

THE EVIL FROM WITHIN

Addressing the Growing Specter of the Insider Threat

Challenge

The growing specter of insider threats causes many headaches and sleepless nights for organizations. Insider threats can not only be launched by a malicious user, but by other insiders that include partners and contractors. Insider threats can also be caused by simple, internal user errors and abuses.

Solution

Juniper Networks addresses and mitigates insider threats. Led by Juniper Networks security solutions and the interoperability of its complete security and access control product portfolio, Juniper Networks empowers organizations to defend their businesses from dangerous, costly insider threats.

Benefits

- Keep critical data safe and secure
- Ensure that only the “right” people can access sensitive applications and data
- Protect your network, applications, users and data from contamination
- Safeguard your business and reputation

The increased velocity of business has forced organizations to face challenges that years ago were not even considered. One of the biggest challenges involves a security issue that has taken center stage and threatens the very existence of the enterprise. In 2008, the “outside-in” attacks have been eclipsed by the insider threat, both in terms of the sheer number of incidents and also the associated dollar figure for damage that can result from this type of breach. The average dollar figure for damage due to an insider attack has grown by over 108 percent in just 12 months. The question that begs to be asked is this: While we continue to deploy security, why are organizations at greater risk than ever before?

The Challenge

Traditional security assumed that the threats which enterprises needed to protect against came from somewhere outside of their network. As a result, security deployments focused on providing perimeter-based protection.

The insider threat opens up a whole new attack vector which bypasses the perimeter security strategy. Employees are the most often cited insiders who compromise the organization’s security but they are certainly not the only insider threats. Insiders consist of anyone who has access permissions above and beyond the general public. This can include partners, contractors, and guests—just to name a few. For our purposes, we will examine two of the more common insider threats involving the organization’s employees.

Good employees unknowingly doing bad things: In this case, an employee commits an act that unknowingly and unintentionally exposes a network to risk. This includes actions such as internal errors, abuses, sloppy use, and ignoring security safeguards. A recent case involved a trojan that was unknowingly placed on a legitimate site. Users accessing this site had their PC’s quickly compromised. When the user logged into the corporate network, the implanted script began harvesting password and user credentials, shipping them off to the hacker without the user’s knowledge. An innocent employee visit to a legitimate Web site exposed the organization to substantial risk with no knowledge or malicious intent.

Bad employees exhibiting bad behavior: A disconcerting trend is the increased incidence of trusted employees who knowingly expose their organization to risk. Disgruntled employees and those looking to inflict harm to the organization are among the biggest security threats because they know the network, know what security is in place, and know how to best “fly under the radar” to avoid deployed security and detection.

The Motivation

Some insider threats are launched to “get back” at the organization. A recent case that made the news was an IT manager who had left the organization, but also left a logic bomb behind which was set to erase critical data two weeks after his departure from the organization.

In other cases, the insider will knowingly expose the organization for his/her private financial gain. This was the case with a New York-based hospital where a billing clerk sold patient insurance information to a third party who then resold it to patients who required a procedure but did not have health insurance. The damage was twofold because not only was an identity stolen, but the legitimate patient’s health records were no longer accurate, as procedures were being performed on a person who claimed to be the legitimate patient but was not.

The Exposure

Regardless of the motivation behind an employee committing the “insider threat,” the results can be devastating to the organization, to the shareholders, and to an individual if their credentials are involved in the breach. Attacks occur quickly and are usually over within hours to days. Unfortunately, the detection of an attack has historically not been as fast, often taking weeks or even months to detect. This is particularly concerning because the breach has been committed and the breached data is long gone before the breach is ever discovered and acted upon by the organization.

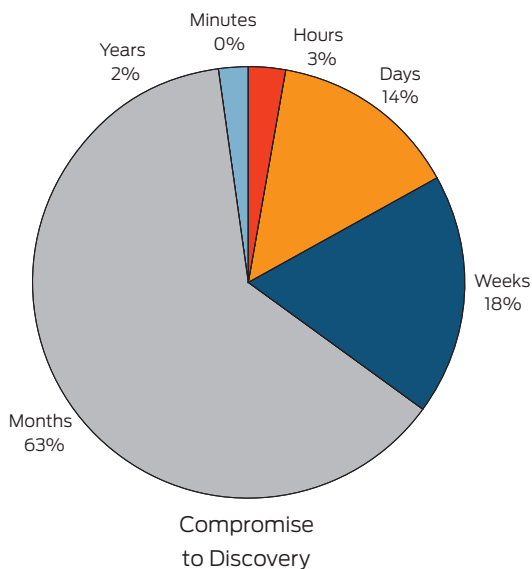
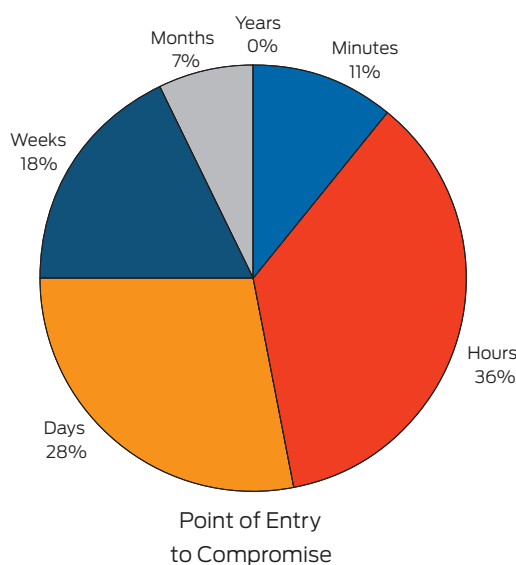
In the case of an insider threat, the breach can affect the organization’s bottom line as was the case with CardSystems. At one time, CardSystems was among the world’s largest dealer of credit card transactions. With a breach that exposed tens of millions of credit cards and CVV2 security code information, CardSystems business and reputation were irreparably damaged and the company was ultimately forced out of business.

The Juniper Networks Access Control Solution

Juniper Networks® has long recognized the insider threat as a key challenge for both IT and business lines. As such, Juniper has architected an answer to help organizations plug this highly volatile and potentially most damaging security hole exposing the organization to unacceptable risk.

Several key tenets were employed to architect this solution:

- Ensuring that the “right” people have access to the right information and applications. The sheer volume of personnel accessing critical network resources expands almost daily. The heterogeneous audience demands a granular access control that ensures that only authorized personnel get access to the resources they require and nothing more. Locking down everything else helps to limit exposure and is a good start at securing the network.
- Organizations are fluid. New employees are hired, roles within organizations change, and people leave organizations. It is essential that permissions and access rights are fluid and change as employee roles within organizations change. Furthermore, it is important to verify the identity and role of the individual before allowing access. Challenging the employee helps ensure that the user is, in fact, the stated individual.
- Sometimes employees with the appropriate access will take advantage and commit a breach with the data to which they rightfully have access. For security forensics as well as compliance, it is essential to log who is accessing what, and when. Moreover, reporting information must be complete, easily accessible, and simple to understand. This provides the virtual paper trail necessary to quickly react to any potential breach—both from a security and a compliance perspective.
- As indicated earlier, some of the biggest insider breaches are a result of an infected endpoint contaminating the network. Starting clean helps to ensure that your network stays clean, and this is done through ensuring that endpoint devices are



Source: Verizon Business “2008 Data Breach Investigations Report”

clear of infection from viruses, keyloggers, trojans, worms, and other malware. If a device (whether it is a corporate device or third-party/unmanaged device) is infected, it is important to limit access (for example, quarantine the infected device) until remediation is complete. In order to ensure minimal disruption, self remediation may be indicated where employees are able to take action on their own to cleanse their infected endpoint and attain or regain network access as quickly as possible.

- Visibility and control must be complete. It is impossible to find or report on security without a single and comprehensive view of the network from both a real-time and historical perspective. Aside from saving on OPEX costs, it is the only way of getting an accurate picture on the security posture of the organization.
- Gone are the days of “rear view mirror” security. It is no longer acceptable to wait weeks to months in order to ascertain that a breach has occurred (see diagram above on Verizon study). The ability to detect, mitigate, and report on exploits and breaches must be in real time. This means that the various deployed security elements must work together and collaborate in rooting out those attacks that are stealthy, sophisticated, and built to evade traditional security point products. It also means automating the tedious process of log correlation, which is still largely done on an ad hoc and/or manual basis. This, however, can only be relied upon with a highly accurate solution that is able to take multiple feeds from multiple vendors into account, and deliver a prioritized list of violations that are actionable at a moment’s notice.
- Not every violation requires a complete shutdown. Blocking traffic every time a suspicious incident occurs simply does not address the requirements of today’s high performance business. Rather, it is important to select the “appropriate response” based on the violation that has occurred. This may include actions such as rate limiting, reporting, quarantine, or update.

Features and Benefits

Juniper delivers a comprehensive solution to address and mitigate insider threats with Juniper Networks Adaptive Threat Management Solutions and Juniper Networks Unified Access Control:

- Ensuring that only the “right” people can access the network, sensitive applications and data by verifying the identity and role of individuals and devices before they are allowed access to the network, applications, and data.
- Preventing infected devices from accessing and contaminating the network.
- Detecting anomalous or malicious behavior on a network, and taking fast, explicit action before the threat can proliferate
- Log and report on who is accessing specific applications, when, and from where, simplifying insider threat tracking

Solution Components

Juniper Networks’ insider threat solution incorporates and integrates the award-winning products that populate Juniper’s network, security and access control product portfolio, including:

- Juniper Networks IC Series Unified Access Control Appliances, the policy management server at the heart of UAC
- Juniper Networks SA Series SSL VPN Appliances
- Juniper Networks family of firewall platforms, including the Juniper Networks SSG Series Secure Services Gateways and Juniper Networks ISG Series Integrated Security Gateways
- Juniper Networks EX Series Ethernet Switches
- Juniper Networks IDP Series Intrusion Detection and Prevention Appliances
- Juniper Networks Network and Security Manager
- Juniper Networks STRM Series Security Threat Response Managers

Summary—Mitigating the Insider Threat

The good news is that Juniper Networks has done the heavy lifting when it comes to securing your business against the insider threat.

Juniper Networks security solutions work across heterogeneous network environments to deliver investment protection, and leverage existing network infrastructure to deliver comprehensive network and application access control and security. Juniper is able to deliver a complete solution to address and mitigate insider threats. Integrating and interoperating with Juniper’s complete portfolio of award-winning access control and security products. Juniper’s security solutions are the foundation through which organizations can successfully defend their networks and businesses from the scourge of insider threats.

Next Steps

For more information about Juniper Networks products and services, please visit www.juniper.net.

For additional information about Juniper Networks security solutions, please visit www.juniper.net/security.

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.