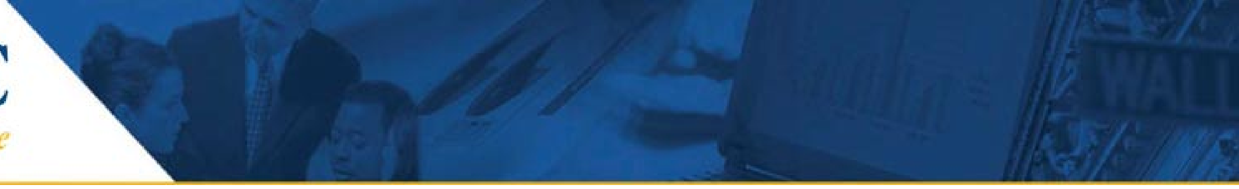

IDC VENDOR SPOTLIGHT

Unified Threat Management Appliances and Identity-Based Security: The Next Level in Network Security

September 2007

Adapted from *Worldwide Threat Management Security Appliances 2006–2010 Forecast and 2005 Vendor Shares: Easing the Pain* by Charles J. Kolodgy, IDC #204841, and *Worldwide Identity and Access Management Compliance 2006–2010 Forecast* by Sally Hudson, Vivian Tero, and Rose Ryan, IDC #201365

Sponsored by Cyberoam

Enterprises, regardless of size, are increasingly realizing that their computer systems are vulnerable to as many security threats from within the company as from without. These insider threats lead to security loopholes created out of user ignorance and malicious intent with unauthorized access, leading to loss of data confidentiality, bandwidth abuse, and more. Outsider threats such as spyware, phishing, and pharming are targeting individual users to carry out attacks from within the enterprise. In addition, there is increasing regulatory pressure to secure sensitive data, such as customer information, from threats such as a blended attack that targets a vulnerable user or IP address in an attempt to gain control of a client machine and access the corporate database or perpetuate an attack. Indeed, traditional network security has focused on authenticating and governing IP addresses without necessarily concerning itself with the identity of the user behind the address. Today's rapidly evolving threat environment, however, calls for a new security paradigm — identity-based security integrated with a unified threat management (UTM) appliance. This paper examines the growing need for an identity-based approach to security threats, the implications of adopting identity-driven security, and the role of vendor Cyberoam in this strategically emerging market.

Insider Threats: Targets and Attackers

Insider threats are changing the nature of network attacks. Acting as initiators themselves or as conduits for other attacks — both external and internal — they are leaving enterprises vulnerable to threats from within and from without. Insiders are causing enterprise loss out of ignorance or malicious intent.

Three key trends are driving the security market today. Because insiders have unaudited access to a significant amount of enterprise resources, enterprises suffer losses of a far higher magnitude in attacks through these individuals. Given the nature and extent of access that insiders enjoy, external attackers are targeting unsuspecting insiders to carry out their attacks from within the enterprise. In trying to protect employee, customer, and corporate data, regulatory compliance requirements are driving the need for securing and controlling users while protecting the enterprise.

These key trends mark a shift in the security market, with the need to protect and control the individual users taking precedence in providing enterprise security. Solutions that focus on the network layer address controls fail to control these attacks. Identity and access management (IAM) solutions on the other hand have been limited to application security and are not being extended to network security and reporting.

1. **Insider threats from intentional security breaches.** The largest security threat to enterprises lies within the network. With access to a significant portion of the enterprise resources, insiders pose the greatest risk to enterprise data and systems. Insiders, including current and former employees, temporary workers, partners, and customers, may be the unsuspecting threat carriers for external and internal attackers who use them and their lack of security awareness to gain access to enterprise data. IDC research shows that a majority of large enterprises are more concerned about insider threats than external threats. Although small companies are still more concerned with external threats, the gap has narrowed considerably over the years. While the reasons for this perspective may vary, the evidence shows that the per-incident costs of an internal breach are significantly higher than those of an external breach, and internal breaches are generally more difficult to uncover.

   Most companies do not have visibility into who is accessing what in the network until after the security breach has happened. Breaches continue to be caused by either a disgruntled or soon-to-leave employee or an outsider who compromises internal user rights to access intellectual property and other data. The press is full of instances in which employees are intentionally selling or inadvertently releasing personal information, including social security and credit card numbers. However, many of the most damaging cases involve the stealing of proprietary information. One of the most blatant cases involved a DuPont researcher who stole trade secrets and tried to sell them to his new employer. This insider accessed more than 16,000 documents, which DuPont estimated were worth $400 million, before he was discovered.

   To address these threats, enterprise security has now expanded to include control and monitoring of the internal user. As such, user identity has become a key component in enterprise security.

2. **Insider threats with external hackers exploiting insider ignorance.** Social engineering is a technique that uses the ignorance of insiders to gain entry into the enterprise. As the saying goes, "Security is only as strong as the weakest link." Attackers have long recognized that the best way around an obstacle is to find someone willing to tell you what you want to know. In most instances, the insider is completely unaware that he or she has provided information that can be used to breach a security system. Social engineering is rarely exposed. One case that did make the news was the case of the T-Mobile hack that exposed Paris Hilton's cell phone information. The flaw in the T-Mobile Web site was uncovered when an employee was tricked into divulging the critical information the hackers required. This is a simple example, but the issue is becoming much more complex as financial gain takes precedence over other motives for attacks. Organized criminals use the trust that exists between users and their colleagues and acquaintances to compromise insider targets and, through these contacts, extend the attack to other users.

   In targeting privileged users, attackers are using publicly available vulnerability information and freely available rootkits, launching small attacks that change patterns rapidly to escape security radars. In addition, the use of multiple methods to reach the insider is necessitating the deployment of multiple security solutions. Deploying multiple solutions comes at a high cost and brings with it the possibility of security mismanagement due to the complexity in managing multiple security solutions.

   Further, traditional security solutions that have relied on the magnitude of attacks to detect them are likely to fall short of their goal. Proactive security based on protecting and controlling individual users is necessary to address these threats. A combination of identity-based security and a comprehensive set of security solutions is required to protect enterprises.

3. **Regulatory compliance pressure to protect sensitive data.** Given the magnitude of threats to employee, customer, and corporate data, compliance regulations such as HIPAA, GLBA, SOX, PCI DSS, and more are forcing enterprises to undertake security measures that control the access and activity of users. Faced with penalties in the case of noncompliance with regulations and loss of reputation in the case of data loss, enterprises are under pressure to implement compliance measures within the enterprise.

   Compliance regulations are forcing organizations to have more network access controls with increased levels of network monitoring and reporting. The volume of information produced by existing systems is fast becoming too confusing and too much to handle for policy enforcers and auditors.

   The nature of compliance requirements is such that the target for protection and control is the individual user within the network.

Given the nature of insider threats, accidental or intentional, as well as compliance requirements, linking user identity to security is emerging as the key requirement to ensure enterprise security.

The Identity-Based UTM Appliance

As federal and state governments and industry groups take aggressive steps to mandate that enterprises address the growing problem of information leaks, intrusions, and other security breaches, enterprise IT organizations are now seeking efficient ways to monitor and report on these activities from sources inside and outside the enterprise before the breach takes place. In the absence of identity-based policies, monitoring, alerts, and controls, enterprises can rely only on logs to determine that a breach has actually taken place and resort to post-breach action, by which time, the loss has already taken place.

The stark reality is that if an enterprise infrastructure is not equipped to monitor and log specifically who is accessing what and from where, security threats and policy and compliance violations may be taking place without notice or an auditable trail.

The loss isn't always just financial in nature. On the one hand, it is difficult to place a value on the potential value of intellectual property such as software code, brands, designs, and more. On the other hand, loss of customer, partner, or employee data leads to loss of reputation and trust that is difficult to regain.

Identity-based security solutions provide discrete identity information along with network log data. With identity and network data combined, enterprises are able to identify patterns of behavior by specific users or groups that can signify misuse, unauthorized intrusions, or malicious attacks from inside or outside the enterprise. Alerts can be placed based on predefined norms of enterprise behavior by individuals, groups, departments, or levels of hierarchy. A significant deviation in insider behavior would then trigger a security alert, which staves off potential breaches.

Identity-based network information can be analyzed and used by security professionals, human resources, and auditors to demonstrate and confirm compliance with established corporate policies, as well as with government- and industry-imposed regulations.

The importance of identity-based security has assumed greater significance with the emergence and rapid rise of unified security in the form of UTM appliances. Blended threats have given rise to the need for multiple security features for comprehensive protection to the enterprise. But the complexity involved in managing multiple security solutions has led to unified security with multiple security features over a single platform. There is growing recognition that identity management is a critical component of security and that UTM solutions are capable of extending their security to encompass user identity.

In the absence of the binding of security to the user identity, the UTM solution would be unable to offer policies, alerts, and controls based on the user identity across all its features. Because blanket policies by their very nature offer common policies across the enterprise, they force enterprises to give either more or less than the desired freedom and flexibility to individuals. Hence they affect employee flexibility in functioning even as they fail to alert enterprises to a potential breach.

Because most networks use only the IP address to log in and verify users, all that is known is which computer is being used for the previously mentioned purposes. The activity could be perpetrated by anyone, inside or outside the firewall, at any time of the day or night. What's required today in managing individual accounts goes beyond simple directory management. Detailed accountability is becoming essential to managing and ensuring security in small and medium-sized businesses and large corporations.

A secure approach is to extend the UTM platform to incorporate identity-based security technology. The strength of the UTM technology is that it's designed to offer comprehensive security while keeping security an easy-to-manage affair. UTM appliances that incorporate identity-based controls, utilizing rule-matched criteria for identifying and logging in users, can expand and innovate based on emerging threats as well as customer business requirements. In addition to allowing the device to perform its standard network security roles, network access is granted to the individual, regardless of the machine's IP or MAC address. Activities and security policy rules can be enforced by the UTM appliance on network segments based on identity. Threats can be identified whether they come from inside or outside, further protecting the gateway from accidental penetration by viruses, worms, spyware, phishing, and pharming.

Benefits of an Identity-Based UTM Appliance

An identity-based UTM appliance that integrates identity data addresses the previously mentioned security issues and commonly provides the following benefits:

- Protection from external system infections and compromises from outside the firewall due to Trojan horses, viruses, worms, and the like infiltrating the corporate IT system, including spyware, phishing, and pharming, which often occur without the user's knowledge but usually because of nonbusiness activity such as visiting an online gaming or peer-to-peer media downloading site.

- Protection from intentional intrusion from within and without by employees, hackers, or professional thieves where the objective is to obtain proprietary, confidential, or competitive information to use against the company's interests or for financial gain. This has disastrous effects on reporting and compliance rules and regulations. The appliances can also protect privacy and systems integrity.

- Enhanced productivity due to bandwidth allocation and control over Internet surfing.

- Reporting that tracks identity-based usage, problems, intrusions, and so forth. In many enterprises, it's difficult to determine which employees are engaging in nonbusiness activity such as chatting online, shopping, conducting personal business, or engaging in music downloads or online streaming. Any instance of misuse or intrusion has financial consequences for the enterprise, from simple employee productivity to system downtime to compromise or loss of valuable data or information.

- Identity-based policy creation across all security features based on individual work requirements and network usage pattern.

- The ability to automate risk assessment and controls for segregation of duties.

- The shortening of audit and reporting cycles. Determining who is accessing what information and when they are doing so is made possible by automated auditing. Likewise, automated tracking of access and permission rights — who granted these rights and when and why they were granted — has become part of the cost of doing business for most organizations worldwide.

- As discussed, government regulations and compliance and industry governance standards will be increasingly significant issues in the worldwide business environment. Through user identification and controls, identity-based UTM appliances enable enterprises to comply with such compliance regulations and standards.

Business Drivers

Identity-based unified threat management has assumed significance by addressing the three business drivers — insider threats, compliance requirements, and the rise of UTM appliances — with an integrated hardware device and software management solution, offering comprehensive security to enterprises. The dedicated hardware device is installed behind the router, WAN switch, or even a firewall.

Regulatory Compliance

A separate IDC survey of end-user organizations suggests that Sarbanes-Oxley will remain the primary regulatory driver in the short to medium term. Organizations also expressed a desire to align their control objectives and leverage investments across multiple compliance-driven initiatives. Organizations on this track started by identifying the common data sets and business components. Security for access control addresses an immediate and common requirement across regulations and processes.

Identity-based security has the potential to greatly reduce an IT staff's workload because these products can provide valuable information that facilitates the consolidation and correlation of network activities based on individuals. This is because policy compliance management and monitoring is primarily focused on individuals rather than on abstract information such as network addresses. With this information, it is easier to understand what users are doing and to use that knowledge for compliance reporting.

Current solutions are geared toward application access management rather than network access management. An identity-based security solution at the perimeter is able to control and track outbound network usage based on identity. IDC believes that identity-based security has emerged as a key component of a compliance platform. We predict that compliance and corporate governance initiatives will require user identity (as opposed to machine identity) to be a strong component of network security in 2007 and beyond.

The Rise of UTM Appliances

Since 2004, advanced UTM has been replacing conventional firewall and virtual private network (VPN) security solutions as the primary network gateway defense. The older, conventional solutions, such as firewalls or VPNs, are not sufficient in today's networked environment. With blended attacks entering enterprises through multiple protocols, firewalls and VPNs are not enough to prevent security breaches throughout the whole network infrastructure.

In 2005, firewall implementations dropped 16%. However, due to the surge in the UTM and intrusion detection and prevention (ID&P) markets, the entire threat management security appliance market grew over 10% to a total of $2.78 billion. The strongest growth came in UTM security appliances.

Over the next five years, UTM revenue is expected to exceed that of standard firewall/VPNs. Threat management appliances, and in particular UTM appliances, are popular with small and medium-sized enterprises (SMEs), which represent a substantial market. In 2007, IDC expects 80% of all network security solutions to be delivered via a dedicated appliance. The market for threat management appliances has remained strong because these devices represent the most straightforward, secure, and comprehensive solution because they utilize both hardware and software to provide several important benefits.

The all-in-one approach simplifies product selection, product integration, and ongoing support. Customers or service providers can easily install and maintain the appliance once and be done with it, avoiding the multiple or recurring software installations and proliferating servers involved in multiple security solutions. Increasingly, this process is handled remotely.

Because UTM appliances are generally plug and play with very little installation required and compatible with large, centralized software-based firewalls, they are suited for such remote operations. With a UTM appliance, application performance is standardized across the network, bringing consistency in performance. When a box fails, it is easier to swap it out than to troubleshoot. This process gets the node back online quickly and can be accomplished by a nontechnical person — an especially important feature for remote offices without a dedicated technical staff onsite. Management of UTM appliance operation, performance, and application functionality can be administered from a centralized management console.

Next-generation UTM appliances (those that can incorporate identity knowledge and controls) should help facilitate the breakdown of organizational silos and be scalable to eventually support enterprise risk management initiatives. The use of these UTM devices, with integrated firewall, intrusion prevention, content security, and identity, expands where the devices can be used — specifically, they become part of the IT arsenal for internal security to deal with targeted network attacks that go after only a small group of users. The solution's ability to integrate with existing IT operations is critical.

Given these benefits, UTM appliances have emerged as the single fastest-growing solutions in the security arena. By focusing on user identity as the basis for security, identity-based UTM appliances offer a comprehensive defense against current threat tactics. They are poised to become the next-generation solutions to emerging IT security and compliance challenges.

Considering Cyberoam

Cyberoam is a division of Elitecore Technologies Ltd., with U.S. headquarters in Newburyport, Massachusetts, and offices in India. Cyberoam offers a mature, UTM solution with identity-based security, linking user identity to security right from authentication to policy setting, controls, and reporting, offering Boundless Network Security to enterprises against internal and external threats.

By offering identity-based policy making and visibility across all its security features, Cyberoam allows administrators to create customized user-based policies based on the user or department work profile. In addition, it offers instant visibility into "who is accessing what in the enterprise." In doing so, it enables enterprises to meet compliance requirements in addition to facilitating instant action in case of a security breach even in dynamic IP environments such as DHCP and WiFi. By eliminating IP addresses as intermediate components to identify the user, it offers complete control over environments in which multiple users share computers.

Specific Cyberoam identity-optimized UTM features include the following:

- Stateful-inspection firewall
- Virtual private network
- Gateway antivirus
- Gateway antispam
- Intrusion detection and prevention
- Antimalware
- Content filtering
- Bandwidth management
- Multiple-link management

With more than 1,700 installations in corporations, governments agencies, and educational institutions worldwide, Cyberoam has set the pace for identity-based UTM solutions.

There are three classes of Cyberoam Internet security appliances:

- **CRi Series – SMB, SOHO, and ROBO.** The CR25i and CR50i offer comprehensive security to small office-home office (SOHO) and remote office-branch office (ROBO) establishments. This affordable, easy-to-configure, and easy-to-manage solution not only lowers capital and operating costs but also eliminates the need for technical manpower for device management. For ROBOs, these appliances offer secure connectivity between branch offices and the head office in addition to remote monitoring from the central office aided by Cyberoam Central Console (CCC), the centralized network management solution.
- **CRi Series – SMEs.** The CR100i, CR250i, and CR500i are designed to offer gateway security for the headquarters and branch offices of small and midsize enterprises. These all-in-one solutions provide full network protection and identity-based security for each user so that security and access policies can be established individually or departmentally, or at other corporate levels.
- **CRi Series – Large Enterprises.** The CR1000i and CR1500i offer the robust, multilayered security and system management demanded by large organizations, with a high degree of user identity–based security granularity. In addition, the devices provide bandwidth management, delivering traffic flow at higher, more reliable speeds. Multilink management provides the redundancy and multiple ISP link management over multiple WANs to ensure uninterrupted Internet access.

These security solutions control access to network-based resources using stateful-inspection firewall and Internet access management controls. They complement identity management solutions already in place by controlling access to network resources. These solutions go beyond the current IAM products that fail to extend identity-based access to the network.

Additionally, Cyberoam offers a management console for coordinated, centralized control over dispersed network appliances with centralized reporting. The CCC enables MSSPs and large organizations to centrally manage and monitor multiple, dispersed Cyberoam appliances to reduce the drain on internal and external resources.

The CCC also empowers network administrators to create and enforce security policies and custom signatures to strengthen branch and remote office security, ultimately lowering operational complexity. It can likewise lower the operating cost of deploying and maintaining multiple devices within an organization.

Challenges

Although market-proven and successful to date, Cyberoam faces challenges selling into a well-established network security appliance market. Many organizations say they want to know who does what and when, but the reality is that those organizations have not made user identity a strong component of their network security. IT managers still see it as something exclusive to the application layer. They're also concerned about how much extra work would be required. What they need to understand, however, is that identity-optimized UTM leverages the existing identity infrastructure. When this realization hits home, IDC would expect organizations to start making this connection with greater frequency.

Conclusion

In a world where network security is the first, second, and third line of defense and as attack methodologies, including blended threats, become more complex, no organization can afford to take information security threats lightly. Existing network security solutions have proven conquerable, and a spate of software plug-ins has come to market to provide ad hoc fixes.

IDC believes the combination of a hardware device and sophisticated system management software, known as identity-based UTM, delivers an effective, intelligent solution for the future. Identity-based UTM can be deployed across any size enterprise — small, medium, or large — with equal effectiveness and requires very little ongoing maintenance other than adding, removing, or requalifying users.

IDC believes that identity-based UTM represents the next generation in the burgeoning UTM marketplace. When enterprises realize the value of having identity as a full component of their UTM solution — the increased internal security, protection against insidious and complex attacks, understanding individual network usage patterns, and compliance reporting — Cyberoam will benefit as the innovator.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com