

Bandwidth

The Leading IT Security & Data Center Solutions Publication – Vol. 08, Issue 1

IN THIS ISSUE...



Check Point Defines Scalability and Management: Preview the Second Wave of Intrusion Prevention Systems

Check Point has brought a new approach to designing dedicated intrusion prevention into your network. Check Point's approach to IPS reflects the fact that for IDS/IPS applications, scalability has several dimensions. Discover more about Operational Scalability and how Dynamic Shielding Architecture leverages profiled host information to proactively protect the network.

Read more from Check Point on page 10

Eliminating Security Nightmares

A Proactive Security approach assigns a predictable and manageable monthly subscription for security. Learn how Akibia's Proactive Security Services can help customers to limit security threats by getting ahead of them.

Read more from Akibia on page 5

The Shift to User-Centric Products and Services

Enterprises have an option that delivers increased mobility without compromising security – user-centric networks. Learn more about how user-centric networks significantly expand the reach of traditional port-centric networks, preserving and extending investments in existing network infrastructure.

Read more from Aruba on page 6

Addressing Encrypted Security Threats Inside SSL

The criticality and confidentiality of Internet-accessible applications has caused organizations to rely more heavily on SSL encryption. Find out how IT organizations can overcome the encrypted security threats inside SSL.

Read more from Blue Coat on page 8

TABLE OF CONTENTS

3 Brainshark Validates the Security of Its SaaS Solutions with Akibia

4 Deciphering Data Loss Prevention

5 Eliminating Security Nightmares

6 People Move. Networks Must Follow. Securely. Reliably. Pervasively. By Aruba

8 Addressing Encrypted Security Threats Inside SSL with Blue Coat

10 Check Point Defines Scalability and Management

12 Check Point and Nokia: An Innovative Approach To Meeting New Demands and Fighting Threats

14 Akibia News

Bandwidth is a publication of



Please send comments, questions or suggestions for future issues to bandwidth@akibia.com

Akibia Partner News

At Akibia we kicked off fiscal year 2009 on April 1, 2008 with significant momentum and excitement for the services, support and products we provide to our customers. Akibia was awarded the Check Point PureAdvantage Platinum Partner of the Year and was recognized by Citrix for significant growth related to our emerging partnership. These accolades come as Akibia is celebrating its 20th anniversary.

Akibia Wins Check Point Software PUREAdvantage Platinum Partner of the Year Award for the Second Consecutive Year

Akibia was recognized because it excels as a Check Point partner providing expert Check Point consulting, integration, support and education services. Akibia's engineers are experienced and proven in implementing Check Point solutions and Akibia is routinely commended by joint customers for its superior Check Point integration and support capabilities. The partnership between the two companies has grown significantly in terms of customers, revenue and strategic successes as a result of Akibia's strong consulting team, its ability to quickly integrate new and emerging Check Point solutions within its portfolio, and its knowledgeable and educated sales and support staff, as well as the strength of Check Point's data security solutions.

"Akibia exemplifies partner excellence," said Marty Leamy, vice president of Americas field operations for Check Point. "We have recognized Akibia for the second consecutive year with the Check Point Software PUREAdvantage Award because of the value Akibia brings to our partnership and our shared customers, in terms of support, technical capabilities and depth of market penetration."

Akibia Achieves Citrix Solution Advisor Gold Status

Akibia's first year as a Citrix Solution Advisor produced exceptional results that exceeded expectations for the program. Akibia found significant demand among its customer base for Citrix's Application Delivery Infrastructure solutions and was recognized by Citrix Systems as "Best Application Networking Group (ANG) Growth as a Silver Partner in 2007." As a result of the success of the Akibia and Citrix relationship, Akibia moved quickly to Gold status.

"In recognizing Akibia as a Gold Solution Advisor, Citrix is acknowledging the strength of Akibia's services team, and their ability to serve as a Trusted Advisor to our joint customers seeking solutions for application delivery," said Dino Petrakis, area vice president, Northeast region, Citrix. "Akibia's knowledge of the needs and requirements of enterprise organizations and their ability to meet those requirements with customized Citrix-based networking solutions will ensure an effective and long term partnership benefitting both companies and our customers."

Brainshark Validates the Security of Its SaaS Solutions with Akibia

Brainshark, a provider of on-demand presentation solutions, helps its customers deliver business communications that are both powerful and convenient. More than 600 world-class companies rely on Brainshark's software as a service (SaaS) offering to communicate critical information to employees, customers, and partners. Both Brainshark and its customers share the mutual goal of achieving the highest level of IT security and data protection.

The Challenge

Brainshark is often asked by its prospects to provide documentation to prove the security of its SaaS applications. Brainshark's customers are some of the largest organizations in the world, and they use Brainshark within their daily business communications for marketing, selling, training, and other corporate communications. Their customers' security standards are high and Brainshark makes it a priority to meet and exceed these requirements.

During the negotiation and prospecting stages of the sales cycle, Brainshark's sales team is often asked by customers for third party documentation or "proof" of the company's strength of security. While Brainshark knew its systems were secure and could prove it with its own documentation, customers often required verification from an external company.

"To address customer and prospect questions, we needed to undertake a third party security assessment," said Arnie Greenfield, vice president and CTO of Brainshark. "One of our main requirements was that the company was a well-respected and experienced organization whose name would resonate with our clients and prospects. Akibia met our requirements, and the requirements of our customers."

The Solution

Akibia's Vulnerability Assessment and Penetration testing procedures are based on industry best practices perfected over hundreds of engagements at client sites. For Brainshark, Akibia conducted a three-pronged assessment, including vulnerability tests, a port scan and penetration testing. The vulnerability assessment included tests for SQL injection, cookie manipulation, access control weaknesses, session state, and cross-site scripting. The focus of the tests was to identify host as well as application security concerns.

Once the assessment was completed, Akibia and Brainshark partnered to review the results, discuss remediation of the few non-critical concerns the assessment brought to light, and complete a report to be delivered to a specific customer that had requested a meeting to review security.

The client was quick to applaud the work of Akibia's security team and Brainshark, and expressed satisfaction with the results of the security assessment. "Our customer was very comfortable with the results of the assessment. The client was already confident in the ability of our solution to improve business productivity, now with confidence in our security posture, the client can truly achieve maximum benefits from our solution," added Greenfield.

The Benefit

As a result of the security assessment by Akibia, Brainshark now has peace of mind that comes with an expert third party validation of its security policy. Its customers also trust the results of the assessment, and are investing further in leveraging the Brainshark solution.

"We now have a 'stamp of approval' from one of the top security consulting organizations to confirm the security and

integrity of our solutions. This goes a long way in easing our sales cycle and ensuring continued customer confidence in the security of our solutions," said Greenfield.

About Akibia, Inc.

Akibia provides innovative IT solutions that enable leading companies worldwide to optimize, secure, manage and support their mission-critical infrastructure. As an independent advisor, Akibia partners with its customers to deliver solutions that improve the availability and performance of their data center and security infrastructure. Combining expert consulting, integration and support services with world-class customer service, Akibia helps IT organizations maximize the value of their existing infrastructure, while mitigating risk and reducing complexity. Founded as Polaris Service in 1988 and headquartered in Massachusetts, Akibia is an independent services company with offices throughout the United States and Europe.



www.akibia.com

Deciphering Data Loss Prevention

By **Tim Richardson**, PRODUCT MARKETING MANAGER, AKIBIA

The data loss prevention (DLP) space has been incredibly interesting to watch in the last year. Acquisitions by RSA Security (Tablus), Symantec (Vontu), Check Point (Pointsec), McAfee (Onigma & Safe Boot), and Websense (Port Authority) has consolidated this market quickly and appear to have validated the need for these technologies.

While many of the technologies encompassed by DLP have been around for a while, Data Loss Prevention as a market space is in its relative infancy. The current market definitions of what DLP encompasses is fluid, interpretive and is being driven by various manufacturers.

As I have talked to our clients about data loss prevention, I typically try to understand what is driving their interest, discuss how much of the organization is involved in the initiative, and get an overview of some of the tools and technologies they have in place today that may be part of a data loss prevention strategy. Based on this information, we can begin to help our clients define the scope of the initiative by discussing the three fundamental elements of data loss prevention: policy, data and channel.

Policy

Regardless of size, all organizations practice some kind of data classification policy – client lists, intellectual property, contracts, financial data, processes, client data, employee compensation & benefits, are a few of the easy ones to identify. As the size of an organization increases so does the complexity of validating that appropriate policies are being practiced. Typically classification involves variables that are tied to an individual's relationship with the organization (employee, non-employee), their role (employee title, business partner, customer, competitor, auditor, etc.), and

their responsibilities (customer service, finance, executive, shipping, etc.).

Data

Data resides in a myriad of places within an IT environment. One of our partners estimates that 80% of all data resides in unstructured mediums such as email, documents, presentations, intranets, extranets, portable storage devices, smart phones, etc. These data stores allow the creation, manipulation, and sharing of data in dynamic ways. Unfortunately, these uncontrolled data stores create risks for organizations that can be difficult to identify, let alone quantify. Concerns about risk are driven by regulations and governance (such as breach notification laws, PCI, HIPAA, and the myriad of financial industry regulations), competitive differentiation, and client privacy.

Channel

After acknowledging that data is everywhere and that classification is inherent, the third element is to understand how and where it moves. Networks provide the most prevalent transport mechanism (both wired and wireless) to computers, laptops, smart phones, and specialty devices. These devices commonly have expansion ports that allow hard drives, tapes, thumb drives, iPods/MP3 players, etc to store and transport large amounts of data. With our ever-increasing move towards mobility, the opportunities and incidences of data compromise increase.

What to do?

The approach we recommend for DLP projects is to do a risk based analysis – specifically documenting a client's data classification policies, discovering where their data resides, and understanding how

it is transmitted. By understanding these three different elements and identifying how these elements are vulnerable to threats, we help our clients create a prioritized list of how and where data should be protected. This type of analysis can be intensive or light, depending on the priorities of the organization and the issues that need to be addressed.

While organizations have been exposed to data loss risks for a long time, data governance initiatives are accelerating the need to document that data assets are protected. I expect to see data loss prevention driving many initiatives within organizations in the coming years as companies work to validate that their data classification policies are working effectively.



www.akibia.com



Eliminating Security Nightmares

By Michael Halperin, VICE PRESIDENT OF TECHNOLOGY, AKIBIA



Security professionals often say that the potential for a security incident causes sleepless nights and stressful days. Even as professionals build secure enterprise infrastructure and keep pace with security best practices, hackers and malicious attackers are building ways to circumvent these controls. Meanwhile, business users with the best of intentions are accidentally exposing data because of a lack of security training and awareness. There's a reason these fears keep security professionals up at night, any one of these issues could result in millions of dollars in corporate losses related to regulatory fines, lost customers or theft.

For most security managers, a security incident is doubly crippling. While they struggle to get budget approval for important security enhancements throughout the year, security executives then have their programs scrutinized when failure does occur. In the case of a security incident the security team is exposed as not having the appropriate safe guards in place (although they likely tried to get budget

for the appropriate technology months ago), but also now must ask for significant budget to perform a forensic investigation, identify the issue, and guard against it happening again.

This approach not only jeopardizes enterprise security, but it also wreaks havoc on a company's IT budget. Instead, forward thinking security managers are getting ahead of the issue by deploying a Proactive Security approach. This approach assigns a predictable - and manageable - monthly subscription for security. It includes regularly scheduled vulnerability assessments, where potential issues can be spotted and averted before becoming real problems. It also provides for incident response, in the case a security event does occur. By having a team already lined up for incident response, and a predictable, accounted for cost, companies can avoid security spending spikes and benefit from faster response and remediation of the incident, as the contract is already signed and in place.

Proactive Security Services Help Companies Get Ahead of Security Issues

Akibia provides Proactive Security Services as a way for our customers to limit security threats by getting ahead of them, while also providing a safety net - of resources and talent - should a forensic investigation be needed. Akibia's Proactive Security Services includes:

- **Security Roadmap Planning & Deployment** – Akibia experts help you build your security strategy, and provide an objective expert opinion on the plans you have in place. In addition, Akibia has integration expertise across an industry leading portfolio of best-of-breed

security technologies to help your staff ensure smooth, successful, and effective technology deployments.

- **Security Awareness** – Akibia security experts help educate users, IT staff, and Senior Management on security issues, threats, and best practices. The education helps ensure the effectiveness of your security program. Akibia experts can help in educating Senior Management on industry and client-specific security threats, creating support for critical funding of security initiatives.
- **Oversight and Validation** – Having the right technology is the easy part. The hard part is making sure your security technologies and policies are working as designed. Akibia experts perform a wide variety of functions including penetration tests, vulnerability assessments and perimeter scans to ensure your security program is working effectively.
- **Digital Forensics** – Akibia's Forensics experts help prepare you for data collection and analysis related to forensics investigations before any incident occurs, then perform the investigation and analysis required to pinpoint the specifics of the event. Effective forensics planning and performance can save organizations millions of dollars.

For more information on Akibia's Proactive Security Services please contact your sales representative, or call 1-866-4-AKIBIA.



www.akibia.com

People Move. Networks Must Follow.



Our increasingly mobile society is forcing many industries to develop ways to make their services accessible whenever and wherever customers require them. In the not too distant past, one could conduct banking transactions only at a bank branch and only during business hours. As mobile customers demanded more convenient access to banking services, banks moved away from an institution-centric model of business to a user-centric model in which banking applications were brought to the customer. The bank branch gave way to the ATM and ultimately to the smart card.

The Shift from Institution-Centric to User-Centric Products and Services

Increased mobility for the customer, however, resulted in reduced control and security for banks. Unauthorized card duplication, phishing, and ATM

substitution all skyrocketed as banking products and services moved closer to the user. The demand for mobility fostered innovations which, in turn, undermined security.

The networking industry is undergoing a similar transformation, and facing the same issues, as the banking industry. Enterprises want to enable users to work wherever and whenever it is most convenient, economical, and expeditious for them to do so - in the office, at home, in hotels, or on the road. The issue is that traditional, port-centric networks use perimeter-based security that was designed and optimized for fixed, non-mobile users. For traditional network suppliers mobility breaks security, and security precludes mobility.

Fortunately, enterprises have an option that delivers both mobility and security - user-centric networks. Aruba's user-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a

cohesive, high-performance system that securely delivers the enterprise network wherever users work or roam. User-centric networks significantly expand the reach of traditional port-centric networks, preserving and extending investments in existing network infrastructure. Additionally, the high performance and robustness of Aruba's solutions provide the first viable alternative to wired networks, making the all-wireless office a reality.

Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, enabling follow-me security that is enforced regardless of where and how the networked is accessed. Application continuity services enable follow-me applications that continue running even as the user moves between wireless LANs, wired LANs, and cellular networks.



Securely. Reliably. Pervasively.

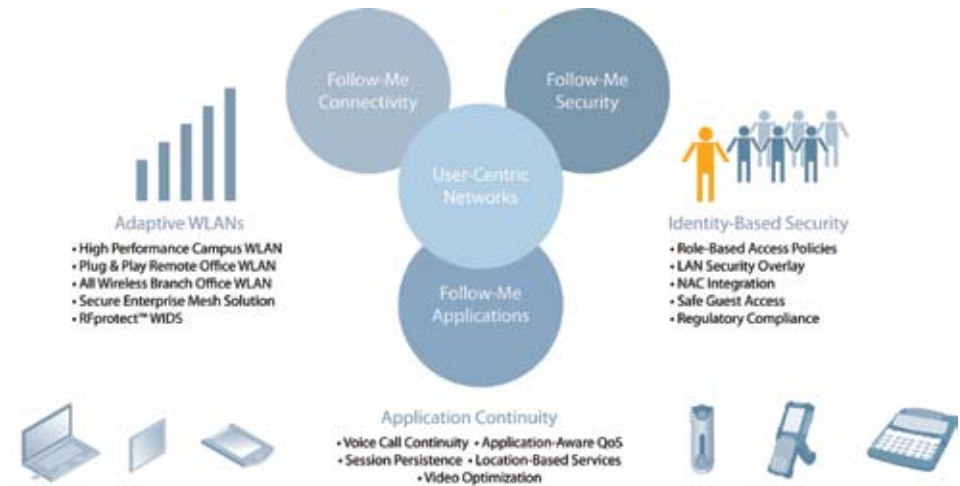
Aruba has integrated all of the elements required to deliver enterprise mobility – security, application, network and radio frequency (RF) management services – into a unified solution including an award-winning portfolio of wireless LAN, security, diagnostic, network management, and integration products.

Applications of User-Centric Networks

User-centric networks are applicable in enterprise, education, finance, government, healthcare, hospitality, and retail for a wide range of uses including large-scale WLANs, branch and remote office access, ultra-high security and regulatory compliance, guest access, and multimedia-over-wireless, among others.

Aruba's networks are used in some of the world's largest enterprise, campus, and hospital wireless LAN and FMC deployments. Microsoft, for example, has deployed Aruba user-centric networks at offices in more than 60 countries, while Ohio State University has a campus wireless LAN with roughly 10,000 access points. The reason these customers turned to Aruba for their high density data, voice over IP (VoIP), and streaming video networks is because Aruba's architecture is massively scalable. All three types of applications have different flow, quality of service (QoS), and timing requirements, and Aruba's application-aware design optimizes the network accordingly.

Furthermore, geographic boundaries don't impose limits on security, performance or management. Whether connecting from a large regional office, a small branch facility, or even from one's home, the security policies follow the user while the extended network can still be managed from a single central location.



The All-Wireless Workplace

The latest technological development – 802.11n – brings even greater benefits and opportunities. The 802.11n standard heralds a new world for enterprise wireless networks. It brings higher data rates, longer range and more reliable coverage than previous Wi-Fi technology. Available 802.11n access points support data rates to 300 Mbps per band, superior to common 100 Mbps Ethernet connections. The substantial performance increase over older Wi-Fi equipment removes the last serious objection to adoption of the all-wireless workplace concept, where no cables need to be run to individual desks and workstations.

To extend the network to locations that would be prohibitively expensive, if not impossible, to reach using a wired solution, Aruba has introduced its Secure Enterprise Mesh technology. Secure Enterprise Mesh enables a converged data, voice, and video network to be deployed or expanded, securely sending information from location to location over an exclusively wireless network. Because no cabling is required, the network can be installed, moved, or

changed quickly and easily as needed.

Cooperative control and mesh clustering features allow the wireless network to self-organize, determine the optimal path for communication to any given client, and self-heal in the event that a wireless path is blocked or a mesh access point fails.

Aruba's user-centric networks deliver both mobility and security without compromise. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work.

ARUBA[®]
networks

www.arubanetworks.com

Addressing Encrypted Security Threats Inside SSL



Web applications (and their derivatives – IM, P2P, Web Services) continue to comprise the overwhelming majority of new applications being deployed across today’s distributed enterprises. Much of the new growth in Web application development is focused on business-critical applications. Furthermore, many of these applications and related components are hosted by third parties or accessed over public infrastructure. Not surprising, the criticality and confidentiality of Internet-accessible applications has caused organizations to rely more heavily on SSL encryption.

SSL encryption was designed to create a trusted class of Web traffic – when the

little padlock shows up in a browser, the traffic is deemed “secure.” This confidentiality has enabled businesses and consumers to take advantage of “anywhere, anytime, any user” encrypted connection to drive tremendous commercial exploitation of the Web. There is, however, a downside: encryption, the very thing that keeps prying eyes from SSL traffic, also makes it nearly impossible to see, understand, or manage that traffic. Indeed, in most organizations, port 443 (the designated port for SSL traffic) is not scrutinized – traffic freely and blindly flows in and out of the enterprise. This raises three sets of issues: first, IT lacks any control over

this traffic; second, IT has no ability to protect itself from threats flowing in the encrypted traffic stream; and third, IT cannot prioritize and accelerate encrypted traffic - some of which may be mission-critical.

Most SSL traffic is, of course, benign and provides no threat to the organization. Further, much of it is key business traffic to business partners or to outsourced application providers. One example is Salesforce.com, the online CRM provider, where all data is transferred using SSL technology.

On the other hand, users can use SSL technology to circumvent the usual policy



controls. They can use SSL encrypted web email services (such as Yahoo! mail) to send out confidential information. They can also set up an SSL tunnel between the organization and their own home PC to transfer information and users have been known to use SSL to surf for inappropriate content on the web. The newer types of Spyware are now using SSL to get around spyware controls both for entering organizations and for sending out their information to the spyware control points. And, of course, often the worst attacks for individual users is phishing attacks where the user is fooled into entering their private information onto a bogus site and these are very often secured by SSL as it helps the user feel confident that this is a legitimate banking or finance site.

If an organization were to adopt a solution to resolve these issues, it would need to understand native SSL traffic flowing to external applications, be operationally affordable, not impede business (neither performance nor privacy), and be extensible and adaptable.

Unfortunately, most technology efforts to resolve these issues for unencrypted traffic have proved inadequate – none can “see” the encrypted traffic. While SSL offload or SSL VPN technologies can help organizations manage SSL traffic for applications that they control, there has not been a practical solution for “inside-out SSL.” In other words, traditional security and networking solutions cannot effectively protect users inside the corporate network from safely accessing applications and information outside the corporate network (e.g., Salesforce.com, employee benefits providers, and the wide variety of non-business-related applications their employees use).

IT organizations can overcome these limitations with intelligent proxy appliances

that allow inbound and outbound encrypted traffic to be terminated – thereby enabling unprecedented visibility and context of the encrypted content. From there, proxy appliances can reinitiate the sessions according to the policies set by IT. Termination by a proxy is the only way to gain visibility and control of SSL communications. It provides a critical control point for protection (against viruses, worms, spyware, and phishing), policy (manage the who, what, where, when, and how of user/application interaction), and performance (cache, compress, and prioritize traffic).

...the criticality and confidentiality of Internet-accessible applications has caused organizations to rely more heavily on SSL encryption.

Lastly though, organizations have to be responsible about use of this technology, understanding the privacy of the individual. The set up of the devices needs to understand the context of the SSL session before deciding whether to intercept the data stream. As an example, if you trust a certain site (or types of sites) then there is no need to intercept, for instance, data to and from Salesforce.com or known banking and shopping sites (as defined by URL filtering categorization). Perhaps an organization allows users to access web-

based email from work, but this should be intercepted. At this point, before carrying out any inspection, the user should be informed with a message that points out that the data is about to be checked for their own good and the good of the organization. The user then has the option to cancel the request. The most dangerous types of SSL transactions are those to unknown destinations – the new phishing site that has just been created or just a plain IP address that is unknown and the organization’s efforts should be focused on those, as they hold the most danger.

Blue Coat

www.bluecoat.com

Check Point Defines Scalability and Management: Preview the Second Wave of Intrusion Prevention Systems



In the intrusion detection and prevention (IDS/IPS) market segment, throughput and latency get most of the attention in product reviews and evaluations. There are many sound reasons for this. A service device that inspects your most critical traffic must be able to perform reliably under a range of different conditions at wire speed.

Check Point's approach to IPS reflects the fact that for IDS/IPS applications, scalability has several dimensions. In the area of throughput, Check Point's IPS-1 appliances are comparable to any of the leading vendors. The Check Point

product line includes devices that can deliver traditional performance scalability from economical appliances at 50 Mbps and 200 Mps up to in-line protection in excess of 2 and 4 Gbps.

Check Point recognizes that reliability and performance is merely "table stakes" in a much larger game. Check Point has brought a new approach to designing dedicated intrusion prevention into your network. This approach requires leaving behind the 1:1 threat-to-signature model that has been a part of almost every first generation IDS and IPS product. While the ability to regularly and rapidly

update the threat library in a network is a mandatory requirement, the organization of this threat information and the techniques used in updates must also be designed with a view toward scalability – Operational Scalability.

Operational Scalability is a characteristic that has been a weak link in this product category. Ongoing management and maintenance of IPS requires a thoughtful approach to day-to-day administration and tuning.

Strong on-the-wire detection capabilities are of no practical use if they merely



generate noise. Check Point's IPS-1 Dashboard delivers Situational Visibility. The IPS-1 Dashboard improves communications and productivity by allowing the security team to share real-time, high-level graphical views across the network. It guides incident response workflow with its unique ability to drill-down and organize events and alerts to effectively recognize true threats and pinpoint attack sources.

IPS-1 Dashboard brings a new level of information presentation to your network by allowing security operations personnel, tier NOC staff and event analysts to

**Check Point
has brought a
new approach
to designing
dedicated
intrusion
prevention into
your network.**

collaborate using the same set of powerful information tools to identify, investigate, validate, remediate and report on important or exceptional intrusion events.

At the heart of Check Point's new approach is an attempt to tie threat and intrusion prevention to the needs of the business. Operating managers, from the CIO down the chain of command, describe their security requirements in business terms (projects, applications) not in arcane exploit or threat descriptions.

Based on the most important or revenue-dependent business applications and services running in the network, a focused comprehensive set of threat 'packages' may be injected at whatever interval operational needs require. This also brings the need

for robust network devices that were designed for frequent library updates. This can be challenging for host-based IPS systems or those deployed on modified PC architectures. These devices may become unstable, unreliable, failure prone or require reset during or after updates to their signature/protection libraries.

Dynamic Shielding Architecture

Dynamic Shielding Architecture leverages profiled host information to proactively protect the network. Dynamic Shielding Architecture works as follows:

- Receives host- and network-profiled information, either from active scanning tools like Nessus or passive scanning tools like the Dynamic Network Protection component;
- Cross-references that information against the configured signature profiles for IPS-1 and determines appropriate action;
- Takes actions, which could range from automatic updates of signature profiles, escalating the confidence Index of a host and with the release currently in development, the ability to quarantine a compromised machine.

These actions notify the security team of the violation, while providing the best available protection against the rogue server being exploited until the security team has time to investigate the server deployment to determine who deployed it and why. This proactive adaptation of the protection profile relative to the changing dimensions of the security environment ensures much broader network security than what a standard, static IDS/IPS deployment can provide.

Check Point's SmartDefense Research Team (SDRT) delivers these threat library updates containing complete service and application protections. Check Point's protocol-based updates may be configured to automatically update each IPS-1 Sensor or to notify administrators of detailed updates for update during scheduled

maintenance windows – easing the ongoing administration and supporting business needs.

The IPS-1 Dynamic Shielding Architecture™ is truly a breakthrough in intrusion prevention security and it is the foundation of Check Point's Aware, Adaptive and Actionable network security. While standard IPS products are static in nature, the IPS-1 Dynamic Shielding Architecture™ automatically recognizes these stealth attack threat points that exist on your network – such as unsanctioned network changes, and critical vulnerabilities – and dynamically protects those threat points from the inevitable attacks.

Another unique differentiator that Check Point brings to the Intrusion Prevention market is the concept that security managers have unique needs for management – for network visibility – that cannot be met with conventional network infrastructure management tools.

Today's requirements for security analysts are not device-based like ordinary SNMP-monitored network equipment. Real-time intrusion prevention requires architecture and tools designed to display patterns of potentially threatening data flows in several dimensions. IPS-1 Dashboard provides more flexibility and control with tighter integration and more uniform information presentation to establish 'best practices' incident response procedures highlighted by a ("3 Click" IP Packet Export for Forensics).



Check Point™
SOFTWARE TECHNOLOGIES LTD.

www.checkpoint.com

Check Point and Nokia: An Innovative Approach To Meeting



Networks are changing fast and threats are fast-changing. Security appliances must adapt to the performance demands created by the former and rise to the challenge of the latter, ensuring that users can continue their work unimpeded by throughput problems or hacks that wreak havoc on the network.

"Overwhelmingly, the IT metric that matters the most is information productivity," says Bill Jensen, product marketing manager at Check Point Software Technologies, a worldwide market leader in the firewall, data security and VPN markets. "Can people get the information they need in a timely manner? Is the IT infrastructure being productive?"

It's not an easy metric for IT leaders to measure up to. Performance needs are spiking with the proliferation of technologies such as VoIP and multimedia applications, and the distribution of servers throughout the business to branch offices that must be

able to communicate with each other. At the same time, security threats have become more insidious, evidenced by the trend of malicious activity disguising itself as innocent applications. "It's good traffic gone bad. It looks like it's supposed to be good, and a traditional firewall would think it was good, but in reality there's a Trojan horse hiding within there," says Jensen. "It takes a heck of a lot more processing power to really ferret that out. Instead of just looking at the envelope of this package, you have to look at the entire content." Check Point and Nokia – strategic partners who, for nearly a decade, have together delivered innovative Internet security solutions – are making sure IT leaders don't have to compromise on security in order to deliver to their organization's intense information availability demands. The new Nokia IP 2450 security platform for firewall/VPN, with Check Point's CoreXL software, takes advantage of the latest Intel open-platform quad-core CPUs and

acceleration technology to maximize the power inherent in the processors, and the protection that comes with being able to do deeper inspections of more sizes and types of packets faster than ever before.

Generally, one of the cores in a multi-core system can be expected to achieve 100% utilization, but others are likely to be less efficient, running at 20% or 30% utilization. With CoreXL, that utilization approaches 100% for all the cores. What it means for customers, Jensen explains, is that they can start activating integrated intrusion prevention on the firewall, achieving up to 1.8 gigabits per second throughput with 70% of intrusion prevention settings turned on. That's typical of what is required for a web server that sits face-to-face with the world of external threats. With 30% of intrusion detection settings activated even higher throughput can be achieved – up to 5.3 gigabits per second.



New Demands and Fighting Threats



Nokia and Check Point have partnered with Intel on its open-platform processor architecture as an alternative to ASIC-based firewalls, for good reason. For one thing, on many ASIC-based systems, performance can drop by roughly 95% with just a single intrusion prevention setting activated. That drop-off has lead many organizations to buy an

additional intrusion prevention or intrusion detection system and sit it right behind the firewall. "Now, there are uses for intrusion prevention and intrusion detection – there is no doubt about this – but as a cover for what the firewall should be doing is not one of them," says Jensen. The Nokia IP2450 security platform enables them to avoid making these extra purchases, helping them to master security sprawl and reduce the complexity of their security infrastructure.

Another reason to choose open platforms over custom ASICs is that ASIC-based systems are not well equipped to deal with today's application-layer threats, which can morph at an alarming rate. ASIC-based systems are programmed to do a very specific task very fast. But businesses need both speed and agility in their security systems. They require platforms that can adapt to security threats that may take on new forms on a near-daily basis, and businesses can't upgrade ASIC-based systems to handle this problem without

losing performance. "When people were looking at these ASICs, they thought they were getting increased productivity because these things were supposed to go blazingly fast," says Jensen. "But now, with the shift to application layer threats, that information productivity is threatened."

An advantage of the joint Check Point and Nokia IP2450 solution is that companies can automatically upgrade the appliance protections to manage new and morphing threats, if they have a software subscription to Check Point's solution or belong to its SmartDefense services. "You can upgrade that joint solution automatically, you are going to have a predictable level of performance – which we know CIO's love – and as you go into the future, you can continue to keep that one appliance and continue to upgrade it as new protections and new capabilities come out," he says.

Such capabilities ensure that IT managers are able to meet the business demands for productivity and performance, as well as satisfy their needs to have in place an insurance policy against the wide world of threats. After all, the only time IT leaders are ever really measured on security is when something bad happens, and it's been a frustrating trade-off for them not to be able to get the performance and protection they need in a single solution.

Nokia and Check Point work closely together to integrate their core strengths into the Nokia IP2450 security platform, as well as other joint products aimed at protecting your business. As Check Point continues to enhance its CoreXL software, for example, Nokia has improved platform performance with its accelerated data path technology. A dedicated research and development team at Check Point is charged with making sure that Nokia customers continue to very quickly get its

most advanced security technology, such as the SmartCenter management infrastructure or plug-ins that add functionality to that platform. The two vendors also perform joint quality assurance testing to make sure that everything meets both companies' satisfaction before it goes out to corporate sites.

Additionally, all customers benefit from the fact that Check Point and Nokia technology is battle-hardened, thanks to its use in some of the most demanding environments, such as on trading floors and behind the world's largest financial exchanges. "It's been in the places where it gets attacked quite often and quite severely, and it's held up," says Jensen.

The Nokia IP2450 security platform is just the latest example of how Check Point and Nokia are ensuring that customers get both protection and the performance they need to meet their information productivity requirements. No one knows what the next threats will be or where they will come from, but customers of the joint Check Point-Nokia solutions know they'll be able to deal with whatever heads their way.

NOKIA

www.nokiaforbusiness.com



Akibia News

Akibia's Data Center Relocations

Leveraging 20 years of experience managing, supporting and optimizing multivendor data center environments, Akibia has the expertise to effectively and efficiently complete your data center move, from dismantling and moving systems, to tracking and testing and bringing the systems back online. Whether consolidating data centers, moving to a new location to reduce power and facility costs or moving as part of a disaster recovery plan, Akibia is the right partner to help make your move a success.

As an independent multivendor maintenance and support provider with twenty years of data center expertise, Akibia is uniquely suited to manage your entire data center relocation. As a result of our in-depth technical expertise in Sun Microsystems, Hewlett Packard, Compaq and Dell hardware platforms, as well as UNIX, Linux and Windows operating environments, you can rest assured that your critical systems will be seamlessly relocated by Akibia. Leading global companies rely on Akibia's Data Center Relocation Services for a variety of reasons:

- **Experienced Project Management** - Akibia will expertly plan and execute your entire data center relocation and assume total accountability for successfully bringing your systems back online.

- **Multivendor Data Center Expertise** - Akibia's expertise in multivendor servers and operating systems allows us to act as a single point of contact for your move.
- **Minimal Downtime** - We partner with our clients to design a relocation plan that minimizes system downtime and the impact on existing business operations.
- **Data Center Optimization** - Akibia can help you address critical data center concerns such as server utilization, performance, capacity planning and consolidation, to ensure your new data center is optimized for performance and supports future growth requirements, while containing costs.

Our services include a pre-move audit to catalog the systems being moved, asset management, bar-coding and packing of the systems, vendor and insurance coordination, transportation of systems and re-installation at the new site. For more information about Akibia's Data Center Relocation Services contact your sales representative or visit: www.akibia.com/support/support/relocations.

Thought Leadership - The perception of security is important to your product success

By **Ken Smith**, PRINCIPAL SECURITY CONSULTANT, AKIBIA

Whether you are selling enterprise software, hardware, or providing internet-based services, your prospects perception of your security posture is tantamount to your product's success.

Organizations are becoming increasingly demanding in relation to security when they bring new products into their IT environment or sign up with new Software as a Service (SaaS) solutions. Many prospects will require your product solution to meet rigorous standards and be subject to their own vulnerability assessment before making a purchasing decision. Some will require a third party vulnerability assessment be performed on a quarterly or annual basis.

Many solution vendors have become quite diligent in their security efforts related to product development and testing. But the work doesn't end when you release a new product. You must wrap security around the way you sell, implement, and support the solution.

While undoubtedly you have taken steps to ensure the security and integrity of your product, it's important that the prospect gets the feeling that you understand security

For example, I once witnessed a product company lose a substantial deal because the sales rep used an antiquated and insecure method

to remotely access his own network for the product demo. The prospects information security staff quickly pointed out that this isn't the type of thing that a company that understands security would allow to happen.

In another instance I saw a large deal grind to a halt when the prospect's security staff was informed that the new product installation team would be doing their integration and customization work remotely, using a third-party remote access solution that would essentially be opening up an encrypted back-door into the company's network.

Another area where solution providers tend to slip on security concerns is when supporting their products remotely. It's important to understand your prospect's security policies and have some well thought-out options ready. For example, many larger organizations will frown upon your plan to install a VPN device on their network in order to provide remote support.

Developing a good security story around your product and the way you implement and support your customers will go a long way. These efforts will pay off with increased customer trust and loyalty.

Akibia's Proactive Systems Monitoring Service

Akibia's new Server Monitoring and Performance Reporting Service is a proactive service that assists enterprises in reducing unplanned downtime by continuously monitoring the organization's server environment on a 24x7x365 basis, and notifying their designated IT staff immediately in the event of an issue, according to the terms of their Service Level Agreement (SLA). This enables the client's IT staff to quickly put in place corrective action that minimizes unplanned server downtime.

When Akibia's server monitoring service is combined with Akibia's world-class system maintenance services, Akibia assumes responsibility for issue resolution - Akibia's technical support team diagnoses the issue, identifies the corrective solution and dispatches a field engineer with the appropriate parts to resolve the issue, where necessary.

Akibia's new server monitoring service combines our extensive data center experience and state-of-the-art infrastructure to ensure we deliver the highest quality server monitoring service to our clients.

Customers that take advantage of Akibia's monitoring service, are able to capitalize on the following key benefits Akibia provides:

- **Increased Systems Uptime and Availability** - Unplanned downtime is lowered through issue avoidance and reduced time-to-repair, in the event of a failure.
- **Increased IT Staff Productivity and Efficiencies** - The IT staff is more proactive in dealing with server issues, which frees up time that was once spent fixing problems to focus on more strategic IT initiatives.
- **Cost Avoidance on Monitoring Tools and Infrastructure** - By leveraging Akibia's state-of-the-art infrastructure, enhanced monitoring and management systems, extensive technical expertise and best practices, organizations avoid the cost of hiring and training the required staff, as well as acquiring, managing and maintaining the necessary tools and infrastructure to deliver 24x7x365 server monitoring.
- **Optimized Infrastructure** - Akibia's monitoring service includes detailed reporting and analysis on systems utilization and performance, as well as historic trending data - enabling clients to maximize the value of their IT infrastructure. Akibia also provides clients with access to our senior engineers to help interpret the reports and make recommendations on how to optimize their environment.
- **Plan for the Future** - The broad suite of reports available through Akibia's server monitoring service helps clients better understand how their environment is performing. Our advanced reporting capabilities educate clients on their environment and provide valuable input to assist them with capacity planning - allowing them to make more informed buying decisions based on a thorough understanding of their existing systems utilization rates.
- **Reduced Risk and Increased Control** - Leveraging our in-depth data center expertise across a wide-range of hardware platforms and operating systems, Akibia's server monitoring service provides clients with the peace-of-mind that their IT infrastructure is stable and operating efficiently. When an issue arises, Akibia's engineers will efficiently and effectively analyze, validate and isolate the issue in the context of the client's environment, and contact the customer according to the terms of their SLA.
- **Compliance** - Akibia's proactive server monitoring service enables clients to demonstrate due diligence from a compliance standpoint.

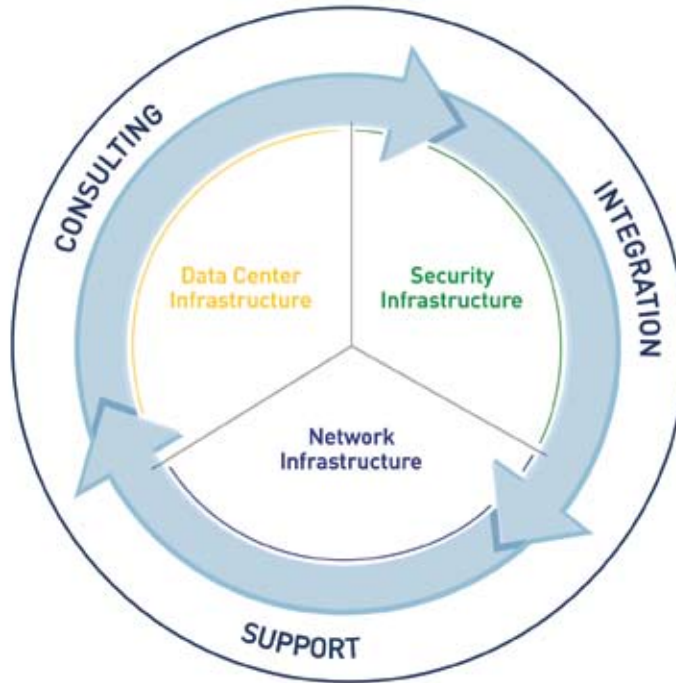
Akibia Hits 20 Year Milestone

Founded as an independent service provider in 1988, Akibia has grown steadily over the past twenty years because of our commitment to customer service and our flexibility in delivering customized solutions that fit our customers needs. At Akibia we recognize this milestone could not be reached without the support of our customers and partners. Many of our customers have been with us since day one, we hope our newer customers will obtain the same value year in and year out, from Akibia's data center and network and security services. We look forward to many more years of shared successes and milestones with our customers and partners.



Akibia Portfolio Overview

Enabling Your IT Infrastructure



CONSULTING

- Infrastructure Consulting
- Risk Management & Compliance
- Security Strategy & Policy Development
- Digital Forensics
- Data Center Optimization

INTEGRATION

- Microsoft Infrastructure
- Security & Network Infrastructure
- Messaging & Content Security
- Identity & Access Management
- Vulnerability Management

SUPPORT

- Multivendor Systems Maintenance
- Proactive Monitoring
- Data Center Relocations
- Hardware Procurement
- 24x7 Firewall Support
- Education
- Managed Services



OPTIMIZE



SECURE



MANAGE



SUPPORT

For an electronic copy of the current or past issues of Bandwidth, please visit www.akibia.com/knowledge

Akibia, Inc.
4 Technology Drive
Westborough, MA 01581

USA: 1-866-4-AKIBIA
EMEA: +31 (0) 318 581950
www.akibia.com

PRESORTED
FIRST CLASS MAIL
U.S. POSTAGE
PAID
N. READING, MA
PERMIT NO. 254