

EVALUATING PRODUCTS BASED ON APPROPRIATE USAGE:

Contents

Introduction – the perfect storm 1

History of Use Cases 2

Use Cases in Product Testing 2

Use Cases in Product Evaluation 3

Environmental Usage 3

The Future of Use Cases in Security 4

About NSS Labs 5

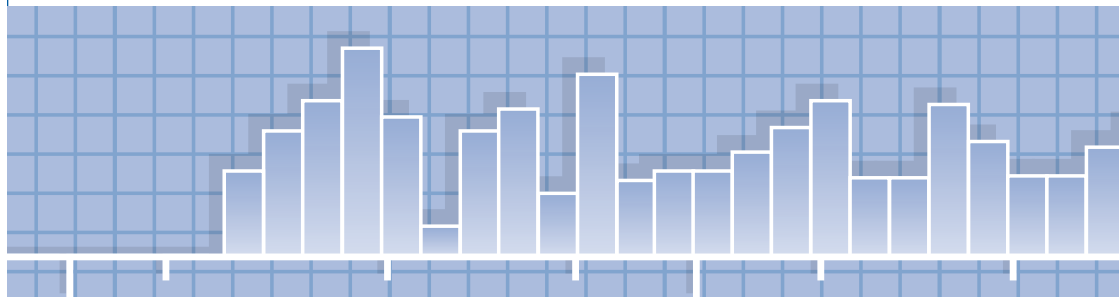
Appendix: Security Effectiveness Scorecard™ 6

Appendix: Case Study 7

MATCHING NEEDS AND CAPABILITIES

SUMMARY

Information security products have evolved rapidly over the last decade. However, the science of evaluating products has virtually stood still during that same time period, creating a knowledge gap that has made it difficult for information security buyers to determine whether or not a product meets specific security and/or compliance needs. This paper discusses a new method for evaluating technology products based upon the appropriateness within the context that they will be deployed. By applying a Use Case-based methodology, information security professionals can more clearly identify detailed protection requirements for a given environment. For example, a Use Case can clarify different application security requirements between retail storefronts and back-end e-commerce datacenters. The benefits of such an approach include: ensuring the appropriate level of security is implemented, avoiding over-paying for products, as well as a clearer understanding of protective capabilities of the system.



INTRODUCTION – THE PERFECT STORM

Never before have Information security professionals been faced with so many challenges; including rapidly evolving technology that is spawning a new generation of threats, more sophisticated and all-inclusive information security technology, and the dissolution of the perimeter.

- New vulnerabilities: Web 2.0 technologies such as AJAX and Ruby have at once enabled new functionality, but also introduced the opportunity for a whole new generation of vulnerabilities.
- Threats are evolving: Attacks, whether viruses, hacks or otherwise, are becoming more targeted and sophisticated. In addition, they are increasingly professionally motivated for profit and executed by organized crime.
- Old threats never die: There is a resurgence of older exploits and viruses because many security products focus solely on the most recent threats. The resurgence means IT pros and vendors need to protect against new and old threats simultaneously; thereby increasing the requirements for detection and remediation.
- IT environments are becoming more complex as the perimeter is dissolving. Layered security is evolving into zoned security. No longer is a simple perimeter and DMZ strategy sufficient. Today's organizations must account for remote workers, branch offices, partner extranets, guest access, and the overlapping of neighboring wireless networks.
- Products are evolving and differentiating: Many new Information Security products are highly specialized, while older technologies are being consolidated into multi-function solutions. For example, not all IPS products are alike because product manufacturers have diverse target markets, product positioning, internal development capabilities, and architectural design philosophies. Thus, some network IPS offerings are designed for the core and address RPC and NetBIOS protocols, while other IPS products may focus on browser-based client attacks and are positioned more as perimeter devices.

Testing and evaluating complex technologies' abilities to stop sophisticated attacks in the myriad of environments has become an impossible task for the average information security professional. They don't have the time, resources or expertise to perform the analysis and still take care of their other daily duties. Given such dynamic change, understanding exactly what is required becomes an important precursor to 'shopping' for security solutions.

In addition, most testing labs are still evaluating products based upon general purpose, "Ivory Tower" criteria and testing practices (such as simple capture/replay and packet blasting), even though products have evolved and specialized. Some security products are architected to protect inside the core of a network, while others are designed to protect e-Commerce applications, and yet others are best suited to protecting against client attacks. As of today, no one security product does all three perfectly. As a result, products that perform well in a lab setting often under perform in live production environments. To remain relevant, product testing must evolve and adapt.

HISTORY OF USE CASES

Use Cases are a concept from software and system engineering that is employed to capture the functional requirements of a system. Software developers identify Use Cases to set the parameters for how a product will behave under various conditions. This method of understanding and defining requirements is an effective method for transforming a need into formal logic (lines of code), and lines of code that then become a functional product.

In addition, Use Cases have been used to effectively describe appropriate usage of products in various industries. Both the Automotive and Pharmaceutical industries have a history of defining product capabilities in terms of Use Cases. For example, products that are more susceptible to adverse side effects or misuse (such as pain killers) are approved for some uses and not others. Thus, the Physician's Desk Reference (PDR) is a popular independent reference for the medical community.

USE CASES IN PRODUCT TESTING

Testing products based upon Appropriate Usage (applying a Use-Case based methodology) provides a clear picture of which technologies are effective against a particular type of attack. Thus, products can be evaluated by comparing their capabilities against specific deployment scenarios and protection requirements.

Measuring products based upon appropriate usage has a number of benefits:

- Accurately identify protection capabilities of a specific product.
- Ensure product protection capabilities match the security requirements for certain types of environments.
- Provide guidance on technology buying that more accurately matches customer needs with product capabilities.
- Recommend product usage based upon rational testing methodologies and empirical data.
- Avoid over or under-spending for solutions.

USE CASES IN PRODUCT EVALUATION

For Information Security products, Use Cases identify what content should be allowed to pass and the types of attacks a given product is designed to protect against. Thus, architecting a security solution entails understanding the traffic patterns of the network infrastructure to be protected.

Such Use Cases should take into consideration:

- Functional protection requirements. Am I protecting Oracle DBMS servers or Microsoft Windows XP desktops? What implications are there for security coverage for each class of assets? Or what threats should the solution be aware of?
- What compensating controls or existing solutions are already deployed?
- Specific Compliance requirements. Example: Is PCI DSS compliance needed? Where do I need to encrypt card holder data?
- Performance: how much traffic must be handled?
- Administration and reporting: What specific information will be needed/required in logs and reports? User access to specific types of data?

Once the requirements are understood, comparing use case testing results enables quick identification of products that meet functional and performance objectives.

ENVIRONMENTAL USAGE

Where a product is deployed and what it is protecting has a significant impact on the specific requirements. There are significant differences between datacenter, perimeter, ROBO/SOHO, e-commerce and SCADA environments; for example, protocols and operating systems in use. For more detail, see the NSS Labs Security Effectiveness Scorecard™ in the appendix. These environmental protection factors should be considered when evaluating solutions, because one size does not fit all.

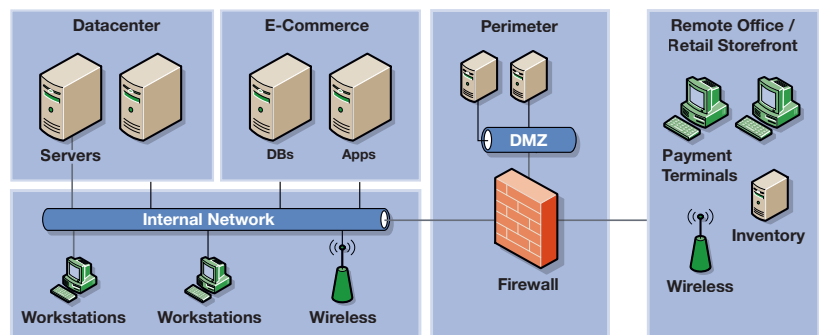


Figure 1. Network environment classifications

Datacenter – Main Function: Protect datacenters and network cores. Focus on server protection for complex internal applications. Uptime is mission critical in these production networks and high availability/failover is required. False positives are unacceptable, and products are often maintained by experienced professionals who custom-tailor policies to prevent false positives. Company Profile: Medium, Large, and extremely large businesses. Protocol complexity and throughput requirements are the extremely demanding.

Network Perimeter – Main function: Protect the desktop and a simple DMZ from the Internet. Focus on Client and Server protection from Internet-based attacks, and includes simple DMZs with web, mail, DNS, but no e-Commerce storefront. Uptime is very important and HA/failover is preferable, but always not required. False positive rates are important, but not critical. Company Profile: Headquarters or regional distribution center for a large retailer.

Remote Office / Retail Storefront – Main function: Protect the desktop. Focus on client protection from Internet-based attacks. Uptime is important, but not mission critical 24x7x365. Network devices need to provide backup network access (via dial-up, ISDN, DSL line) and high availability for larger retail stores. False positives rates are less important. Company Profile: Coffee Shops, food service, mid-sized merchants, large department stores, etc.

e-Commerce Site – Main Function: Protect electronic storefronts. Focus on server protection for complex DMZs that include application servers & database servers that require protection from sophisticated Internet based attacks. Most traffic adheres to protocol standards. Uptime is extremely important and (in most cases) HA/failover is required. E-Commerce sites are tested as “production networks,” therefore low false positive rates are required as false positives mean lost business.

Company profile: Small hosted internet storefront applications, large online shopping malls or other high volume sites.

THE FUTURE OF USE CASES IN SECURITY

NSS Labs is leading the charge to educate the industry on the benefits of Use-Case based design and analysis. A number of trends are driving increased adoption of Use Cases; including software development best practices, network and systems design, and even compliance auditing against standards like the PCI DSS.

Stakeholders in the information security product marketplace, such as product managers, IT and compliance professionals, product evaluators, and auditors, can all benefit from speaking the same language. Use Cases offer an effective vehicle for unifying the discourse of product needs and capabilities.

As buyers in the marketplace continue to identify new and evolving requirements (whether for compliance or security), the thoughtful application of Use Case methodology will not only make their jobs easier, but provide clearer guidance for product vendors seeking to communicate the benefits of their offerings.

ABOUT NSS LABS

Founded in 1991, NSS Labs is the globally recognized leader in independent security performance testing and certification. With operations in Chicago, IL and San Diego, CA, NSS Labs offers a range of specialized networking and security testing services to vendors and end-user organizations world-wide. NSS Labs' comprehensive certification schemes address a wide range of security products, including Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Secure Content Appliances (SCA), Content Monitoring and Filtering (CMF) devices, Unified Threat Management (UTM) systems, firewalls, VPNs, Web Application firewalls, vulnerability scanning, cryptographic devices and PKI products.

More info: www.nsslabs.com

SECURITY EFFECTIVENESS SCORECARD™

CLIENT NAME: _____
PRODUCT: _____
DATE: _____

INDUSTRY COMPARATIVE RANKING

	System	Service	Fault	Recon	DoS
NSS SUM Average	15%	80%	55%	30%	20%
Client Product	50%	0%	65%	15%	10%
Delta	35%	-80%	10%	-15%	-10%

TARGETS

	System	Service	Fault	Recon	DoS
Apple	85%	50%	90%	35%	50%
Borland	0%	20%	95%	75%	50%
CA	20%	80%	65%	25%	75%
HP	55%	50%	65%	65%	70%
IBM	35%	85%	40%	50%	80%
McAfee	85%	15%	65%	55%	25%
Microsoft	95%	25%	5%	35%	40%
Novell	5%	90%	65%	5%	20%
Open Source	0%	85%	25%	70%	15%
Oracle	15%	40%	70%	20%	60%
RedHat	50%	10%	55%	45%	0%
SAP	65%	40%	15%	80%	50%
SUN	60%	85%	85%	35%	30%
Symantec	40%	65%	70%	35%	85%
Veritas	0%	45%	40%	45%	30%

PROTECTED ENVIRONMENT

	System	Service	Fault	Recon	DoS
Datacenter	45%	15%	55%	40%	10%
Perimeter	10%	35%	30%	80%	45%
ROBO / SOHO	30%	65%	65%	0%	20%
Ecommerce	65%	95%	40%	45%	25%
SCADA	10%	15%	85%	50%	25%

EXPLOIT TYPE

	System	Service	Fault	Recon	DoS
Attacker Initiated	85%	40%	35%	35%	10%
Target Initiated	95%	80%	20%	85%	N/A
Network	90%	45%	50%	60%	50%
Local	85%	50%	60%	65%	20%

EXPLOIT SEVERITY BY PROTOCOL / SERVICE

	System	Service	Fault	Recon	DoS
HTTP / Web	50%	95%	85%	95%	35%
SMTP / Email	25%	90%	35%	40%	90%
RPC	5%	45%	95%	0%	85%
Telnet & SSH	85%	75%	70%	40%	55%
FTP	40%	45%	20%	55%	70%
DNS	30%	65%	45%	65%	0%
SQL	40%	10%	55%	80%	40%
XWindows	30%	65%	25%	80%	95%
NFS & AFS	30%	10%	80%	65%	80%
SCADA	80%	20%	50%	10%	40%

EXPLOIT DATE

	System	Service	Fault	Recon	DoS
1998	10%	5%	45%	50%	35%
1999	5%	25%	20%	35%	80%
2000	15%	40%	50%	35%	95%
2001	5%	65%	25%	40%	90%
2002	5%	5%	10%	85%	55%
2003	85%	45%	30%	10%	10%
2004	30%	15%	50%	30%	5%
2005	25%	95%	0%	0%	15%
2006	55%	90%	50%	45%	40%
2007	35%	15%	70%	5%	45%
2008	10%	15%	35%	30%	40%

TARGET OS/APPLICATION COVERAGE BY DATE

	Pre	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Apple	95%	85%	0%	85%	65%	60%	60%	50%	65%	20%	20%	20%
Borland	25%	25%	90%	50%	30%	80%	0%	95%	50%	85%	10%	20%
CA	25%	30%	70%	65%	60%	95%	5%	15%	75%	80%	85%	95%
HP	65%	70%	70%	20%	75%	65%	75%	70%	70%	5%	0%	10%
IBM	70%	60%	65%	80%	55%	60%	15%	30%	30%	80%	10%	90%
McAfee	95%	20%	55%	30%	25%	0%	40%	50%	65%	0%	35%	80%
Microsoft	70%	45%	35%	25%	10%	80%	15%	50%	95%	65%	65%	85%
Novell	65%	55%	80%	60%	70%	95%	50%	35%	55%	20%	35%	50%
Open Source	65%	75%	25%	10%	75%	10%	50%	90%	5%	55%	40%	60%
Oracle	90%	75%	20%	55%	45%	60%	85%	60%	90%	70%	95%	80%
RedHat	70%	35%	80%	75%	0%	20%	15%	20%	70%	0%	95%	25%
SAP	15%	90%	45%	25%	50%	0%	25%	80%	80%	40%	20%	90%
SUN	10%	20%	80%	0%	75%	70%	95%	25%	35%	20%	35%	70%
Symantec	0%	0%	5%	5%	55%	85%	55%	95%	30%	10%	45%	0%
Veritas	10%	65%	40%	5%	70%	65%	70%	70%	45%	25%	40%	45%

SERVICE DATE EFFECTIVENESS

	Pre	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
HTTP / Web	45%	80%	85%	10%	10%	50%	65%	60%	35%	45%	90%	85%
SMTP / Email	85%	85%	35%	75%	35%	65%	10%	90%	90%	60%	80%	10%
RPC	30%	30%	30%	20%	95%	85%	5%	90%	15%	50%	30%	85%
Telnet & SSH	70%	30%	20%	75%	20%	50%	70%	10%	0%	80%	50%	10%
FTP	60%	40%	25%	80%	20%	10%	55%	10%	90%	0%	35%	50%
DNS	70%	75%	10%	10%	35%	60%	45%	50%	25%	25%	35%	50%
SQL	90%	25%	65%	40%	55%	0%	65%	15%	5%	50%	15%	25%
XWindows	75%	95%	60%	5%	5%	15%	65%	65%	90%	20%	75%	65%
NFS & AFS	25%	70%	10%	50%	95%	25%	40%	25%	0%	5%	20%	90%
SCADA	10%	45%	20%	45%	50%	80%	15%	25%	25%	65%	20%	15%

CONFIDENTIAL INFORMATION - DO NOT DISTRIBUTE

APPENDIX: CASE STUDY

USE CASES IN THE PAYMENT CARD INDUSTRY

The payment card industry (PCI) has developed one of the most prescriptive sets of requirements to date. The PCI Data Security Standard (DSS v.1.1) contains 204 unique requirements for securing cardholder data in merchant, service provider and bank networks. PCI DSS primarily prescribes processes that should be followed and technologies to be used in payment card networks. It does not, however, identify deployment Use Cases for those technologies.

As such, NSS Labs has created a series of Product Security Standards (PSS) which reflect the needs of various types of payment card environments (Use Cases), as well as relevant DSS requirements. Note: NSS provides a certification program that verifies a product's capabilities accordingly.

Use Case example of a retail storefront:

In a retail storefront environment, there are no servers accessible from the Internet, and the primary risk is client side attacks against Web Browsers (IE & Firefox), Microsoft Office products, and Media Players such as Windows Media Player, QuickTime, and Real Networks.

Example 1. A retail storefront requires a firewall that is capable of separating the payment card network from the back office environment, and possibly even wireless access.

Example 2. A retail storefront requires a UTM that is capable of protecting against client attacks, while effectively separating payment card traffic from back office, and even possibly wireless traffic.

Further, a merchant or service provider is obligated to comply with different requirements depending on their PCI Level. In PCI terms, higher levels equate to increased risk, usually due to the fact that the customer conducts more transactions, or a higher dollar volume of financial transactions.