

Operationally Efficient IT and Data Protection Controls

Implications in the Virtual World

Jonathan Gohstand

jgohstand@packetmotion.com

IT Security: Today's Challenge



Increased Audit Compliance



Evolving, Complex Risks



“Operational efficiency is the biggest challenge facing the information security industry.”

- Information security architect at a large healthcare provider



Limited Resources

It's all About “Operational Reality”!

As IT resources get more and more constrained, the focus needs to be on your team can realistically do, not what the vendors says their products can do.

As external or internal audit requirements become more onerous, the need for consistency of activities becomes acute. (otherwise the audit work will drain your resources)

How to get there?

- *A simple taxonomy of security controls, applied as efficiently and consistently as possible.*

Getting in Front of Regulation: Gartner Research **Gartner** *The Top 10 Risk and Security Audit Findings to Avoid**

Gartner's recommendation: "Develop, in advance of negotiation with auditors, reasonable and appropriate controls for reasonably anticipated risks."

That is, understand the reasonable concerns that auditors are going bring up, and implement reasonable solutions for them in advance. You'll get better security, and a more efficient and effective audit

Example findings from the Top 10

"Audit Finding #1: Data Classification

Gartner's Recommendation: Conduct an inventory and classification project. (Manual classification will always be dangerously incomplete, so automation of this process is strongly recommended.)"

"Audit Finding #3: Administrator Controls and Shared Accounts

Minimum Remediation Required: Avoid the sharing of accounts of any type by users, and tie each identity and each privileged account to a specific individual."

"Audit Finding #5: User Activity Tracking and Log Analysis

What it Means: The enterprise is unable to track user activity and produce a record of which employees have accessed which systems or data, or when."

*Gartner Document 152216, October 2007

Basic Control Taxonomy

- 1. Identify Data That Counts**
- 2. Place Access Controls on That Data**
- 3. Maintain an Audit Trail of Data Access**
- 4. Change Management Overlay Control:
Platform Protection**
- 5. Change Management Overlay Control:
Watching IT Administrators, 3rd parties, etc.**

1. Identify Data

- Find the data that's important to protect

You can't protect it if you don't know about it

Often the problem is data exported from the obvious places to the not-so-obvious places

To drive efficiency

- On the network edge: Focus on the really obvious stuff
 - Personal Health Info, SS#s, etc.
- On the inside: Watch the people to find the data

2. Access Control

- Limit access to those who need it

The tough part is minimizing access to those who *really* need it.

To drive efficiency

- Look at it from two ways: Both the asset (data itself), and people's access to the network
 - Monitor actual activity to figure out who needs access
- Centralize authentication database (Active Directory)
 - If you can't use AD directly, try to correlate to it.
 - E.g. No access to key app server if not domain authenticated
- Involve business management to help “own the data”

3. Audit Trail

- Establish an audit trail of access to data
- Identify abnormal access patterns

To drive efficiency

- Establish an audit trail that is relatively easy to search & analyze
 - Normalize audit trails (consistent format and repository)
 - Audit trail allows the specific user responsible to be identified
- Consider the need to not risk application performance or availability
- Utilize a combination of network and native (server) approaches
- Operate at both granular and aggregate levels. Use aggregate data to more efficiently spot abnormal access patterns

4. Overlay: Platform Protection

- **Need to maintain the integrity of the platforms (operating systems, databases) that the data sits on.**
 - System and configuration files, user database, etc.
 - Effective access controls rights

To drive efficiency

- Consistent approach (see Audit Trail slide)
- Only invest in systems that boil up the changes
 - E.g. Access Control Changes: Focus on the effective rights on the key target files/data, not the “blow-by-blow” activity

5. Overlay: IT Administrator / 3rd Party Controls

- Audit activity, implement controls on privileged users

Often the hardest control to implement

Biggest issue is attitude: acceptance that the risk has to be taken seriously

To drive efficiency

- Consistent approach (see Audit Trail slide)
- Ensure correlation between admin IDs and actual users
- Segregation of duties drives effective controls

The Taxonomy Applied

<i>Your Company Name Here</i>	Target #1: Trading Algorithms	Target #2: Customer Management System	Target #3:...
Data ID	Risk: Status:	Risk: Status:	Risk: Status:
Access Control	Risk: Status:	Risk: Status:	Risk: Status:
Audit Trail	Risk: Status:	Risk: Status:	Risk: Status:
Platform Protection	Risk: Status:	Risk: Status:	Risk: Status:
Administrator Controls	Risk: Status:	Risk: Status:	Risk: Status:

The Brave New World – Virtual and Cloud!

Let's GO!

Background

Virtualized Data Center (VMware)

Virtual Private Cloud

IAAS/PAAS

SAAS

Gartner Survey Results

Top Virtualization Security Issues



- ① Information security isn't initially involved in the virtualization projects
17w
- ② A compromise of the virtualization layer could result in the compromise of all hosted workloads
68w
- ③ Lack of visibility and controls on internal VM-to-VM communications
69w
- ④ Potential Loss of SOD for network and security controls
29w
- ⑤ Restricting and auditing administrative access and management tool access
31w
- ⑥ Configuration management and Patching of offline images
32w
- ⑦ Storage area network security and protection of offline images
20w
- ⑧ Increased chance of misconfiguration because of the use of different tools
28w
- ⑨ Risks from combining workloads of different trust levels on the same physical machine
56w

Gartner

Key Issues

- **An inflection point**
- **Consistency and flexibility**
- **System administration**
- **Loss of ownership of hardware resources**
 - Hypervisor issues (platform)
 - Segregation of duties
- **Dealing with 3rd party hosting providers**
- **Audit/security platform consolidation**

Summary

Five basic controls

Seek consistent implementations of each

- Combine network and native sources into a unified trail

Maintain and periodically review a matrix of controls and targets

Be as proactive as is practical to get in front of regulation

Never trust a vendor when it comes to operational efficiency: talk to existing customers of similar size and try before you buy.

User Activity Management – A New Approach

Gartner

Gartner's View

- Activity Monitoring a "Top 10 Strategic Technology for 2010"
- Cited as 2009 Cool Vendor:
- "PacketMotion's solution is unique in providing broad-scope user activity and resource access monitoring from the network, without any dependence on application or system logging".
- "...set apart by a trend toward delivering cost-effective, low-risk IAM – an understandable focus in a time of highly constrained IT, IT security budgets and personal resources."

Single platform for compliance, internal audit, and security

- Consolidates multiple "point products"
- Complete user activity visibility
- *Operationally efficient*



Low risk: no agents, no in-line appliances

Backup

Actual Control Examples

Control Example: Platform Change Management

Control: “All instances of changes to system objects are recorded and reviewed periodically”

Implementation:

- ✓ Limit access to management interfaces to authorized users
- ✓ Audit changes to all relevant objects: system files; users and groups; database stored procedures, views, indexes, schemas etc.
- ✓ Consider a combination of network and native audit sources to *minimize logging footprint and eliminate agents.*

Control Example: Password Strength

Control: Passwords must be of sufficient strength. However the application lacks support for strong passwords.

Implementation:

- ✓ Rely on Windows domain password strength. Audit all cases of a user's application ID not being used from that person's PC. If a user must use their (strong) domain ID before accessing the application, this is adequate compensating control.

Control Example: Access Control Management

Control: Audit and authorize all changes to access control rights on critical data and system areas

Implementation:

- ✓ The trick to doing this efficiently is to focus on changes to “total effective rights” on critical objects (e.g. a sensitive file folder).
 - ✓ Just relying on an audit trail of changes to groups will not be efficient.
- ✓ Also: use actual access to drive the process
- ✓ The approach should be “Did anyone get new/increased rights on this specific target? If so, how did they get them?”

Control Example – 3rd Party Support Staff

Control: Ensure 3rd party support staff do not “leapfrog” from the systems they support into the rest of the network.

Implementation:

- ✓ Apply access control lists on or behind the VPN concentrator to limit 3rd parties to accessing the systems they’re supposed to.
- ✓ Virtual or actual firewalling to alert/block outbound administration traffic from systems supported by 3rd parties.

Fraud Detection Abuse of Legitimate Access Rights

Control Example – Detecting Abuse of Authorized Access (Fraud)

Control: Baselining “normal” access levels for authorized users to critical data (key file shares, databases, etc) and detecting usually high levels of access that indicate possible fraudulent activity.

Implementation:

- ✓ Usually the target application lacks baseline capabilities. Gathering and counting individual access events can affect performance and involves a lot of data. Instead use (identity correlated) network level activity monitoring, especially across a team of users doing a similar job function.

Activity Baseline – Report Example

Use Per Person Per Day Statistics to Set “Excessive” Threshold



Baseline Access - Finance Team

For week of 15-19 June 2009

Web Applications Access Baseline Summary

Report Totals		Per Person Per Day Statistics		
			Access Count	Volume (MB)
Number of Days	5	Average	242.8	28.8
Number of Users	6	Standard Deviation (from average)	182.1	29.1
Total Accesses	8,740	Median	204.0	11.6
Total Volume (MB)	1,038	Maximum	540	84.2



Web Applications Access Baseline Detail

#	User Name	Account ID	Web Applications Access Count Statistics (Web site filters apply; does not include SSL traffic)			Data Volume Statistics (MB) (Web site filters do not apply; includes SSL traffic)		
			Total	Avg/Day	Median/Day	Total	Avg/Day	Median/Day
1	Marty McFarland	mmcfarland	3,237	540	424	110.6	18	14
2	Rick Giles	rgiles	2,000	333	382	187.6	31	18
3	Mitchell Christensen	mchristensen	1,360	227	246	150.4	25	9
4	Bob Lux	blux	876	146	162	505.3	84	43
5	Jonathan Gohstand	jgohstand	1,266	211	19	84.6	14	8
6	Paul Smith	psmith	1	0	0	0	0	0

Virtual Network Segmentation

Network Segmentation/Enforcement

What's the Basic Requirement?

Blocking certain traffic **INSIDE** the network

- Developers from production systems
- Limiting 3rd party support people to the systems they are supposed to work on
- Departments in financial services that are not supposed to exchange info
- PCI (credit card) servers from everything else
 - PCI DSS rules say that if you don't separate the credit card systems from the rest of the network, the entire network is "in-scope" for PCI DSS, which is basically out of the question.
 - PCI rules do not say exactly HOW the separation must be done.

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. “System components” are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a “flat network”) the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and will be used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon such things as a given network’s configuration, the technologies deployed, and other controls that may be implemented.

Appendix F: PCI DSS Reviews – Scoping and Selecting Samples provides more information on the effect of scoping during a PCI DSS assessment.

Why Is Network Segmentation So Hard?

Relying on access controls on the systems you are trying to protect is not good enough

- Too many systems; no way to protect them all
- PCI separation requires a *network* approach

Network gear (switches) is all you have to work with and it's next to impossible to do it there

- Limited capabilities, operational challenges (e.g. ACL management)

Using internal firewalls is problematic



Why Not Just Use Firewalls?

Difficult to integrate into network architecture

- Network team will bring up a lot of concerns

Re-addressing of critical systems required

- Very risky: addresses may be hard coded in source code or scripts

Identity-based policies required, but firewalls/ACLs are IP based

- Heavy operations overhead and potential for mistakes
- Operationally difficult to keep policies up to date

Potential application availability and performance impacts

- The firewall is always blamed when something goes wrong

Limited notification to end user of policy violation

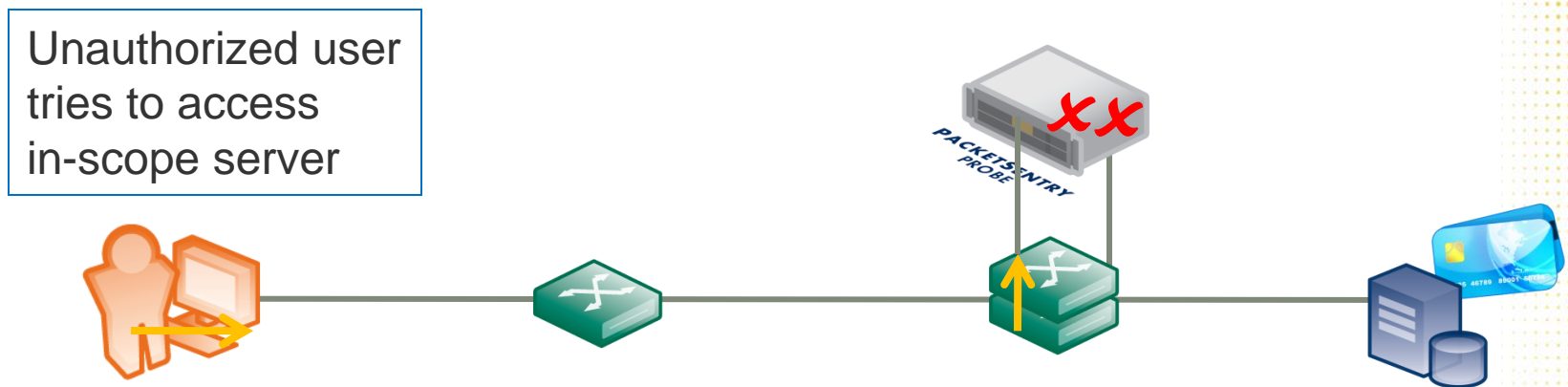
- Upset users; more help desk calls

→ *Expensive and disruptive!*

PacketSentry Virtual Segmentation

Create identity-based policies to block all traffic that would violate policy.

Send connection resets to kill connections that break policy *as they are being set-up*



Virtual Segmentation Benefits

Not in-line

- No network architecture or application availability impact
- No re-addressing

Fast, low-risk install

Identity based policies - dynamically updated

- Low operational overhead

End-user notification via email

- Fewer, easier help desk calls

Compensating Control

- Audit trail of activity for clients that have access to PCI assets

→ *Cost-effective and transparent to operations!*

Virtual Segmentation: Consistent With The Internal Network Paradigm

Firewalls make sense at the network edge, where you want to deny everything unless you know what it is

But firewalls don't fit with the paradigm on the internal network, which is to allow everything, and have as few "moving parts" as possible to drive availability and performance

PacketSentry Virtual Segmentation is consistent with the internal paradigm: Nothing in-line; let everything pass as normal, and only operate on flows that break policy

