Aberdeen Group
A Harte-Hanks Company

April 2013

Virtual Patching and Database Security: An Effective Compensating Control

Recently, independent industry analyses suggest that just four specific endpoint security controls would have successfully protected against at least 85% of cyber intrusions actually experienced, and that only 13% of all possible threat events were observed in actual incidents. Patching promptly is part of highly effective approaches to managing vulnerabilities, but patching is not always practical or even possible — which is why many companies look to virtual patching as an effective compensating control. One prime example: virtual patching in the context of database security.

Patching is Highly Effective … But Is It Always Practical?

As Aberdeen most recently noted in *The Virtues of Virtual Patching* (October 2012), for many companies the process of managing the **vulnerabilities** in their IT infrastructure consumes a significant portion of their limited IT resources, while also keeping them painfully distracted from other projects aimed at innovation and growth. The strategic deployment of selected **compensating controls**, such as **virtual patching**, can provide a kind of protective shield that effectively provides the organization with the flexibility to assess, prioritize, test, and remediate vulnerabilities on their own schedule — a potentially attractive alternative to the value-destroying activities of Patch Tuesdays, emergency patches and workarounds, endless testing, and unplanned downtime. Aberdeen's research has shown that the leading performers leverage virtual patching as a strategy to augment their traditional patch management processes, and to improve the overall efficiency and effectiveness of their vulnerability management initiatives.

Patching and Endpoint Security

The Australian Government's Defence Signals Directorate (DSD) has been garnering some well-deserved accolades lately for its recently updated publication on Strategies to Mitigate Targeted Cyber Intrusions, in which their analysis suggests that four specific endpoint security strategies and controls would have successfully protected against at least 85% of the cyber intrusions that they responded to in 2011:

- **Whitelist endpoint applications**
    - Permit execution of approved / trusted programs
    - Prevent execution of unapproved and potentially malicious programs and dynamic link libraries (.DLL files)
- **Patch endpoint applications**

Analyst Insight

Aberdeen's Analyst Insights provide the analyst perspective of the research as drawn from an aggregated view of surveys, interviews, analysis, and industry experience.

Definitions

√ **Vulnerabilities** are aspects of IT infrastructure that can potentially be exploited, leading to *unauthorized access*, *loss or exposure of sensitive data*, *disruption of services*, *failure to comply* with regulatory requirements, or other unwanted outcomes. Vulnerabilities can stem from many sources, including: software defects, improper configurations, human error.

√ **Compensating controls** refer to alternative countermeasures or safeguards put in place to mitigate specific risks, in lieu of the nominally recommended controls, as a result of legitimate technical or business constraints.

√ **Virtual patching** (*external patching*, *vulnerability shielding*) refers to establishing a *policy enforcement point* that is external to the resource being protected, to identify and intercept exploits of known vulnerabilities before they reach their target. In this way, direct modifications to the resource being protected are not required.

  - E.g., PDF viewer, Flash Player, Microsoft Office, Java
  - Patch or mitigate high-risk vulnerabilities within two days
- **Patch endpoint operating system vulnerabilities**
  - Patch or mitigate high-risk vulnerabilities within two days
  - Discontinue use of Microsoft Windows XP or earlier
- **Minimize the number of end-users with domain or local administrative privileges**
  - Use separate, unprivileged accounts for email and web browsing

When it comes to information security, however, one size rarely fits all organizations. The DSD publication cites end-user resistance to these four controls as "low" for patching and "medium" for application whitelisting and restricted administrative privileges. This may be true in a tightly controlled government / military / defense environment, but in many other corporate cultures these restrictions would be met with abhorrence by end-users who have zero tolerance for anything that is perceived as a barrier to getting their work done.

From an end-user perspective, implementation of the DSD Top Four basically means that no one can install and run any software that isn't approved and enabled by a centralized IT function. Many of us have the experience that these models usually devolve to the centralized IT function being unable to keep up, and to end-users finding ways around these controls to keep up with the everyday demands of doing business. Why not prevent 100% of cyber intrusions, by just disconnecting everyone from the internet?

The DSD publication also makes it clear that these four endpoint security controls tend to have high upfront cost (in terms of *staff*, *technology*, and *technical complexity*) and medium ongoing cost (primarily *staff*) — which not all organizations are willing or able to bear. It's one thing to have a policy that all critical patches must be implemented within 48 hours, but quite another to have all the necessary resources and processes in place to make this happen.

Patching and the Security of Back-End Systems

A result similar to the one generated by the Australian DSD's analysis can be inferred from the excellent analysis of 855 actual incidents shared by Verizon Business, in their 2012 Data Breach Investigations Report. Their very clever "4 A's" threat event framework — referred to as *VERIS* — uniquely classifies each potential event in terms of the *Asset* (what asset was affected), the *Action* (what action was taken on the asset), the *Agent* (whose actions affected the asset), and the *Attribute* (how the asset was affected) — resulting in a concise matrix of 315 distinct possible events. Based on their incident caseload for 2011, however, only 40 (13%) of all possible threat events were actually seen — that is, 87% of the threat-space was not even

Related Research

The "DSD Top Four" controls have the benefit of detecting and preventing cyber intrusions earlier in the **attack lifecycle**:

√ Identify vulnerabilities (i.e., reconnaissance of IT networks and systems)

√ Implement exploits

√ Execute exploits

√ Automate exploits (i.e., run at scale)

√ Modify exploits (e.g., adapt as vulnerabilities are identified and eliminated) in play. As shown in Table 1, 98% of the observed events were the result of **malware** and **hacking**, targeting *endpoints* (user devices) and *servers*.

Overall, 81% of all incidents leveraged hacking, 69% involved malware, and 61% used a combination of both. The simple point is that prompt patching of high-risk vulnerabilities in platforms, applications, and databases should be just as effective a strategy for the security of back-end systems as the Australian DSD found it to be for their endpoints.

Table 1: Patching Protects Against Malware and Hacking, Leveraged in 98% of Observed Events

Frequency of High-Level Threat Events (N=855)		Malware			Hacking		
		External	Internal	Partners	External	Internal	Partners
Servers	Confidentiality, Possession	381			518		1
	Integrity, Authenticity	397			422		1
	Availability, Utility	2			6		
User Devices	Confidentiality, Possession	356			419		
	Integrity, Authenticity	355			355		
	Availability, Utility						

Data excerpted from Verizon Business, *2012 Data Breach Investigations Report*; 36 of 315 high-level threat events are shown
Source: Aberdeen Group, April 2013

So Why Can Patching Be So Difficult?

Trying to keep up with the vulnerabilities and threats that assault enterprise IT infrastructure is an important but often very difficult activity:

- **Important**, because ignoring or deferring patches or configuration changes for known vulnerabilities — in the absence of other compensating controls — is not a responsible strategy, nor is it reasonable for most companies to disconnect their businesses from the Internet.
- **Difficult**, because the total number of malware samples in the threat database topped 100 million in 2012 (source: McAfee Labs *Threats Report*, 3Q 2012), and because dozens of critical updates and vulnerabilities are disclosed week after week — on average, more than 150 per week in 2012 (source: IBM X-Force *2012 Trend and Risk Report*, March 2013). Increasingly savvy attackers adapt and automate their techniques, and emerging technologies such as social, mobile, and cloud create new avenues for attack.

For many companies, investments aimed at dealing with the "unrewarded" risks of vulnerabilities and threats to their IT infrastructure consume a

Definitions

√ **Malware** refers to malicious software or scripts designed to access or harm information resources without their owner's authorization.

√ **Hacking** refers to intentional attempts to access or harm information resources without authorization by thwarting logical security mechanisms. Hacking is usually conducted remotely, lending itself to attacker benefits of anonymity, automation, and scale.

significant portion of their limited IT resources. At the same time, it diverts their attention from managing the type of "rewarded" risks that really matter to management: those that try to create value for their customers and ultimately help to sustain the business. But there's really no way around it: companies who want the compelling benefits of their IT computing infrastructures must also deal somehow with the corresponding vulnerabilities, threats, and risks.

Four Strategic Approaches to Managing Vulnerabilities

How can companies reduce the total economic impact of managing the vulnerabilities affecting their endpoints, networks, servers, applications, and databases? Based on Aberdeen's research, companies adopt four fundamental strategic approaches — all of which can help to reduce risk and lower total cost:

1. **Start sooner** — i.e., reduce the time between the initial disclosure of vulnerabilities and the initiation of remediation
2. **Finish faster** — i.e., increase the speed at which affected systems are remediated, through increased automation
3. **Work smarter** — i.e., prioritize and implement the patches that impact the most critical business processes, or the patches that provide the greatest good for the greatest number of systems
4. **Create more options** — i.e., implement additional protections (compensating controls) to allow additional flexibility for assessing, prioritizing, and deploying patches and configuration changes for affected systems at the time most convenient for the company

When Virtual Patching Makes Sense

Virtual patching is a prime example of the "create more options" strategy. Sometimes known as *external patching* or *vulnerability shielding*, virtual patching refers to establishing a **policy enforcement point** that is external to the resource being protected, to identify and intercept exploits of known vulnerabilities before they reach their target. In this way, direct modifications to the resource being protected are not required.

A high-level summary of common scenarios where the strategy of virtual patching makes operational and financial sense for the business is provided in Table 2:

- It buys additional time until patches are available
- It provides a compensating control when patching is not possible or not practical
- It reduces the need for "emergency" patches or workarounds
- It requires fewer policy enforcement points (i.e., at selected points in the network, as opposed to applying a patch on every system)
- It gives enterprises the flexibility to patch on a planned schedule

Definitions

√ A **Policy Decision Point** is where access policies are evaluated and combined to yield a yes / no value for use by a *Policy Enforcement Point.*

√ A **Policy Enforcement Point** is where a yes / no policy decision from a *Policy Decision Point* is used to grant or deny access to a protected resource. Policy Enforcement Points typically reside throughout the organization, e.g., within applications, databases, file systems, network devices, and endpoint systems.

√ A **Policy Administration Point** is where access policies are defined and managed.

- It helps to mitigate the high opportunity cost of unplanned downtime for critical systems, databases, and applications

Table 2: Scenarios When Virtual Patching Makes Sense

Scenario	Examples
Patches may not be available	▪ 42% of vulnerabilities publicly disclosed during the calendar year 2012 still had no patch available at year-end, up from 36% in 2011 (source: IBM X-Force)
Patching may not be possible or practical	▪ Older, out of support systems ▪ Outsourced code ▪ Original Equipment Manufacturer (OEM) systems, e.g., where license agreements may prohibit modifications to the underlying platform
Patching takes time – and time is money	▪ The patching process itself — i.e., assessing, prioritizing, testing, remediating — is costly, especially for emergency patches or workarounds ▪ The opportunity cost of unplanned downtime or system outages — e.g., lost end-user productivity, lost or deferred revenue, and in some cases lost customers — is prohibitive

Source: Aberdeen Group, April 2013

Virtual patching can protect critical enterprise systems against vulnerabilities and zero-day attacks temporarily, until a patch is available and deployed — and in some cases more permanently, for systems that are still in service but for some reason not patchable or not worth patching. Virtual patching also gives the enterprise more flexibility and control — that is, the enterprise can patch on its own schedule, and avoid the value-destroying activities of Patch Tuesdays, emergency patches and workarounds, endless testing, and unscheduled downtime.

Ironically, **loss of end-user productivity** (66%) and **unplanned downtime or system outages** (64%) were the most commonly experienced consequences of actual security-related incidents for the respondents in an Aberdeen study from 1Q 2013. Downtime is downtime, after all, regardless of whether it is the result of patching or the result of not patching, and these are costly scenarios that many companies would like to avoid. They are also relatively easy scenarios to quantify, as noted in the sidebar at right. Readers are encouraged to do their own back-of-the-envelope calculations for the impact of downtime, based on modifying the simple stated assumptions to reflect their own sensibilities.

The Impact of Downtime

√ $1,140 per hour for every $10M in annual revenue generated by an application or process, assuming that revenue is continuous and that all revenue lost goes unrecovered.

√ $55K per hour for every 1,000 employees, assuming a fully-loaded annual cost of $100K per employee and that all employees are fully idled.

Aberdeen's Research Findings: The Use of Virtual Patching in the Context of Database Security

Of particular interest for this Analyst Insight is the use of virtual patching in the context of **database security**. Databases are the crown jewels of sensitive enterprise data; they are typically the cornerstones for mission-critical applications and services that drive the organization's *raison d'être*.

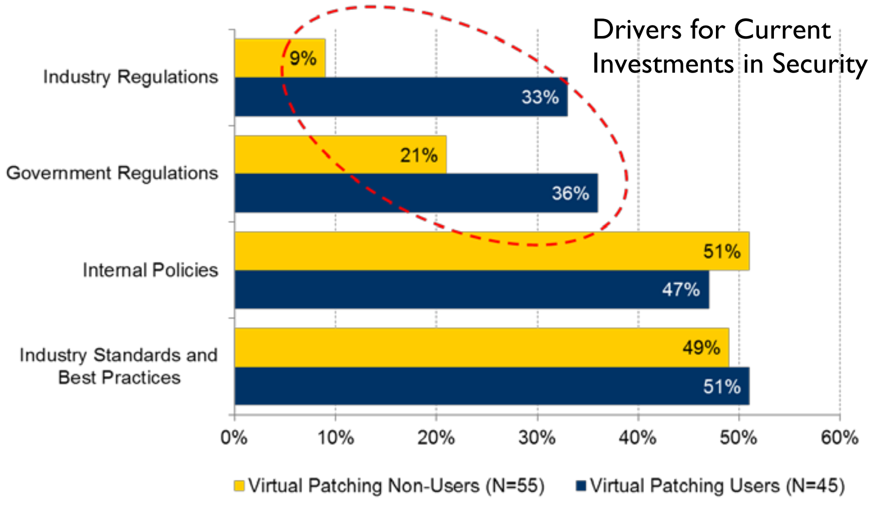
At the same time, the typical enterprise database environment is complex and diverse; for many companies, "protecting the database" actually means:

- Protecting multiple databases, running on multiple computing platforms, which are
- Supporting multiple enterprise applications, hosted in multiple locations (both physical and virtual), which are
- Managed by multiple database administrators (DBAs), who themselves are often in multiple physical locations

In an Aberdeen study of more than 110 companies conducted in 1Q 2013, about 3 out of 5 (57%) respondents had currently deployed one or more "external" database security solutions, i.e., external to the native security capabilities of the database itself. Of these, more than half (55%) indicated current deployments of virtual patching.

The attractiveness of virtual patching as an effective compensating control for database security is strongly supported by Aberdeen's recent research findings. For example, Aberdeen asked respondents to indicate the leading drivers for their current investments in security. A comparison of responses from 45 companies using virtual patching with those of 55 companies not using virtual patching shows the degree to which **industry regulations** (e.g., the Payment Card Industry Data Security Standard) and **government regulations** are particularly strong drivers for investments in virtual patching (Figure 1). With respect to more "voluntary" forms of compliance, such as **internal policies** and **industry standards and best practices**, there was little difference between the two groups.

Figure 1: Virtual Patching Seen as Effective Compensating Control



More than one response accepted; does not add to 100%
Source: Aberdeen Group, April 2013

Fast Facts

Aberdeen's benchmark research has shown that the leading performers ("Best-in-Class") are 2-times more likely than lagging performers ("Laggards") to use virtual patching:

√ Best-in-Class (57%)

√ Industry Average (31%)

√ Laggards (26%)

Solutions Landscape (illustrative)

Solutions for managing vulnerabilities range from those designed to increase the automation and intelligence of traditional patching, to those designed to reduce the pressure for immediate remediation by providing secure and cost-effective compensating controls. Table 3 provides an illustrative list of the latter type of solutions, by category.

Table 3: Solutions Landscape (illustrative)

Enterprise Assets	Traditional Patching	Compensating Controls (Virtual Patching)	
Databases	▪ Database patching	▪ Virtual database patching	▪ McAfee (Virtual Patching for Databases)
Endpoints	▪ Patch management ▪ Configuration and change management	▪ Host-based intrusion prevention (HIPS)	▪ McAfee (Host Intrusion Prevention) ▪ Trend Micro (OfficeScan Intrusion Defense Firewall) ▪ Symantec (Endpoint Virtualization)
Datacenter	▪ Patch management ▪ Configuration and change management	▪ Intrusion detection / prevention	▪ Trend Micro (Deep Security) ▪ HP TippingPoint (Digital Vaccine)
Applications	▪ Application patching	▪ Web application firewalls (WAF)	▪ McAfee (McAfee Firewall Enterprise) ▪ Dell SecureWorks (Managed WAF) ▪ Dell SonicWALL (SSL VPN / WAF) ▪ Imperva (SecureSphere) ▪ Fortinet (FortiWeb) ▪ Trustwave (360 Application Security / WebDefend)

Source: Aberdeen Group, April 2013

Summary and Key Takeaways

- Analysis by the Australian Government's Defence Signals Directorate (DSD) suggests that four specific endpoint security strategies and controls would have successfully protected against at least 85% of the cyber intrusions that they responded to in 2011:
    - Whitelist endpoint applications
    - Patch endpoint applications
    - Patch endpoint operating system vulnerabilities
    - Minimize the number of end-users with domain or local administrative privileges
- When it comes to information security, however, one size rarely fits all organizations:
    - Outside of a tightly controlled government / military / defense environment, controls such as application whitelisting and restricted administrative privileges may face

much stronger resistance, particularly by end-users who perceive them as a barrier to getting their work done

- Experience says that models that prevent the installation and execution of any software that isn't pre-approved and pre-enabled by a centralized IT function often result in IT being unable to keep up with demand, and in frustrated end-users finding workarounds
- Not all organizations are willing or able to bear the high upfront cost (in terms of staff, technology, and technical complexity) and medium ongoing cost (primarily staff) of such controls, and not all have the necessary resources and processes in place to implement all critical patches within the recommended standard of 48 hours

- Prompt patching of high-risk vulnerabilities in platforms, applications, and databases should be just as effective a strategy for the security of back-end systems, as can be inferred from the analysis shared by Verizon Business:
    - Based on their 2011 caseload of 855 actual incidents, only 40 (13%) of 315 possible threat events were actually seen
    - 98% of observed events were the result of **malware** and **hacking**
    - 81% of all incidents leveraged hacking, 69% involved malware, and 61% used a combination of both
- But keeping up with vulnerabilities and patches can be very difficult:
    - The total number of malware samples in the threat database topped 100 million in 2012 (source: McAfee Labs *Threats Report*, 3Q 2012)
    - On average, more than 150 critical updates and vulnerabilities were disclosed each week in 2012 (source: IBM X-Force *2012 Trend and Risk Report*, March 2013)
    - Increasingly savvy attackers are adapting and automating their techniques, and emerging technologies such as social, mobile, and cloud are creating new avenues for attack
- Based on Aberdeen's research, companies adopt four fundamental strategic approaches to managing vulnerabilities — all of which can help reduce risk and lower total cost:
    - **Start sooner** — i.e., reduce the time between the initial disclosure of vulnerabilities and the initiation of remediation
    - **Finish faster** — i.e., increase the speed at which affected systems are remediated, through increased automation
    - **Work smarter** — i.e., prioritize and implement the patches that impact the most critical business processes, or

  the patches that provide the greatest good for the greatest number of systems

  - **Create more options** — i.e., implement additional protections (compensating controls) to allow additional flexibility for assessing, prioritizing, and deploying patches and configuration changes for affected systems at the time most convenient for the company

- **Virtual patching** is a prime example of the "create more options" strategy, to deal with scenarios where:
  - Patches may not be available — e.g., 42% of vulnerabilities publicly disclosed during calendar year 2012 still had no patch available at year-end (source: IBM X-Force)
  - Patching may not be possible or practical — e.g., older, out of support systems; outsourced code; or OEM systems in which license agreements may prohibit modifications
  - Patching takes too much time or money — e.g., the actual cost of assessing, prioritizing, testing, and remediating, especially for emergency patches or workarounds; the opportunity cost of lost end-user productivity, or unplanned downtime or system outages
- Specifically in the context of database security, Aberdeen's research shows that virtual patching is seen as an attractive compensating control:
  - Databases are typically the cornerstones for mission-critical applications and services that drive the organization's *raison d'être*, and are therefore particularly sensitive to the issues of productivity and downtime
  - The typical enterprise database environment is complex and diverse in terms of platforms, locations, applications, and administrators
  - About 3 out of 5 (57%) respondents have currently deployed one or more "external" database security solutions; of these, more than half (55%) indicated current deployments of virtual patching
  - A comparison of responses from 45 companies using virtual patching with those of 55 companies not using virtual patching confirms that **industry regulations** and **government regulations** are particularly strong drivers for investments in virtual patching

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Endpoint Security and the DSD Top 4: One Size Does Not Fit All (blog); 29 March 2013

Network Security: Why the Growth is in Managed Services; March 2013

The Virtues of Virtual Patching; October 2012

Endpoint Security: Anti-Virus Alone is Not Enough; April 2012

Network Security: Firewalls Alone are Not Enough; April 2012

To Patch, or Not to Patch? (Not If, But How); October 2011

Is Your Vulnerability Management Program Leaving You at Risk? Most Likely, Yes; June 2011

Managing Vulnerabilities and Threats (No, Anti-Virus is Not Enough); December 2010

Web Application Firewalls: Defend and Defer; October 2010

Protecting Data in Databases vs. Applications: Better Security and Compliance at Lower Cost; April 2010

Protecting the Database: When (Most of) the Eggs are in One Basket; November 2008

Making Time for Better IT Security: Sooner, Faster, Later; August 2008

Vulnerability Management: Assess, Prioritize, Remediate, Repeat; July 2008

Author: Derek E. Brink, Vice President and Research Fellow, IT Security and IT-GRC (Derek.Brink@aberdeen.com)

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 854-5200, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com.