Bandwidth

Network & Security Solutions Publication – Summer 2007

IN THIS ISSUE...

An Introduction to Digital Forensic Investigations

Digital forensics is considered a subset of the incident response genre and an important aspect of a company's overall security initiative. Learn more about the incidents behind the digital forensics movement and how to approach a digital forensics investigation.

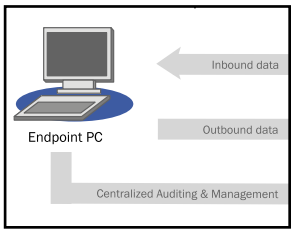
Read more from Akibia on page 4

Citrix Application Delivery Infrastructure

Citrix offers an end-to-end application delivery strategy that makes it easy to deliver any application to any user with the best performance, highest security, and lowest cost. Discover four critical best practices to follow to ensure your applications meet your business goals.

Read more from Citrix on page 6

Preventing Data Leaks on USB Ports with Pointsec



Enterprises are becoming more aware of the risks of data leaks that evade control by traditional layered security technologies, such as the USB port on endpoint devices. Pointsec Protector simply and effectively regulates access and data for any plug-and-play peripheral.

Read more from Check Point on page 8

TABLE OF CONTENTS

Bandwidth is a publication of akibia®

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

EDITOR'S CORNER

In this issue of *Bandwidth*, we are featuring an article on Digital Forensics by one of Akibia's Senior Security Consultants, Evan Wheeler. While working with Evan on this article and the introduction of Akibia's new Forensic services, it was interesting to learn about the ways he has used his forensics skills and knowledge to help several of our clients in ways that I would not have considered a "forensics investigation."

Whenever I hear "forensics," I immediately conjure up images of one of the many CSI episodes that are airing on TV. Scientists, crime scene investigators, and law enforcement are all part of the aura that surrounds "forensics." Within the corporate environment while the cast of characters may not be quite as dramatic, a forensics investigation can impact a broad cross section of the organization.

In working with Evan, and talking to clients, I learned that forensic readiness for an enterprise is not merely about being ready for possible legal actions, but is an important part of a life-cycle management process used within the organization's information technology program.

As you'll learn in Evan's article, one of the areas that benefits most from forensic readiness is an organization's incident response plan. By considering the steps and process that a forensic investigation would take, a company may make some changes to their incident response plan. Their response plan may be modified to include steps that would preserve data and the chain of custody for investigative purposes during an incident response. For others, new scenarios and contributors may be added to their plan that were not originally considered.

Another area impacted that I hadn't considered was how a forensic investigation might change an organization's provisioning process. In preparing the tools, systems, and processes needed to conduct a forensic investigation, an IT department may add steps to their provisioning process that would allow them to store, recall, and deliver device configurations to a third party or internal investigation team at a moments notice. The time it takes to deliver baseline configurations of devices is an integral part of the overall response time for both a forensics investigation, as well as an incident response. Depending on an organization's capability maturity, this may spawn entirely new processes and documentation about their configuration sets, or merely be an additional step in a well established provisioning program.

In both these scenarios, by considering the impact and scope of a forensic investigation, an enterprise can enhance existing programs and processes - enhancements that can help a business be more responsive to the daily operational challenges they face and improving the maturity of their IT programs.

Tim Richardson
Product Marketing Manager, Akibia, Inc.

Akibia Data Center Solutions Customer Case Study: A Leading Financial Services Firm Increases Data Center Efficiencies and Reduces IT Support Costs by Over $1 Million with Akibia

As a major financial brokerage firm, Akibia's customer puts significant requirements on its data center, including demanding the highest level of uptime for mission critical systems. Because of unique demands resulting from the nature of its business systems, administrators and engineers are prohibited from fixing systems during trading hours. Therefore, the company required a custom support contract for systems maintenance and a flexible partnership with its support vendor. The company was wasting money and time because its existing support vendor was unable to adjust to this schedule.

Because the brokerage firm leverages multiple Sun systems for different applications, with different uptime requirements, they were forced to manage many different SLAs with their existing hardware support vendor. This was cumbersome and difficult to manage, especially because the service provider often missed the SLA requirements. In addition, the management of these many systems and the replacement and addition of new systems was time-consuming and burdensome for the company's busy IT staff.

In all, these challenges created a situation that was difficult and frustrating. The data center manager understood that switching to a third party support provider that could customize a solution to better fit his unique requirements would not only reduce his frustrations, but also save the company money.

Solution

For a solution to the company's support issues, the data center manager knew that he had to look beyond the traditional hardware vendors to a third party support provider that would partner with the company to create a flexible and cost-effective support solution. Akibia was that partner. Akibia supports over 130,000 systems worldwide.

As a result of this wealth of experience, it was clear that Akibia had the expertise, infrastructure, processes and best practices to best support the company's needs. Akibia was able to provide a solution that would allow the company to work more efficiently and take advantage of support during off hours.

To address the company's challenges Akibia listened to their needs and created a unique solution. The solution included a single, customized service level agreement that recognized the off hours in which Akibia would be able to access the data center and fix systems. The single SLA, as opposed to the multiple SLAs the brokerage company was managing with its previous vendor, significantly reduced the administrative burden and lowered support costs for the data center manager and his team. With Akibia, the company will save approximately one million dollars in support costs over three years.

The company reports that Akibia routinely exceeds its SLA, a marked improvement from its last vendor and a direct result of Akibia's ability to understand unique challenges and present a solution that fits the company's needs.

In addition, the firm moves quickly to keep pace with demands for high-levels of uptime and embraces innovative technology, making it difficult for the team to maintain an updated record of all the systems in the data center, their warranties and lifecycles. Therefore, Akibia has assumed responsibility for managing the company's system moves, adds and changes, resulting in more effective and efficient technology lifecycle management.

Results

Millions of dollars worth of electronic transactions cross the company's systems on a daily basis. The company's business success, to some degree, can be attributed to their ability to leverage technology. As a result, significant demands are placed on their data center. Working with Akibia has enabled the company to improve systems uptime and enhance the level of service and support provided by their data center for the trading environment – while at the same time realizing approximately one million dollars in cost savings over three years.

With improved service levels and lower overall support costs, the team can now focus on more mission-critical projects, while still continuing to ensure the highest level of system uptime in the trading environment.

A Customized Data Center Support Solution Saves Time and Money

Challenge: A major financial services company wanted to reduce frustrations and complexity, while improving performance related to its data center support services.

Solution: Akibia customized a unique support solution that included a single SLA and a dedicated support engineer on-site.

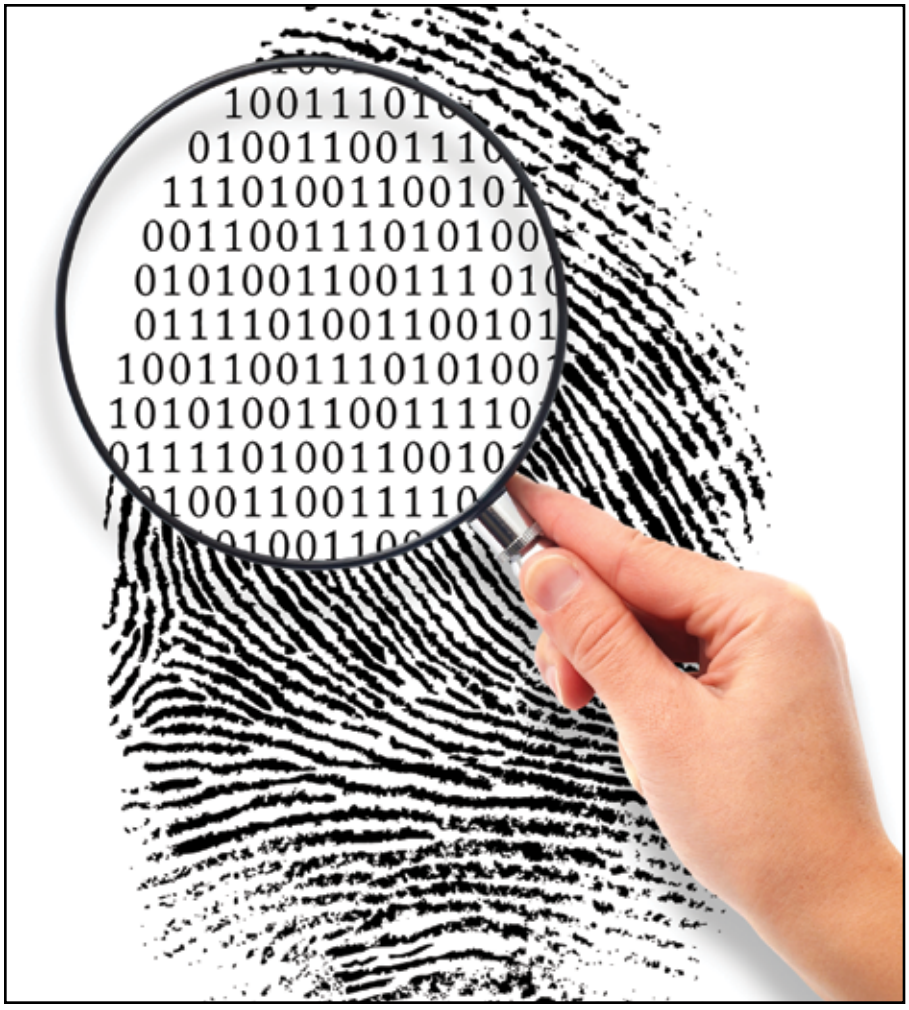
Result: The company reports Akibia routinely exceeds its service level agreement and data center performance levels have increased. In addition the company will save over $1 million dollars on data center support.

akibia®

www.akibia.com

An Introduction to Digital Forensic Investigations

By Evan Wheeler, CISSP - SENIOR SECURITY CONSULTANT, AKIBIA



What is Digital Forensics?

Digital forensics as a discipline is not particularly new however, in the past it was usually associated with law enforcement investigations of computer-related crimes. More recently, it is becoming increasingly common for high profile corporations, especially financial services companies, to have fulltime resources dedicated to battling the onslaught of cybercrime and malware keying in on these profitable institutions. In today's changed landscape, digital forensics is considered a subset of the incident response genre and an important aspect of a company's overall security initiative.

Often the distinction between forensic investigation and incident response is blurred, but in principle not every security incident will require a forensic response. For instance, a virus outbreak among several user workstations may require an incident response team to engage in order to contain the spread of the virus and clean the infected systems. In this case, it may be evident that the source of the outbreak was an infected email sent to a user, and uncaught by perimeter email scanning, perhaps because it was a brand new variant with no existing signatures. Typically, this type of incident would not require further investigation. However, a digital forensics investigation would be necessary if the source of the virus was unknown; if efforts to eradicate it were continually unsuccessful; if the impact on the infected systems was unclear; and if the scope of the infected systems was unknown. This scenario would require specialized personnel who were skilled at system compromise analysis and malware reverse engineering. While this is just one potential incident that would require a forensic investigation, there are a number of others that would necessitate a similar investigation including financial fraud, internal security policy violations, system vulnerability exploits, e-discovery, and sensitive data leakage investigations.

As high profile security breaches continue to make headlines, companies can no longer afford to be in the dark regarding incident response and investigative capabilities. It is important for all organizations to be proactive about possible incidents. Organizations should develop a strategy for approaching a forensic investigation, identify the appropriate partners to leverage during an incident and ensure a thorough understanding of the total security framework and how it would stand up to a digital investigation. Forward-

thinking risk managers and security professionals are focusing not just on implementing specific compensating controls to mitigate traditional technical weaknesses, but they are also spending time and resources planning for various incident handling scenarios similar to a disaster recovery exercise. This planning inevitably involves strong incident response policies, procedures, training, and communication, but also will require digital forensics.

The Incidents Behind the Digital Forensics Movement

So how does digital forensics fit into the incident response landscape and why has it gained so much momentum and publicity recently? Partially this is a result of an increase in corporate emphasis on enforcing more detailed security and acceptable use policies. The "newsmaker" potential of these security incidents, and the ensuing public relations challenges, as well as advances and sophistications in technology are combining to increase the need for digital forensics.

Security policy violations, such as misuse of the Internet, or illegal access of customer data, are gaining the attention of management and human resources. Any time management chooses to pursue a security incident, a strict procedure must be followed to maintain the forensic integrity of the evidence collected and to avoid accusations of prejudice by internal staff involved in gathering and analysis of evidence. For example, recent case law has shown that when administrative action is taken against an employee, and the evidence is based solely on an IP address that was associated with that user's system, the action will not hold up in court. Therefore it becomes important for human resources as well as corporate legal council to be familiar with the company's forensic investigation approach.

Similarly, security incidents on the network are being detected more often due to improved network security controls such as Intrusion Detection Systems (IDS) and security information management systems. As more incidents are detected, it is obvious that more will need to be investigated.

How To Approach a Digital Forensic Investigation

It's hard to prepare for the unexpected, yet in the case of digital forensic investigations, this is a necessity. It is critical for IT, HR and legal to become educated regarding the possible scenarios the organization might face. From there the groups can create a prioritized action plan for reducing the time and resources required to perform forensic incident response activities.

To determine your organization's forensic readiness, it is vital to evaluate the current security posture and analyze technical controls, policies, procedures and skill sets. A skilled forensic investigator can analyze these results and recommend an action plan to fill the gaps identified. This process greatly increases the efficiency of any investigation whether it is performed internally, by a third-party, or even involving law enforcement. Although in this article we are focused specifically on the digital forensic aspects of the incident handling lifecycle, this preparation also increases a company's ability to efficiently respond to any security incident.

Should your organization need to conduct a digital forensic investigation it is important to work with a trusted, third party advisor. Digital Forensics is a very specialized field and to conduct an investigation accurately, and without losing or misinterpreting data requires significant expertise. Maintaining discretion in the investigation is an absolute necessity and a third party can ensure the investigation is conducted without bias or prejudice.

Akibia offers Digital Forensic Services, and you can learn more about our offering on page 15 of this issue of *Bandwidth*.

About the Author: Evan Wheeler, CISSP

As a Security Consultant working in many industries for over ten years, Evan Wheeler is accustomed to advising clients on all aspects of Information Assurance. Specializing in risk management, digital forensic investigations, and secure application design, he offers an expert insight into security principles for both clients and security professionals. Evan has spoken to many audiences on topics ranging from Payment Card Industry (PCI) risk management to building a forensic incident response infrastructure. He currently leads the forensic investigation team as a Senior Security Consultant for Akibia Network & Security Solutions, Inc. and maintains a role as a Security Advisor to the High Performance Computer Modernization Program within the U.S. Department of Defense. As a complement to this diverse experience in the field, he is currently pursuing a Master of Science in Information Assurance at the National Security Agency certified program at Northeastern University.

Register to attend Akibia's Live Webinar on Digital Forensics on Tue., June 19, 2007 at www.akibia.com/about/events.

akibia®

www.akibia.com

Citrix Application Delivery Infrastructure

Whether large ERP solutions or custom web apps, email or e-commerce, client-server applications or SOA, your success in IT today depends on ensuring that your applications help meet your business goals. If the infrastructure you rely on to deliver business applications to end-users wasn't designed with modern application realities in mind, you end up massively over-provisioning, buying too much bandwidth, adding too many servers, and refreshing PCs on an increasingly short lifecycle just to keep up with growing application requirements.

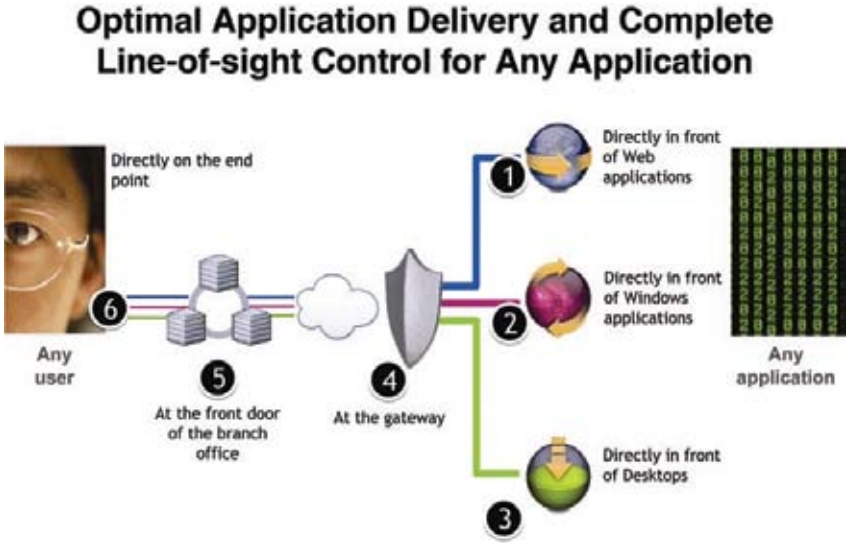
Citrix believes that businesses can avoid these costs and enhance IT agility with an end-to-end application delivery strategy:

- a strategy that includes infrastructure solutions deployed along the line-of-sight between data centers and end-users
- a strategy that makes it easy to deliver any application to any user with the best performance, highest security, and lowest cost
- a strategy featuring products that work great with your existing infrastructure, and even better when deployed together.

Starting from the data center and working out toward the end-user, there are four critical best practice objectives to keep in mind.

Control Applications at their Source

An end-to-end application delivery strategy starts with infrastructure products that are deployed in the data center, directly in front of applications – controlling the initial delivery of applications as close as possible to their source. Web applications are extremely verbose and carry far richer content than client-server applications, creating massive increases in application traffic. They are much easier to exploit, opening new data security risks. The combination of these factors dramatically slows application performance, driving up the cost of servers and bandwidth, and increasing data security risks. To address the challenges of Web application delivery, companies need to look to integrated application networking products, such as the Citrix NetScaler product line, which goes beyond traditional load balancing; optimizing application traffic over the network by incorporating advanced technologies like compression, caching, and security.



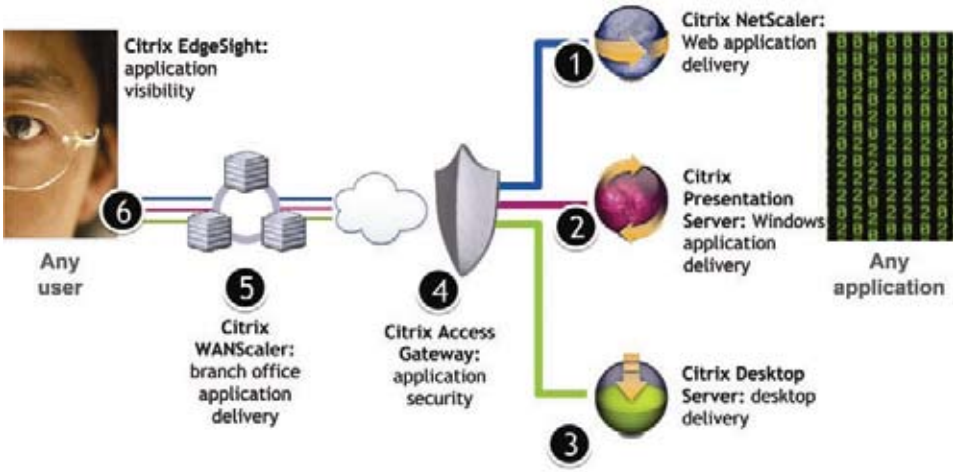
With Windows applications, the issues are much different. The traditional approach is to install each application on every end user's PC, then attempt to manage, upgrade, patch, and maintain them at the endpoints. This model quickly creates huge problems with cost and complexity that grow exponentially as applications and users are added or changed in any way. The Citrix Presentation Server product line offers a far better solution, by installing applications one time in the data center and virtualizing or streaming their delivery over the network. This approach dramatically improves the cost, simplicity, and security of managing Windows applications without compromising the end-user experience in any way.

A well-designed application delivery strategy should also incorporate Windows desktops, as they represent the primary operating environment through which employees access their applications. Major technical advances in recent years have made it possible for the first time to deliver highly dynamic virtual desktops over the network to office workers with zero compromise in end-user experience. This model can dramatically improve the economics, simplicity, and security of traditional desktop management. The Citrix Desktop Server is one example of a solution designed to address this challenge.

Secure Access to Applications

A second key consideration in a successful application delivery strategy is making it easy for users to securely access their applications from any location. Citrix Access Gateway is a next generation SSL VPN that is much easier to install and is specifically designed to provide application-layer access to the exact application resources each user needs. It goes beyond simple network access, with SmartAccess, a unique capability that gives IT control over which actions a user can perform within each application based on his or her unique access scenario. A user accessing a corporate application from an office computer, for example, might be able to use all application functions, while that same user connecting from an untrusted external location might be able to view application data, but not save or print.

Citrix Application Delivery Infrastructure Products



Optimize Applications over the Wide Area Network

As a result of trends like user mobility, globalization, and outsourcing, more than half of all employees at mid to large sized enterprises now access their applications from branch offices. Traditional networks were never designed to deliver the kind of application traffic they are expected to handle today, especially as companies consolidate data centers and start pushing applications like voice and video over the network. Citrix WANScaler is a WAN optimization product specifically designed to address this problem by automatically optimizing all application traffic over the wide area network, an approach that can dramatically improve application performance and reduce bandwidth requirements by as much as 75 percent.

Monitor the End-User Experience

The success of any application delivery strategy rests on the ability of IT to truly monitor the experience of end users, especially with regards to application performance. Citrix EdgeSight gives IT visibility into exactly what the application experience feels like for end-users making it much easier to maintain service level agreements with business stakeholders, spot bottlenecks before they become issues, and quickly diagnose problems when they do occur.

Unlike a few short years ago, businesses today run on applications. In an increasingly volatile world where you face a dizzying array of changes to applications, users, and business climates, making application delivery a strategic imperative is no longer an option. Contact Citrix to learn more about application delivery infrastructure and how these four best practice objectives can help your business.

CITRIX access PARTNER
SILVER
Solution Advisor

www.citrix.com

Payment Card Industry (PCI) Compliance

Sponsored by a collaboration between MasterCard, Visa, American Express, Diners Club and the Discover Card, the Payment Card Industry Standard (PCI) is an effort to protect consumer information and fight Internet fraud through required best practices for securing credit card data that is stored, processed or transmitted by an online retailer. All merchants who process or store credit card transaction data must comply with PCI regulations.

Objectives to Meet PCI Compliance

To achieve compliance, merchants and service providers must adhere to PCI security standards, which offer a single approach to safeguarding sensitive data for all card brands. The PCI security standard is a framework of twelve basic requirements supported by more detailed sub-requirements. Log monitoring and reporting is mandated under Requirement 10 in PCI's 12-step process that instructs companies on how to achieve compliance.

Specifically, PCI requires organizations to:

- Regularly monitor and test networks
- Track and monitor all access to network resources and cardholder data

RSA enVision® has automated this compliance requirement by creating mapped reports that allow organizations to capture and report on the logs from network, security, infrastructure and application-layer events. RSA enVision reports provide your organization with a complete picture of network usage and audit trails for user identification, success and failure indication, origination of event and validation of user views of information.

To achieve those objectives, PCI requires that companies monitor and audit the following types of activities:

- Access Control monitors attempts to access anything on a company's systems including files, directories, database records or applications.
- Configuration Control monitors the configuration, policies and software installed on systems covered by a particular compliance regulation and all systems with access to that system.
- Malicious Software capabilities detect, collect and report malicious activities caused by viruses or other malicious code.
- Policy Enforcement verifies that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- User Monitoring and Management creates a complete audit of the activities of non-employees with access to private data and takes steps to minimize the risk from compromised accounts.
- Environmental and Transmission Security involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA

scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

To achieve and maintain compliance in those areas, companies must use the following functions with respect to the data collected by the RSA enVision Log Management solution:

- Collect, Protect and Store data in a non-filtered, non-normalized fashion that is stored in an efficient and protected manner.
- Establish Baseline levels of activity for the entire system and network environment to define "normal activity" and detect unusual levels of activity.
- Report summary and detailed reports for the mandated periods of time.
- Alert companies to deviations from baseline activities and complex patterns of activity across multiple, disparate devices.
- Debug systems to correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
- Establish Incident Management capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

These functions ensure that the administrative, physical and technical control demanded by PCI regulations are maintained. RSA enVision solutions address all of the technical standards required.

The RSA enVision Internet Protocol Database

Using its advanced LogSmart® Internet Protocol Database™ (IPDB) architecture that is deployed in hundreds of enterprises worldwide, RSA enVision is able to capture All the Data™ from network, security, host, application and storage layers across the enterprise. The LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization from the IT department, to the security department, to the compliance and risk officers and executive management.

The benefits of the LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively without any filtering or data normalization
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered - unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance

Compliance Alerts

RSA enVision provides the ability to automatically generate alerts based on non-compliance with specific regulations and the detection of unusual levels of activity. Such incidents trigger alerts so action can be taken to maintain compliance.

The PCI standard identifies several core IT Security technologies, as well as various processes and procedures, needed to protect cardholder data. To address these requirements, RSA, The Security Division of EMC and Akibia can help your organization by delivering a PCI Solution, which encompasses a range of IT Security technologies, as well as assessment and policy development services.

For more information, contact your Akibia sales representative.

The rising tide of consumer data loss: 100 million records and counting

Over the past few years, hundreds of CEOs have awoken to find their companies in the unenviable position of disclosing the loss or theft of private consumer information, such as credit card and social security numbers. The tide of data breaches has swelled since February 2005, when a leading supplier of identification and credential verification services, announced that over 160,000 consumer records were accidentally sold to identity thieves. In fact, the Privacy Rights Clearinghouse tracked over four hundred instances of consumer data compromise in the U.S. alone-totaling over 100 million personal records in the 23 months following the disclosure. The problem is global and cuts across industries: retailers, hotels, local and federal governments, healthcare organizations, universities, and financial institutions were all forced to report consumer data compromises over the past two years.

RSA®

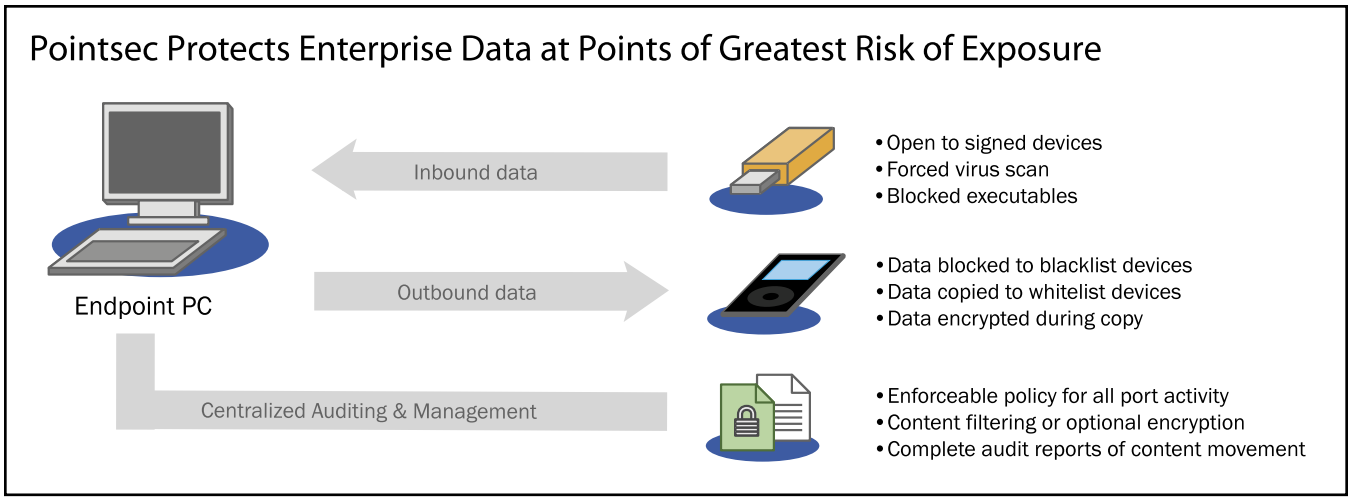
The Security Division of EMC

www.rsasecurity.com

Industry-Leading Solutions for Mobile Data Protection

Preventing Data Leaks on USB Ports

Pointsec Protector from Check Point Simply Regulates Access and Data for Any Plug-and-Play Peripheral



USB Ports are New Vector for Data Leaks

Organizations are under big pressure to do a better job securing enterprise and personal data. A continuous flow of news stories show that data leaks are widespread. According to the Privacy Rights Clearinghouse, more than 100 million records containing private personal information have been lost or stolen since the massive leak from ChoicePoint in 2005. Odds are the real number is higher due to reluctance by organizations to disclose data leaks or related problems with cyber security.

The public scrutiny, embarrassment, financial and judicial penalties triggered by data leaks has stimulated steady efforts to strengthen security. Among the "most critical issues" are data protection, compliance, data leaks, viruses and worms, and access control, according to a recent survey by the Computer Security Institute and the Federal Bureau of Investigation's Computer Intrusion Squad. In addressing these issues, enterprises have discovered a requirement to deploy different solutions that solve particular vulnerabilities at each layer of the networked information system.

Enterprises are becoming aware of another significant vector for data leaks that evades control by traditional layered security technologies: the innocuous USB port on endpoint devices.

USB stands for Universal Serial Bus, an interface standard natively supported by popular operating systems such as Windows, Mac OS X, and Linux. USB has become commonplace for keyboards, printers, televisions, home stereo equipment, video game consoles, and storage-related devices. Unfortunately, the technology that has streamlined the operational cost of interconnection also has become a critical point requiring the attention of security administrators.

The last category is a point of danger for data security because people constantly plug personal storage devices into their work PC to upload music, wallpaper images, or transmit digital photos over the Internet. Their intent may be innocent. But the ability to also siphon off corporate data from an endpoint through the USB port onto a portable storage device places organizations at considerable risk.

How USB Exposes Endpoints to Leaks

A standard corporate desktop PC may have up to eight USB ports. Some are required for peripherals such as a keyboard or security token reader, but there are usually one or more unused ports. By default, USB ports are "always on," ready to serve any USB-enabled device that is plugged into the endpoint computer.

An enterprise may chose to disable USB via the Windows Group Policy and an ADM template. Unfortunately, this capability is an all or nothing policy and does not provide administrators with granular control. This approach is limiting because of the need for USB capability on the endpoint.

Ease of Data Movement with USB Storage

A typical device in this category is a USB flash drive, which stores digital files on NAND-type flash memory. The flash drive may also be called a "USB key," "pen drive," "thumb drive," or "chip stick." When a flash drive is plugged into an endpoint's USB port, the endpoint computer's OS automatically recognizes the device, loads its device driver, and enables file transfers with Windows Explorer or similar applications. Some endpoints may allow execution of programs that are stored on a flash drive.

The USB flash drive appears to a user exactly like another internal drive on the endpoint computer, making the plug in capability ideal for sneaking out sensitive data from the enterprise. The flash drive is not the only USB device capable of swift and secret data theft. Users may employ any of the USB storage devices mentioned above for the same purpose.

POD Slurping and Other Techniques

Stealing data with USB storage does not require a long script. One simply plugs the USB storage device into a USB port, fires up Windows Explorer and drags target files onto the storage device. This action can be performed by a malicious insider, or even a well-meaning insider who is trying to do their job but is unaware of security policies that might otherwise prevent a data leak.

One of the most popular USB storage devices is the iPod. Consequently, some people have coined "Pod Slurping" as a hip term for transferring files to a USB storage device.

A synonymous term is "camsnuffling," which applies to using a digital camera to photograph documents or objects and then transfer them to an unauthorized recipient. Likewise, "bluesnarfing" entails stealing data from a wireless device through a Bluetooth connection.

> ...the ability to also siphon off corporate data from an endpoint through the USB port onto a portable storage device places organizations at considerable risk.

Whatever the term, it's very easy to move digital files from an endpoint to a USB storage device. And once data has moved to a small storage device, it's usually easy to carry it outside the enterprise and on to nefarious use by unauthorized people.

A Simple Solution for USB Port Security

Pointsec's Protector is a simple software-based solution for enterprise-wide control of storage device access through USB and other I/O ports, and of the data flowing through those connections. It provides a policy-driven port security system to a system administrator for granular control of USB access to endpoints that denies all access (black list), provides read-only access or allows full authorized access (white list).

The level of control is configurable by a security administrator, which is critical for striking the best balance between security and cost. In some enterprises, implementing a rigid security policy puts new strain on end user work patterns. Pointsec's objective is to offer a customized endpoint security solution that minimizes changes to end user behavior, while also addressing the most critical elements of your security policy.

Learn More

Pointsec Mobile Technologies, the global leader in mobile data protection, invites you to contact us for more information about Pointsec Protector as a simple solution for enterprise-wide port security. Deployment is rapid, automatic and non-intrusive. Centralized management and operations makes Pointsec Protector an efficient, cost-effective way to control data leaks through USB ports. Pointsec is a Check Point Software Technologies company.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions.

To learn more, please contact your Akibia sales representative at 508-621-5100, or visit www.checkpoint.com/products/datasecurity/protector/index.html.

Check Point™ SOFTWARE TECHNOLOGIES LTD.

www.checkpoint.com

Nokia Extendable Security Appliances

By Farzaneh Yassini - PRODUCT MARKETING MANAGER, NOKIA

Like so many other factors changing in our world, the firewall market is also evolving. The new trend is leaning toward one that extends security appliance functionality and offers stronger investment protection. Security appliances are doing more and are designed with features which can extent product life. This integrated and extended network security platform approach will provide customers with improved security and lower total cost of ownership. As proof points, Nokia is introducing Nokia IP290 security platform – delivering a unified threat management (UTM) platform ideal for small office/branch offices and extended enterprises and Nokia IP690 with a new hardware design supporting multi-core and multi-threading technology and allowing further expandability and performance improvements through add-on interface cards and software upgrades.

Nokia IP290

New security threats, such as viruses, worms and malware are affecting business uptime, and IT resource constraints are driving the need for simple security appliances that mitigate multiple threats. Purpose-built to support advanced security solutions such as unified threat management (UTM) and intrusion prevention (IPS), Nokia IP290 provides performance, expandability and the full set of Nokia secure OS and management tool benefits to secure small and branch offices.

Nokia IP290 multi-purpose security platform is a powerful yet cost-effective security appliance supporting traditional firewall and next generation security applications such as IPS and UTM – including firewall, VPN, intrusion protection, anti virus and web filtering. The small form factor design allows for side-by-side redundancy in a single 1RU space providing a low-cost/high availability solution ideal for IP Clustering or VRRP technologies. Nokia IP290 is ideal for small office/branch offices and extended enterprises that require robust performance combined with simple remote management and high reliability at a low total cost. Nokia IP290 offers the same level of protection in remote locations as in the corporate office, combining market-leading Nokia hardware design and quality with Check Point VPN-1 UTM software and Nokia IPSO™ OS for maximum security, high availability, reliability, affordability, and manageability.

Key Features

- In one compact Nokia appliance, IP290 offers UTM capabilities that go beyond traditional firewall/VPN to include anti-virus and URL filtering
- Six ports of 10/100/1000-Base-T (RJ45) Ethernet
- Optional add-on interfaces include 2 port 1000-Base-X and 2 port 1000-Base-T Ethernet
- Flexible architecture of Nokia IP290 allows IT to granularly expand the platform to meet the needs of a growing business
- Modular design allows field upgradeability without the need to de-rack the system for maximum uptime
- Renowned Nokia hardware design, optimized for security application performance, coupled with Nokia IPSO OS and management tools for an appliance purpose-built for small companies and branch offices
- Offers advanced features like IPSO Flows, VRRP, Clustering and powerful CLI scripts and GUI interface
- Slide-out tray for easy serviceability

Nokia IP690

Enterprises and service providers are faced with a variety of security challenges today. Threats are becoming more sophisticated, security solutions need to perform deeper packet inspections, changing traffic patterns demand higher appliance throughput performance across all packet sizes, and reducing IT costs and expenses mean organizations need higher return on their network security investments. Nokia IP690 was designed with these concerns in mind.

Nokia IP690 is the first Nokia security appliance to deliver a new hardware design supporting multi-core and multi-threading technology, allowing further expandability and an order of magnitude performance improvement through add-on interface cards and software upgrades. You can deploy now and expand capacity as needs grow, without costly hardware forklift upgrades. This versatile, purpose-built platform is designed to meet the most demanding network requirements for large enterprise firewall security. It features excellent price performance for mixed-packet-size real-world network traffic and for networks that need robust performance for firewall and VPN traffic. Nokia IP690 can also be deployed in high availability environments with support for Virtual Router Redundancy Protocol (VRRP) and Nokia IP Clustering, delivering enhanced business continuity.

Nokia IP690 extends network security capabilities through an optimized, expandable rack dense platform designed for supporting next generation security applications while delivering IT investment protection. By deploying Nokia IP690 this year, you will have opportunities to improve and upgrade the solution at the time of choice. First, through updating Nokia IPSO, you will be able to take advantage of the multi-core architecture and improve overall system performance. Second, through the add-on Accelerated Data Path interface, customers get a further boost in performance for small packet throughput. And Nokia IP690 is ready to support next-generation, multi-threaded security applications.

Key Features

- New hardware design supporting multi-core, multi-threading technology
- Optimized to run computationally intense features of Check Point VPN-1 and VPN-1 UTM firewall applications
- 2 GB RAM (expandable to 4)
- Flash or hard disk drive (HDD) based
- 4 GB compact flash for flash based systems
- 40 GB HDD (optional 2nd drive available)
- Redundancy and port density for large enterprise demands
- Slide-out tray for easy serviceability
- Redundant, hot swappable power supplies
- 4 front-facing PCI expansion slots, supporting up to 16 Gigabit Ethernet interfaces
- 4 Port 1000 Base-T interface card (pre-populated)
- Nokia IPSO™ operating system, designed for network security
- Includes SecureXL Check Point VPN-1 and Check Point VPN-1 UTM traffic acceleration
- Includes VRRP and IP Clustering HA functionality
- Includes dynamic and multicast routing
- Nokia Network Voyager and Cluster Voyager WebUI for local and remote administration

NOKIA

www.nokiaforbusiness.com

Akibia News

New Akibia Partnerships

Akibia Partners with Citrix and FaceTime

CITRIX access PARTNER
SILVER
Solution Advisor

Effective application delivery requires an end-to-end strategy incorporating key infrastructure solutions deployed along the line-of-sight between data centers and end users. The Citrix application delivery infrastructure product line includes best-in-class solutions designed to work well with a company's existing infrastructure and even better when deployed together.

Citrix Systems, Inc. is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the Fortune 100 companies and 98% of the Fortune Global 500, as well as hundreds of thousands of small businesses and prosumers.

FaceTime Communications is the leading provider of security solutions enabling businesses to secure and control greynet applications such as instant messaging, adware/spyware, webmail, P2P file sharing, web conferencing and instant voice. Ranked number one in market share among instant messaging management vendors for the third consecutive year, FaceTime's award-winning solutions are used by more than 800 customers including nine of the ten largest U.S. banks. FaceTime Security Labs delivers the industry's first IMPact Index, which assesses "point-in-time" risks posed by viruses, worms and other malware propagating through greynet applications.

FaceTime®

Akibia Training

Akibia has a 20-year history providing IT services and support, including custom education courses for both Network & Security and Data Center technologies.

Network & Security Solutions

Akibia serves as the largest Check Point Authorized Training Center in the Northeastern United States. Check Point training classes are scheduled monthly at Akibia.

Akibia is the first Infoblox Authorized Training Center in the United States. Our courses ensure Akibia and Infoblox users are able to maximize the value of their DNS, DHCP/IPAM appliances. Akibia's next Infoblox training class will be held on September 18 - 20, 2007 in Westborough, MA.

To discuss your needs for Network & Security educational courses, please contact Dominic Agostino at 800-818-8070 x4508 or dagostino@akibia.com.

Data Center Technologies

Akibia's new courses for Data Center Solutions are taught in our state of the art training facilities in Westborough, MA and Austin, TX. They can also be taught on-site at the client location. All courses are taught by experienced, certified instructors and are designed to meet the specific requirements of each student. The courses focus on practical, hands-on experience that students can immediately apply to their daily operations. Akibia's new courses include:

- Solaris 10 Differences for Solaris Administrators
- Solaris 10 Resource Management, Configuration and Tuning
- Solaris 10 Introduction to Administration and Troubleshooting
- Solaris Large System Performance
- Fibre Channel and Storage Area Networks Concepts

For a complete list of Akibia's Data Center educational courses, please visit www.akibia.com/support/education/

Akibia Introduces Digital Forensic Services

Akibia's Digital Forensic Services help organizations identify and obtain digital evidence of improper use of corporate systems and unauthorized access of sensitive data and intellectual property.

With concerns over protecting corporate reputation and customer data at an all time high, organizations must be diligent in identifying and routing out improper use of corporate information and systems. These threats can include improper use of Internet access; exposing customer data and personal information through improper channels; data leakage; system infection and malicious use of corporate data and intellectual property for personal benefits and financial gain. Companies are often required to conduct digital forensic investigations that evaluate the nature of a potential security breach, determine the impact on the organization, and provide evidence, thereof, if necessary.

Digital forensic investigations demand a specialized expertise that Akibia is able to provide. Akibia's security team has significant experience helping organizations develop a complete security framework and implementing critical security applications that reduce risks. As a result, the team brings broad expertise to digital forensic investigations which require in-depth knowledge of the various systems within a client's IT infrastructure environment.

Maintaining the integrity of the data collected and not contaminating the evidence through the investigation are of the highest importance. Akibia's team is recognized by ISC2 as CISSP certified and certified as a SAN GIAC Incident Handler. Akibia's consultants understand how to identify, log and report evidence. Given the potential use of the results of Digital Forensic investigations, including employee termination or administrative action, proper handling of the investigation is an absolute necessity. Akibia's Services include:

- ***Forensic Readiness Assessment***
  It is important for organizations to be proactive in identifying internal threats to information. In delivering a Forensic Readiness Assessment, Akibia's expert consultants help companies identify the appropriate policies, technologies and procedures that should be implemented in order to build a security framework that will support a forensic investigation, should one be necessary.

- ***Digital Forensic Investigation***
  Akibia's Digital Forensic Investigation services is a complete investigation of the potential incident. Akibia's team leverages proven best practices to ensure the integrity of the investigation. Results are reported back and data is presented in a format designed to provide the organization with comprehensive evidence. In addition, Akibia includes recommendations on how to prevent the investigation from happening again.

Learn More about Akibia's Premier Data Center Support Services

Akibia is a leading provider of multivendor data center support and maintenance services including Sun, HP, Compaq and Dell hardware, as well as Solaris, HP-UX, Windows and Linux operating systems. Visit our promotions section at www.akibia.com and see if you qualify for **"One Free Month of Hardware Support Service"** or learn how you can optimize your data center by signing up for Akibia's **"Free Systems Utilization Analysis."**

Akibia Events

Visit www.akibia.com/about/events for more information on Akibia's upcoming seminars and events.

akibia

Payment Card Industry Compliance

Validate the security of your customer data with a Complimentary Compliance Readiness Analysis

Is your organization still struggling to comply with the Payment Card Industry Data Security Standard? Partner with Akibia, and you can leave it to us. **Akibia is a Qualified Data Security Company (QDSC)** authorized by Visa to provide on-site assessment services for all major credit card security programs.

Compliance does not always equal security - the challenge is to achieve compliance while maximizing security. As an independent security solutions provider with 20 years of experience, Akibia provides the expert consulting, integration, training and support services you need to implement a comprehensive security solution.

For more information or to schedule your **complimentary Compliance Readiness Analysis with Akibia** visit **www.akibia.com/compliancereadiness** or call **1-866-4-AKIBIA x4677**. Offer expires 8/31/07.

What is an Akibia Compliance Readiness Analysis?

An Akibia Compliance Readiness Analysis is a **90-minute workshop** where one of our **Qualified Data Security Professionals** will work with you and your team to **identify gaps in compliance**, using the PCI Data Security Standard Self-Assessment.

Who Will Benefit from a Compliance Readiness Analysis?

Organizations facing any of the following security challenges will benefit from an Akibia Compliance Readiness Analysis:

- **Protect credit cardholder data**
- **Meet the 12 sections of the PCI Data Security Standard**
- **Understand your options for Intrusion Prevention Systems and Encryption technologies**
- **Build and maintain a secure network**
- **Maintain a vulnerability management program**
- **Regularly monitor and test networks**
- **Implement strong network access control and measures**
- **Build and maintain an information security policy**

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

Akibia, Inc.
Network and Security Solutions
4 Technology Drive
Westborough, MA 01581
phone 1-866-4-AKIBIA
www.akibia.com

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