BDNA

BDNA for Security

Strengthened Security Through Visibility

Introduction

Whether in the physical realm or the digital, security professionals understand that one of the most important elements of strengthening one's defenses is visibility. A thorough and detailed picture of one's IT estate is key to the ability to protect that infrastructure from both outside and inside threats.

In late 2006, a major clothing retailer in the US found themselves with a problem. Over the course of several months, internal IT intrusion detection systems showed repeated attempts to access internal systems, including those responsible for processing credit card transactions. Strangely enough, the intrusions originated not from outside the company, but appeared to come from two specific stores inside the company's network. Probing into this breach, investigators found that the two stores had incorrectly deployed a company-nonstandard wireless networking device. Furthermore, the wireless access point installed at these two locations was both a model with a known weakness and also misconfigured, making it relatively easy for hackers to attack it and the systems attached to it.

Hackers exploited these compromised wireless devices to launch further attacks throughout the company, eventually compromising financial and operations systems. During the ensuing investigation, the company learned that the attacks on the non-standard and misconfigured wireless network devices resulted in the disclosure of more than forty-five million credit card records, the largest such breach up to that time. The estimated cost of the resulting cleanup and legal settlements associated with this attack amounted to a quarter of a billion dollars.

"Millions of dollars wasted, angry customers, and untold embarrassment for the executives at this company ensured, simply because no one in the organization could knowledgably answer the question, 'What do we have?'"

So, how did a breach of this magnitude occur? Clearly a chain of failures, both procedural and technological, had to have taken place. The compromised wireless access points were nonstandard, and were not configured properly. Appropriate intrusion detection measures were not in place, or were not operational. Neither was sensitive customer data protected by a properly deployed and configured encryption solution.

All of these failures, though, stem from the same root cause—lack of visibility. Lack of visibility into devices connected to the enterprise network. Lack of visibility into the operational state of security software throughout the enterprise infrastructure. Lack of visibility into the deployment of encryption software or hardware. Millions of dollars wasted, angry customers, and untold embarrassment for the executives at this company ensured, simply because no one in the organization could knowledgeably answer the question, "What do we have?"

Visibility into IT Security falls primarily into four categories:

1. Asset discovery, the enumeration of all physical and virtual devices connected to the enterprise network. This can be broken down further into lists of known devices to be protected, and lists of unknown (or rogue) devices from which an organization must be protected.

2. Application software inventory, the list of applications running on each known asset. Each application is a potential attack surface, or a potential point of weakness that attackers may seek to exploit. Knowing the full extent of all applications deployed on corporate endpoints provides security administrators with a clear, concise picture of their organization's potential attack surface. And, like its hardware sibling, rogue software presents its own set of threats to be managed.

3. Security measures themselves. Once deployed, security software such as enterprise antivirus, data leakage protection, or intrusion protection must be monitored to ensure that they stay deployed, properly configured, and continuously running.

4. Regulatory and standards compliance. Compliance with external and internal mandates has resulted in a number of data collection and reporting challenges, each requiring deep visibility into IT operations.

Rogue Assets

What is a rogue asset? A rogue asset is, simply, a piece of hardware or software brought onto a corporate network or company-owned PC without the knowledge or authorization of the organization's IT department. Individual users or department dissatisfied with company standard hardware or software can introduce rogue assets—often with what they believe to be the best intentions. Regardless of the source, these rogue assets are at best a potential technical support sore point, or at worst, a security mushroom cloud waiting to happen. Unfortunately, the ill effects of rogue assets often spread beyond the individual user or work group and often impact the entire organization. For this reason, security managers need awareness of hardware and software running on everything connected to an enterprise network.

Rogue Hardware

One of the most common examples of rogue assets that potentially impact corporate networks is the user-owned laptop. For a variety of reasons, many employees may prefer to use a machine they own, rather than the tools the organization provides for them. While many employees may optimize their productivity while using hardware of their choosing, the lack of IT oversight and visibility into these workstations poses several operational problems for the organization:

- Is the operating system and software on the user-owned computer patched according to the prevailing organizational standard?
- Is the computer configured correctly to meet organizational or regulatory compliance security standards?
- Does the computer run effective anti-virus software, and is it up-to-date and correctly configured?
- Are all the software products on employee-owned computers legally licensed for commercial use?
- Does the computer act as a carrier (such as an active botnet client) of potential external threats to other workstations within the organization?
- Is the user of this rogue computer accessing sensitive or confidential data, and is any of this data ending up, either intentionally or unintentionally, on the hard drive of this unmanaged computer?

Clearly, user-owned computers pose a number of security issues. There are both proactive and reactive security measures that can be used to mitigate these threats, such as Network Access Control or MAC address-level connection control. But before organizations install any technical protections, they still need visibility into the presence of undocumented assets wherever they appear on an enterprise network.

"The net effect of [compliance] on the practice of security is that it's no longer just enough to be effective in protecting an organization from attack. You must be able to thoroughly document exactly how effective you were, and any and all measures taken to be effective."

Rogue Software

The companion to the problem of rogue hardware is rogue software, or software running on company-provided hardware, that has been installed by and end user or a group of users, outside the sanction or support of the IT department. Many of the same issues pertaining to rogue hardware apply as well to rogue software, but rogue software raises some specific questions:

- What is the source of this software? Is any of it pirated? Is it an academic or "home" version unlicensed for business use? Is it otherwise free of malicious code?
- Does this software cause any interoperability or compatibility problems with other sanctioned applications?
- Is the application properly patched, and are there any known vulnerabilities with this software that may pose a threat to other computers around the organization?

Again, and as with rogue hardware, technological measures can mitigate the threat of rogue software being deployed on company IT assets. The deployment of full workstation lockdown solutions or application control software agents are two such measures, but these have many drawbacks that prevent their becoming a blanket protective measure against rogue software. Visibility is still needed into the scope and nature of what end-users, workgroups, and the enterprise itself are deploying.

The Rise of Compliance

Like the IT organizations it protects, the day-to-day business of information technology security has changed dramatically over the past fifteen years. One of the biggest changes has been the rise of external compliance mandates. A complex array of local and national legislation supplemented by industry self-regulation initiatives has appeared, requiring recordkeeping, audits, and disclosure requirements that were unknown a decade ago.

The net effect of this on the practice of security is that it's no longer just enough to be effective in protecting an organization from attack. You must be able to thoroughly document exactly how effective you were, and any and all measures taken to be effective. The additional recordkeeping and data collection associated with regulatory compliance add significant complexity and cost to information security management. A 2005 study from the University of Nebraska reported that Sarbanes-Oxley compliance costs the average publicly traded corporation $2.3 million annually. Much of this cost comes labor required to gather information, inspect security configurations and adhere to internal standards.

STANDARD	AFFECTED ORGANIZATIONS
Sarbanes-Oxley (SOX)	Any publicly traded company
Gramm-Leach-Bliley Act (GLBA)	Institutions handling financial information
Payment Card Industry (PCI	Any organization handling credit or debit card information
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Any organization handling healthcare information, including health insurers and organizations providing healthcare to their employees
Federal Desktop Core Configuration (FDCC)	Any US Government agency
Federal Information Security Management Act (FISMA)	Any US Government Agency

The chart above summarizes some of the legal and organizational mandates that many security professionals have to contend with: Each of these regulations comes with its own set of standards for not only information protection, but also recordkeeping and reporting. The common thread to all these best practice standards is that demonstrating compliance requires extensive visibility into the security posture of your organization.

Security Tool Visibility

In 2008, ChoicePoint, a major consumer data aggregator based in the United States, attracted some unwanted news coverage. For the second time in three years, it had been the victim of an information security breach resulting in the disclosure of thousands of credit and consumer records. This second breach, however, was unique, in that it occurred after extensive security measures were implemented in response to the first breach. The problem was that ChoicePoint "turned off a key electronic security tool used to monitor access to one of its databases, and for four months failed to detect that the security tool was off." To put it another way; even with robust security measures in place, lack of visibility into their implementation of those security measures resulted directly in another embarrassing and expensive attack.

"There is no shortage of security tools and practices—antivirus and personal firewall, data leakage protection, application control, antispyware, network access control, application whitelisting/blacklisting, policy enforcement—each of them requiring management and maintenance."

There is a lesson to be learned from ChoicePoint's problem. There is no shortage of security tools and practices—antivirus and personal firewall, data leakage protection, application control, antispyware, network access control, application whitelisting/blacklisting, policy enforcement—each of them requiring management and maintenance. But ensuring complete and continuing coverage is also a problem. How do you know that up-to-date security agents are deployed on 100 percent of the PCs in your environment? And, even if you have reasonable assurance that you've achieved full coverage, how do you ensure that it stays that way? Once again, an independent, objective source of visibility beyond that native to individual security tools can deliver a much needed reality check.

The BDNA Visibility Advantage

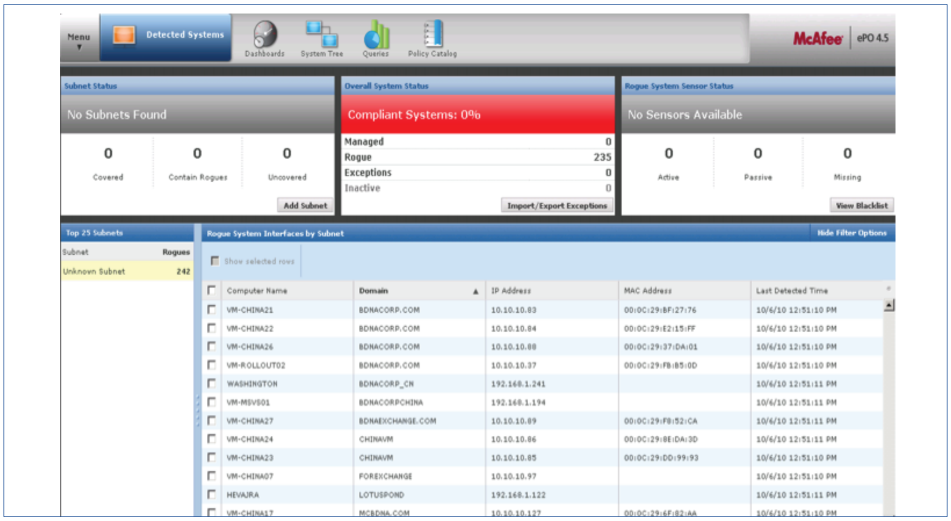
BDNA Discover™—Low Friction Visibility

BDNA Discover is the industry's fastest and least-intrusive way of bringing greater visibility into IT Security operations. BDNA Discover's patented agentless design allows it to be deployed across large distributed infrastructures in a matter of hours, delivering the visibility needed to find and address security issues before they become security problems.

This extensive visibility is particular useful to organizations that have standardized on McAfee ePolicy Orchestrator (ePO) as an enterprise information security solution. Qualifying BDNA as a member of the McAfee Security Innovation Alliance, BDNA's Discover for ePolicy Orchestrator (ePO) has been certified by McAfee for deployment in ePO environments. Here, BDNA Discover acts as an information source for the detection of heretofore invisible devices on enterprise networks. Rogue devices, or those not currently covered by an enterprise ePO solution, made visible by BDNA Discover can be brought under the enterprise security umbrella with a single click in the ePO console. With BDNA Discover and McAfee, achieving and maintaining full security agent coverage becomes an achievable goal.

BDNA DISCOVER FOR McAFEE ePOLICY ORCHESTRATOR

BDNA Discover now integrates with McAfee's ePolicy Orchestrator (ePO), enabling customers using BDNA and McAfee to use the robust agentless IT asset discovery capabilities of Discover as a data source to populate ePO with a list of assets not currently under McAfee management. Computers discovered to be without an ePO agent can be brought under the management umbrella with a single click, and all of the rich information available in BDNA Discover can also be viewed in an ePolicy Orchestrator device view. Using BDNA Discover, achieving 100% security agent coverage is within your grasp.



Subnet Status

No Subnets Found

0	0	0
Covered	Contain Rogues	Uncovered

Overall System Status

Compliant Systems: 0%

Managed	0
Rogue	235
Exceptions	0
Inactive	0

Rogue System Sensor Status

No Sensors Available

0	0	0
Active	Passive	Missing

Top 25 Subnets

Subnet	Rogues
Unknown Subnet	242

Rogue System Interfaces by Subnet

□	Computer Name	Domain ▲	IP Address	MAC Address	Last Detected Time
□	VM-CHINA21	BDNACORP.COM	10.10.10.83	00:0C:29:BF:27:76	10/6/10 12:51:10 PM
□	VM-CHINA22	BDNACORP.COM	10.10.10.84	00:0C:29:E2:15:FF	10/6/10 12:51:10 PM
□	VM-CHINA26	BDNACORP.COM	10.10.10.88	00:0C:29:37:DA:01	10/6/10 12:51:10 PM
□	VM-ROLLOUT02	BDNACORP.COM	10.10.10.37	00:0C:29:FB:B5:0D	10/6/10 12:51:10 PM
□	WASHINGTON	BDNACORP_CN	192.168.1.241		10/6/10 12:51:11 PM
□	VM-MSVS01	BDNACORPCHINA	192.168.1.194		10/6/10 12:51:11 PM
□	VM-CHINA27	BDNAEXCHANGE.COM	10.10.10.89	00:0C:29:F8:52:CA	10/6/10 12:51:11 PM
□	VM-CHINA24	CHINAVM	10.10.10.86	00:0C:29:8E:DA:3D	10/6/10 12:51:11 PM
□	VM-CHINA23	CHINAVM	10.10.10.85	00:0C:29:DD:99:93	10/6/10 12:51:10 PM
□	VM-CHINA07	FOREXCHANGE	10.10.10.97		10/6/10 12:51:10 PM
□	HEVAJRA	LOTUSPOND	192.168.1.122		10/6/10 12:51:11 PM
□	VM-CHINA17	MCBDNA.COM	10.10.10.127	00:0C:29:6F:82:AA	10/6/10 12:51:10 PM

BDNA Normalize can evaluate individual endpoints for installation of McAfee ePO software.

BDNA Normalize—Making Sense of Security Data Overload

Many organizations already have deployed IT operations software such as Microsoft SCCM, IBM Tivoli, or HP OpenView. These purpose-built tools often collect a great deal of information of great use to IT security professionals, but useful security information can get lost in the tremendous volume of operational data collected by these tools. In response to this needles-in-haystacks problem, BDNA has developed BDNA Normalize™. BDNA Normalize allows organizations using existing discovery tools to filter, disambiguate, and enrich operations data to arrive at decision-ready information.

BDNA Normalize can be especially useful for homing in software and hardware asset inventory information required for compliance reporting. Mobilizing operations information for security audit purposes often involves crossing the operations-security chasm. Demonstrating security agent coverage during a compliance audit using only a tool purpose-built for operations is a major chore, potentially requiring many hours of manual reconciliation. BDNA Normalize, however, can automate the operations data filtering and normalizing process, completing this work within hours. In addition, the data produced by Normalize can be published for further use variety of different business systems, such as HRIS, ERP, financial database, and security management tools.

Conclusion

The visibility provided by BDNA solutions can enable and reinforce many IT security best practices. Whether you're considering rogue asset discovery, streamlining a compliance project, or simply want an authoritative list of targets to install a security management tool, BDNA provides the decision-ready information to get the job done.

Headquarters
339 North Bernardo Avenue, Suite 206
Mountain View, CA 94043
T: (650) 625-9530
F: (650) 625-9533
americasales@bdna.com

East Coast
Georgetown Place
1054 31st Street NW, Suite 300
Washington, DC 20007
T: (202) 595-7751
F: (202) 625-8376

Europe
121-123 Rue Edouard Vaillant
92300 Levallois-Perret
France
T: +33 (0)1 41 27 65 42
F: +33 - (0)1 41 27 65 57
internationalsales@bdna.com

Asia-Pacific
202 West Tower, JiaDu Building
64-66 JianZhong Road
TianHe District
Guangzhou
GuangDong Province, China
T: +8620 - 856 13650