions – is an increasingly important enterprise security concern.

Recommendations

- Be prepared to consider innovative new product and service providers – including Gartner's cool vendors – when looking for answers to infrastructure protection problems.
- Do not base product or service implementation decisions entirely on technological innovation, but also on real-world workability and vendor capability.

ANALYSIS

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

1.0 What You Need to Know

The cool vendors in infrastructure protection that Gartner has chosen for 2008 represent the leading-edge providers in technological innovation in many key security areas. These four vendors may not offer appropriate solutions for every enterprise's needs, but CISOs and other security decision makers should keep their offerings, and the changes in enterprises' business and threat environments they represent, on their "radar screens" in the coming year. Gartner's security analysts have identified cool vendors in three other market segments, as well.

2.0 Bit9

Cambridge, Massachusetts (www.bit9.com)
Analysis by Arabella Hallawell and Neil MacDonald

Why Cool: Bit9 is one of several vendors offering point solutions for application control – essentially the enforcement of whitelists and blacklists of applications allowed for or blocked from execution within an endpoint-computing environment. Application control will become increasingly important as a means of malware protection, because signature-based antivirus tools are increasingly limited in their ability to detect many new “flavors” of malware, or to detect them in a timely fashion. Gartner clients are reporting higher infection rates at the desktop, and are relying on e-mail security and Web security gateway solutions to fill the gaps temporarily. Today, application control supplements traditional antivirus protection. In some environments, where tight restrictions are placed on the downloading and execution of unknown code, the Bit9 Parity solution has replaced traditional antivirus protection.

Application control – like any host-based intrusion prevention system (IPS) that depends on the management of rules – can create significant IT management burdens if it is poorly implemented. Bit9 differentiates itself from its competitors by focusing on making the management of whitelists and blacklists less burdensome for IT departments. Most notably, Bit9 has built a vast repository, Global Software Registry (formerly called Bit9 Knowledgebase), that catalogs “known good” and “known bad” applications and files, and serves as the policy enforcement center for Bit9 Parity. An enterprise can use this database to determine whether an executable it does not recognize is known to be good or bad. Furthermore, the Bit9 Global Software Registry can be licensed to security and configuration management and software asset management vendors whose offerings could be improved by its data feeds.

Bit9 has also introduced other innovative ways of managing application whitelists and blacklists. Applications that have been digitally signed by a known vendor or an enterprise’s own IT organization can, for example, be whitelisted automatically. Similarly, applications that have been installed from a trusted file share (for example, a file server) can be automatically whitelisted. Moreover, Bit9 is able to group dynamically linked library and executable files logically into application groups, simplifying the identification and approval process.

Challenges: The core function of whitelisting and blacklisting applications is a commodity – Microsoft, for example, provides this capability using Group Policy Objects within Windows domains – so Bit9’s primary differentiation lies in its automation capabilities, and in Global Software Registry in particular. Bit9, like other small vendors of point solutions for endpoint security, faces challenges in going after the “incremental security dollar” in a market dominated by the traditional antivirus providers. Furthermore, the antivirus providers, including McAfee, Symantec and Microsoft, will likely build out their own application control capabilities as part of broader endpoint protection platforms (EPPs). Some desktop management vendors, such as Altiris (which was acquired by Symantec in 2007), offer alternative approaches.

Several vendors (WhiteCell and Solid Computing) have exited the application control market. A key reason is that for most enterprises, application control techniques supplement, rather than replace, antivirus tools, and the EPP market is a difficult one to enter. This market overwhelmingly favors incumbent desktop players and offers comparatively low growth rates and margins.

Finally, Bit9 addresses only the Windows environment, and because its solution uses “kernel hooking,” it has been slow to support Windows Vista, although Gartner expects support to be announced shortly.

Who Should Care: Information security and IT operations professionals share an interest in application control solutions, which provide security and operational benefits. From a security perspective, antivirus and antispymware solutions do a poor job of protecting enterprises against malware they have never seen. Application control solutions can help to fill this gap, and can help to protect enterprises against end users who unwittingly introduce malware by opening e-mail attachments and downloading unknown code from the Internet. From an operations perspective, tighter control of endpoints helps to reduce the demand for end-user support and reimaging calls. Enterprises seeking to more tightly control which applications can run on end-user systems should consider Bit9 as part of a layered defense, in-depth endpoint security strategy, along with the application control capabilities of their incumbent antivirus EPP providers.

3.0 Damballa

Atlanta, Georgia (www.damballa.com)
 Analysis by *John Pescatore*

Why Cool: Threats continue to evolve, not only in their motivations, but also in the mechanisms they use to breach enterprise defenses. Targeted, financially motivated attacks have become the most damaging, and the use of targeted malware downloads has become a key part of these attacks. In particular, multiuse attacks that trick end users into installing generic malware downloaders that are later used to install malicious payloads have proved to be at the root of many successful attacks. This type of attack – commonly called a “botnet” – purposely aims to escape detection, and the compromised hosts can be “rented out” for many different classes of malicious use.

Damballa has developed a number of algorithms, data collection points and analysis capabilities to detect the operations of targeted malware, such as that employed by malicious botnets, to provide indications that PCs have been compromised by malicious software and to deliver intelligence on inappropriate actions that compromised PCs may have taken. Their offerings include a “security as a service” option that relies entirely on Internet-based monitoring, internal monitoring sensors that can detect internal attacks launched by PCs compromised by malicious software, and a “demilitarized zone” deployment option for the detection of external attempts to communicate with compromised PCs and download attack software. These attacks typically use custom executable payloads and advanced techniques to mask or change command-and-control sites, so Damballa’s algorithms and added analysis do not rely on signatures of executables or simple updates to lists of “dirty” URLs or IP addresses. Damballa’s combination of enterprise visibility and Internet visibility can provide early warning of the malicious “rallying” activity that often precedes attacks.

Challenges: Botnets represent a rapidly growing delivery mechanism for targeted attacks, but the real threat lies in the payload – the malicious executables. The mainstream antivirus and IPS vendors have been slow to introduce capabilities for detecting and blocking targeted malware, but many of them are now developing these capabilities (as are some of the more mature startups, such as Avanti and FireEye). Web security gateway vendors also provide some capabilities for blocking communications to more-static botnet command-and-control centers. These vendors present competitive challenges to Damballa.

Another challenge lies in the fact that the damage caused by bot-compromised hosts is frequently aimed at other enterprises, so those with the compromised hosts may not have a strong incentive to make investments in finding and removing bot clients – until they are hit by an internal attack using the compromised PCs. Damballa is strong on detection; however, it does not provide remediation or cleanup capabilities. Yet, its knowledge base contains details on the file and registry changes that must be undone to restore a compromised host. Damballa will need to broaden its capabilities to detect targeted attacks beyond botnets, or seek partnerships with other vendors to expand beyond its niche target market of early security technology adopters.

Who Should Care: Damballa’s offerings should be evaluated by CISOs and other security managers with security-conscious enterprises, Internet service provider infrastructure managers concerned with the Directory Naming Service and bandwidth impact of bot-compromised hosts, and managed security service providers seeking to extend their security-as-a-service offerings.

4.0 Palo Alto Networks

Alviso, California (www.paloaltonetworks.com)
 Analysis by *Greg Young*

Why Cool: Next-generation firewall maker Palo Alto Networks’ management team comprises founders or former managers of companies such as Bay Networks, Blue Coat Systems, Check Point Software Technologies, Juniper Networks and NetScreen. The company is backed by major venture capital firms, including Sequoia Capital and Greylock Partners. Established firewall vendors are incrementally fusing IPS capabilities into their products, and IPS vendors are reluctant to take on the firewall vendors on their home turf. This presents an opportunity that Palo Alto Networks is addressing with a ground-up design approach that combines firewall, IPS and Secure Sockets Layer (SSL) inspection to challenge the established vendors in the firewall, IPS and secure Web gateway markets. This combination provides an application view of traffic that is not impeded by encryption or by the increasingly evasive applications that are channeled through HTTP, or “hop” from port to port. The result is that, where it might have seemed that an employee was using HTTP over SSL (HTTPS) to communicate with what appears to be a nonmalicious site, it becomes clear that the employee is, in fact, using hopster, meebo, Skype or some other potentially risky application or service, and choose to block it – or not – no matter what type of browser, endpoint or encryption is being used.

Palo Alto Networks has also made the pragmatic choice to use purpose-built hardware, in recognition of the network processing realities of this market, and offers URL filtering from SurfControl. We also like Palo Alto Networks’ marketing approach: Instead of spreading the standard fear, uncertainty and doubt, the company is promoting a better understanding of network traffic and more-granular block to not impede enterprise operations.

Challenges: Certain types of behavior must be considered high risk. Palo Alto Networks is a small company challenging the dominant firewall and IPS players in a multibillion-dollar market. To address this reality, it is positioning its offering initially as a “secondary” firewall, with the goal of gaining customer confidence and eventually replacing the incumbent primary firewall vendor. This strategy should also buy the company some time to get the third-party product certifications (for example, Common Criteria) necessary to convince customers that the firewall is functional and likely not to be vulnerable, and to broaden the range of models that a full enterprise deployment requires.

Who Should Care: Enterprises that want more visibility into HTTPS and other application traffic – and are willing to work with a smaller vendor – can consider Palo Alto Networks’ offering today.

5.0 VoIPshield Systems

Ottawa, Ontario, Canada (www.voipshield.com)
Analysis by Lawrence Orans

Why Cool: VoIPshield Systems has taken a unique approach to the IP telephony security market. The company has amassed a database of IP telephony vulnerabilities that serves as the foundation for VoIPaudit, its vulnerability assessment and penetration testing solution. VoIPshield's focus, unlike those of many players in the emerging voice over Internet Protocol (VoIP) security market, extends beyond solutions based on Session Initiation Protocol (SIP)-based solutions. Its database also includes multiple vulnerabilities – discovered via “ethical hacking” – for Avaya, Cisco and Nortel IP PBX solutions. (Sipera, another VoIP security vendor, also researches vulnerabilities, but its focus is primarily on SIP.) Most enterprises that have deployed IP telephony have used vendors' proprietary signaling protocols, not SIP, so VoIPshield's solution addresses the most relevant threats in today's environment. Most early adopters of VoIPaudit are in the financial services industry.

The VoIPaudit solution ships as an appliance, with pricing starting at \$20,000 and optional modules for vendor-specific vulnerabilities (for Avaya, Cisco and Nortel) priced at \$10,000 each. Approximately 20% of VoIPaudit customers use consultants to perform the vulnerability assessments and penetration testing. VoIPshield plans to release a second product in 2Q08: VoIPguard, the first IPS designed specifically to protect IP telephony systems, with signature-based and anomaly-based detection, and signatures available for Avaya, Cisco and Nortel IP PBXs. VoIPguard pricing will begin at \$10,000, with some configurations reaching \$80,000.

Challenges: VoIPshield's greatest challenge is the same one that plagues the broader VoIP security market: VoIP attacks have been few and far between, so telephony managers continue to place a low priority on VoIP security. This attitude will not change until telephony managers experience more “pain” (for example, widespread attacks or a single highly publicized attack). VoIPshield also faces some product-related challenges. It is focused on North America and doesn't address any specific vulnerabilities for the major European vendors (for example, Alcatel-Lucent and Siemens) or some of the vendors that are strong in the Asia/Pacific region (for example, NEC). Moreover, VoIPshield does not yet address specific vulnerabilities for IP telephony vendors that focus on the small and midsize business (SMB) market (for example, 3Com, Mitel Networks and ShoreTel).

Who Should Care: Telephony and contact center managers who believe that their IP PBXs are attack targets should consider VoIPshield's solution. This applies particularly to the financial services and government vertical industries. Retailers, especially those that are highly dependent on seasonal revenue, also need strong VoIP protection. Even a brief denial-of-service attack against a contact center or PBX, for example, could prove to be costly during a holiday shopping season.

6.0 Yoggie Security Systems

Tel Aviv, Israel (www.yoggie.com)
Analysis by Peter Firstbrook

Why Cool: Yoggie Security Systems developed a personal EPP security appliance (a USB key or small “brick”) for consumers and businesses. These appliances are full Linux computers that run 13 security applications, including a personal firewall and antimalware, host-based intrusion protection, URL filtering and anti-spam tools. These devices can be centrally managed by corporate IT, but Yoggie's ideal customers are SMBs and small office/home office (SoHo) users looking for advanced security.

Yoggie's promoters often point out that these devices offload security processing from CPUs and filter threats in a Linux-based PC before they reach a Windows system. This is a “nice to have,” but isn't necessarily a good reason to buy new hardware. The reason we think Yoggie is cool is that it gives us a glimpse of the future of security. Eventually, the USB appliances will incorporate tokens for authentication, storage, backup and personalized settings for multiple mobile devices. Expansion of the storage to include a lightweight temporary driver will enable users to take security and data with them when they use kiosks, home PCs or other unmanaged devices. We can also imagine this “full-PC-on-a-stick” security appliance being leveraged to provide “appliance-like” security in a virtualized environment, perhaps powered by Vpro chips or VMware.

Challenges: The current version of Yoggie's enterprise product cannot integrate with enterprise EPP solutions – a significant obstacle in the enterprise market. With Moore's Law continuing to increase processing power, it is not clear that offloading the CPU is a sufficient differentiator against enterprise software solutions. Expanding beyond the current feature set will require an installed base for R&D and real-world testing. Better-funded enterprise players, such as Symantec and McAfee, could copy Yoggie's model fairly easily, and with better integration between software solutions and hardware.

Who Should Care: Security practitioners looking for robust but lightweight security for “memory-challenged” older devices, unmanaged devices and SoHo equipment should consider Yoggie today. In the longer term, we expect to see more competition and innovation in the security-on-a-stick market.