Is Your Network a Sitting Duck?
3 Secrets to Securing Your Information Systems

Presenter: Matt Harkrider

Founder, Alert Logic

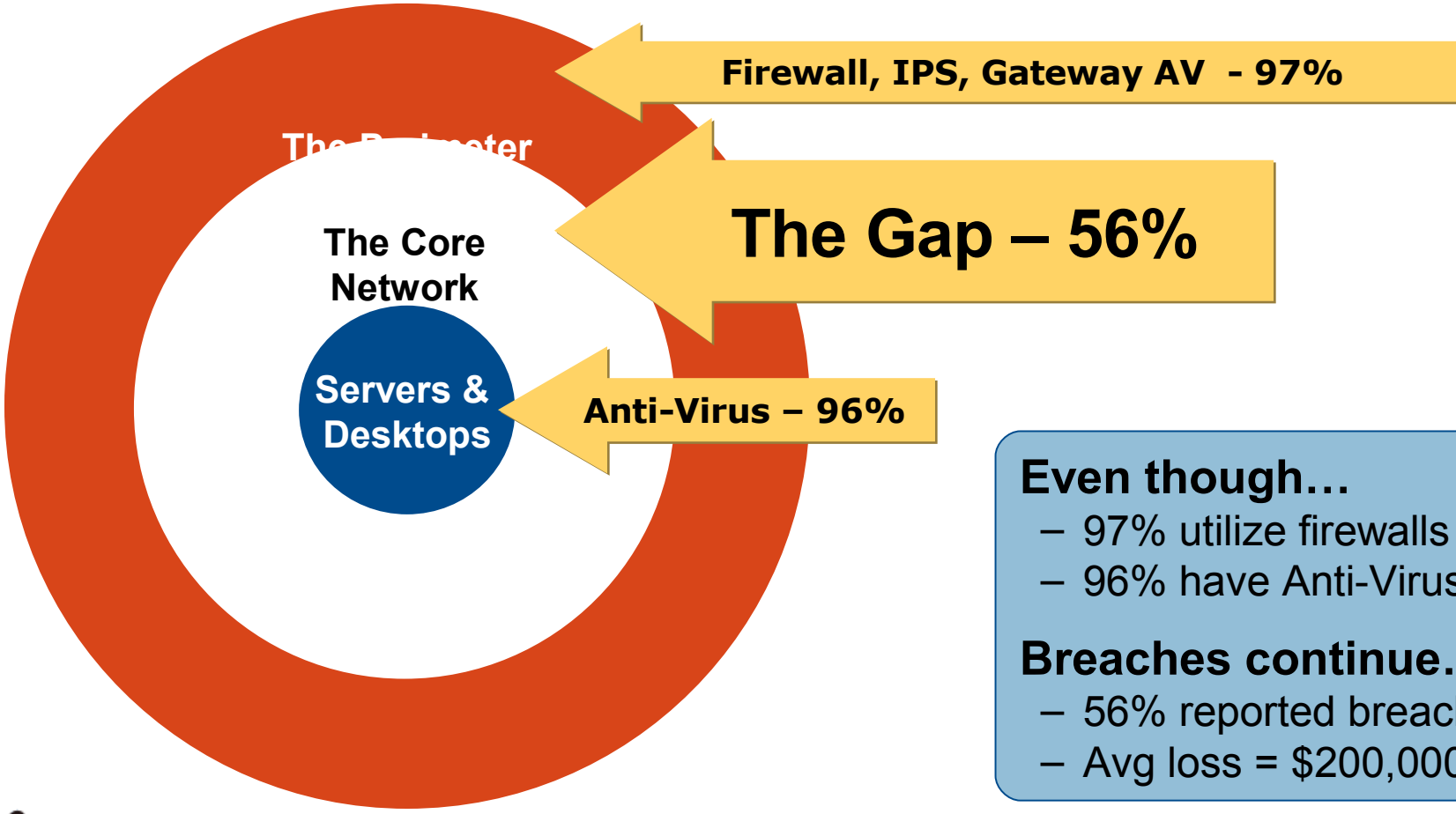
Who We Are: Corporate Fact Sheet

- Founded: 2002
- HQ: Houston, TX
- Privately held
- Customers: 200 +
- Service renewal rate: 99%
- Focus: Network Intrusion Defense
- Key differentiator:
  - On-Demand delivery model

Sample Customers:

False Sense of Security

According to the recent FBI/CSI survey:



Even though…
- 97% utilize firewalls
- 96% have Anti-Virus

Breaches continue…
- 56% reported breach
- Avg loss = $200,000

Third Layer of Security is Required

Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond

- "By the end of 2007, we believe that three out of four organizations will be infected with financially motivated, targeted malware that has evaded their traditional perimeter and host defenses and remains installed and undetected on their endpoints…"
- "…antivirus and firewalls are insufficient for comprehensive malicious-code detection and prevention. Legacy antivirus mechanisms must be supplemented with more-advanced styles of intrusion prevention in network- and host-based security…."
- "…addressing targeted threats should not require that organizations purchase dozens of new security point solutions. Rather, security platforms should evolve to deliver more types of security protection for little or no additional cost."

The 3 Secrets

3 Secrets

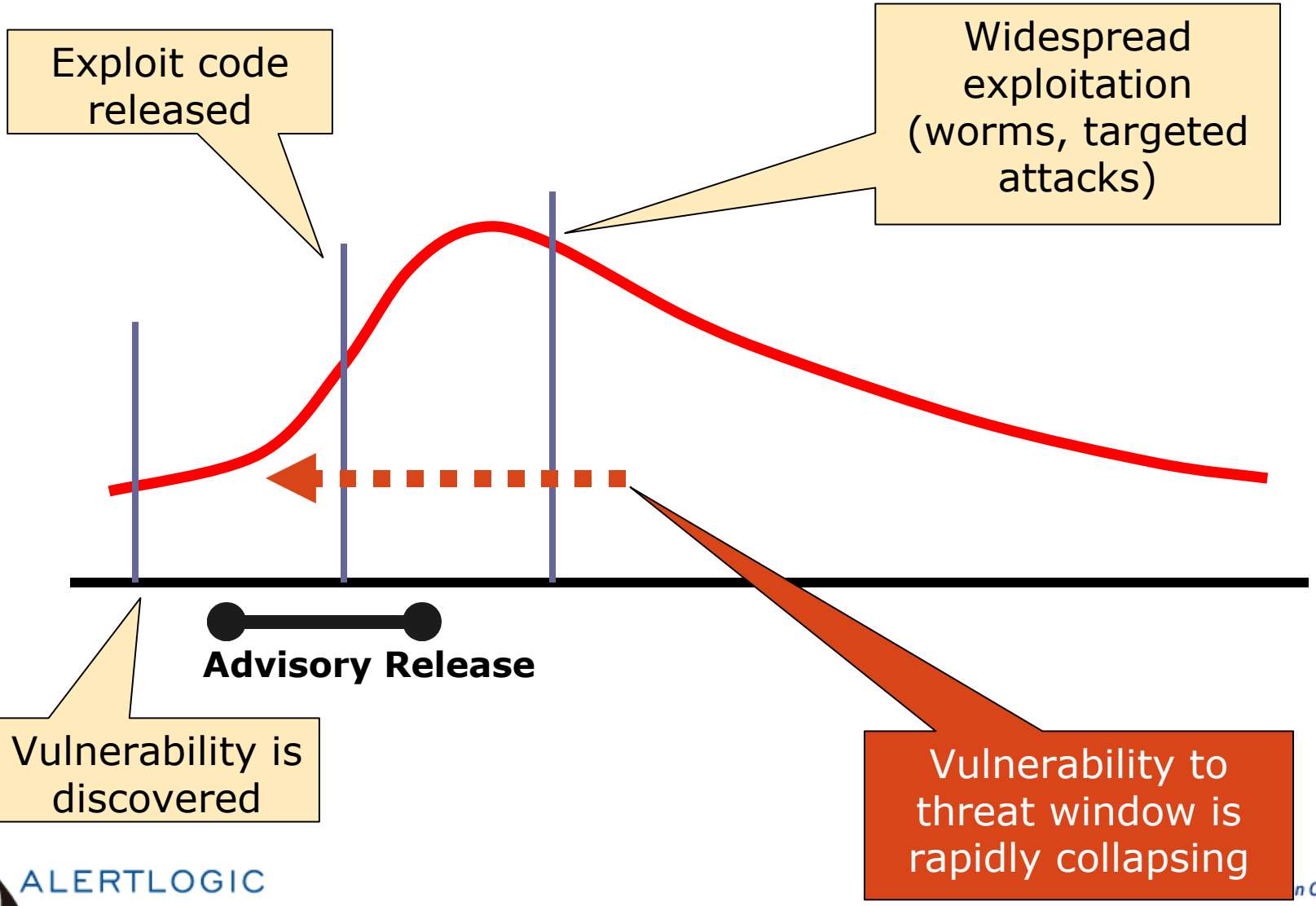
2. Proactive vulnerability scanning
3. Network threat monitoring
4. Don’t “do it yourself”

Vulnerabilities

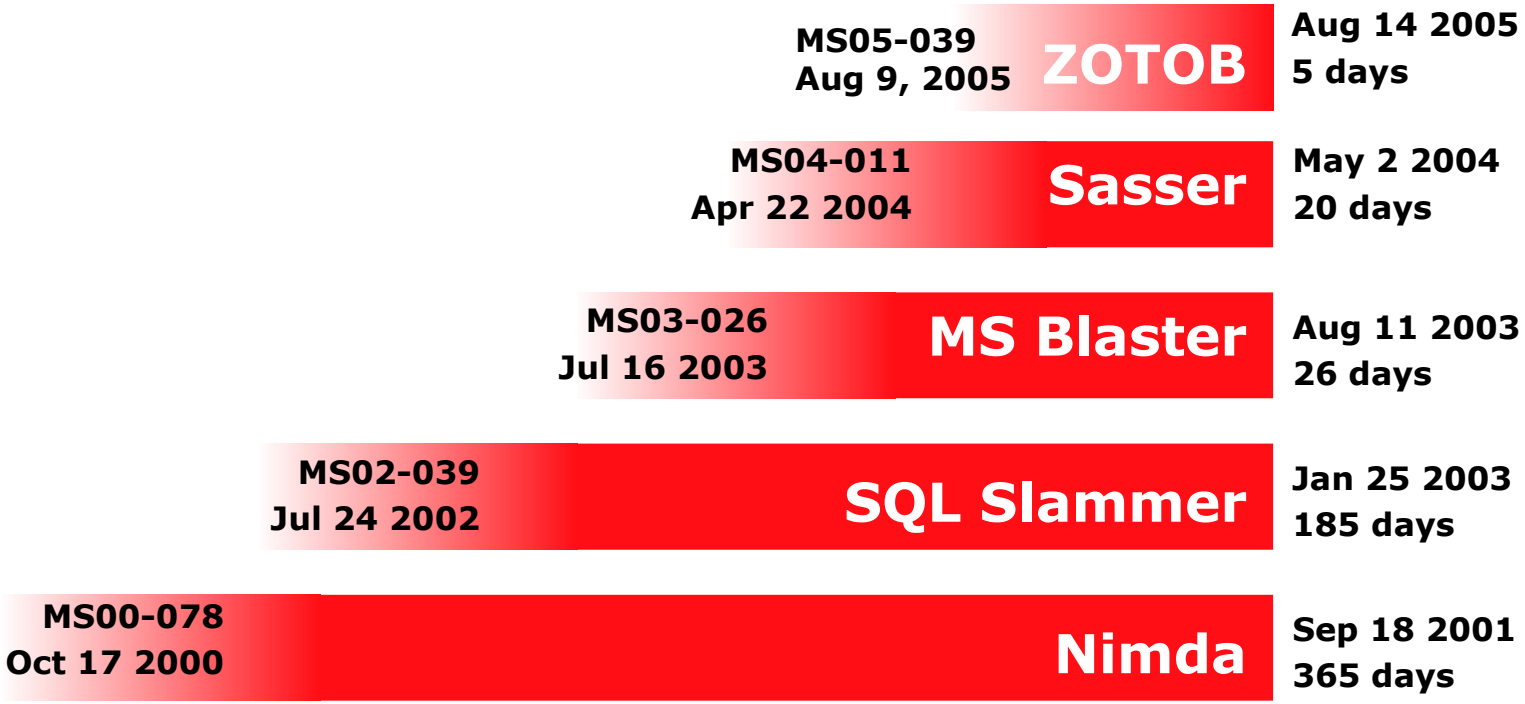
Dangerous Trends

- Time to vulnerability window has collapsed
- Attack vectors change faster than any organization can respond
- Too much emphasis placed on perimeter security

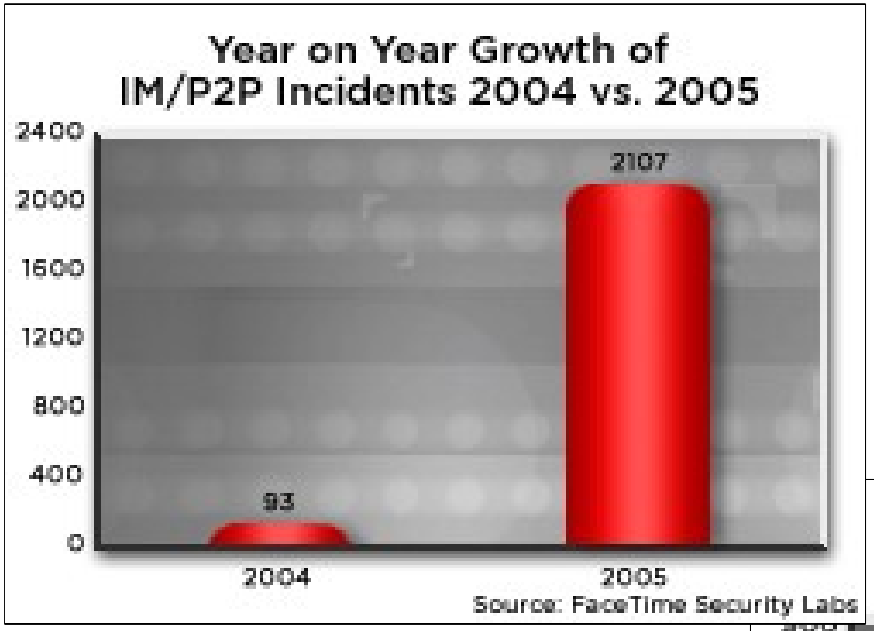
Vulnerability to threat timeline



Historical Evidence

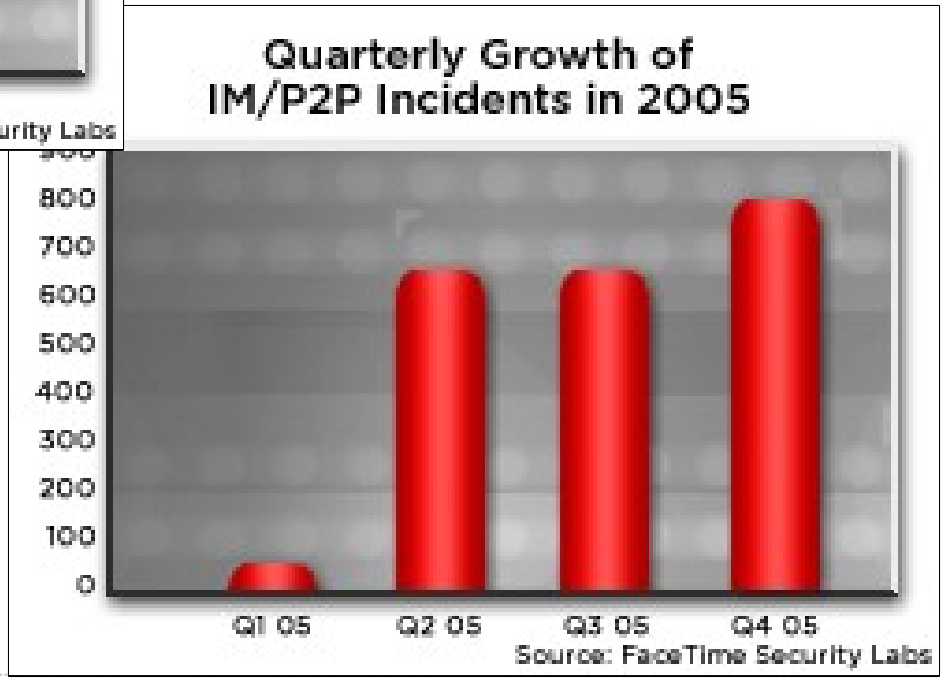


New Vectors Emerge Quickly



Malware spreads through new vectors with ease

Security does not react fast enough to sudden shifts in direction



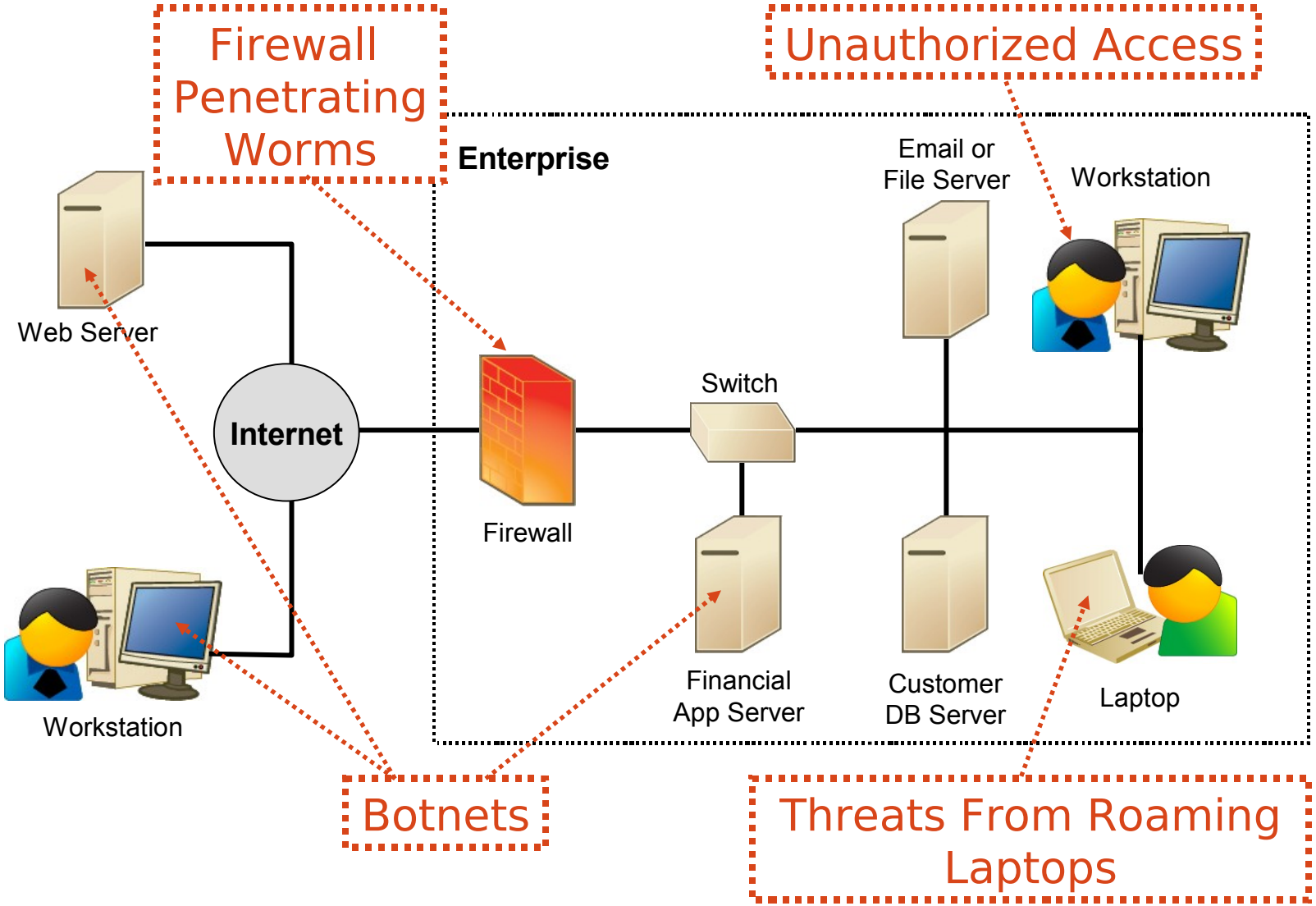
ALERTLOGIC

Network Threat Monitoring

Attacker Trends

- Attackers are better at “flying under the radar”
  - Fewer flashy, public attacks - more stealth intrusions
  - Botnets emerging as a valuable commodity
  - Threats are free to propagate throughout the network
  - Corporate security staffs not properly equipped to keep up with latest threats

Network Dangers



What Can You Do With Bots?

Command	Description
command.list	List of all the available commands
bot.dns	Resolves an IP/hostname
bot.execute	**Runs an *.exe* file on a remote computer**
bot.open	**Opens a file on a remote computer**
bot.command	**Runs a command with system()**
irc.server	Connects to an IRC server
irc.join	Enters a specific channel
irc.privmsg	Sends a private message to a user
http.execute	**Downloads and executes a file through HTTP**
ftp.execute	**Downloads and executes a file through FTP**
ddos.udpflood	Starts a UDP flood
ddos.synflood	Starts a Syn flood
ddos.phaticmp	Starts a PHATicmp flood
redirect.http	**Starts a HTTP proxy**
redirect.socks	**Starts a SOCKS4 proxy**
pctrl.list	**List of processes**
pctrl.kill	**Kills the process**

Threats Free to Propagate

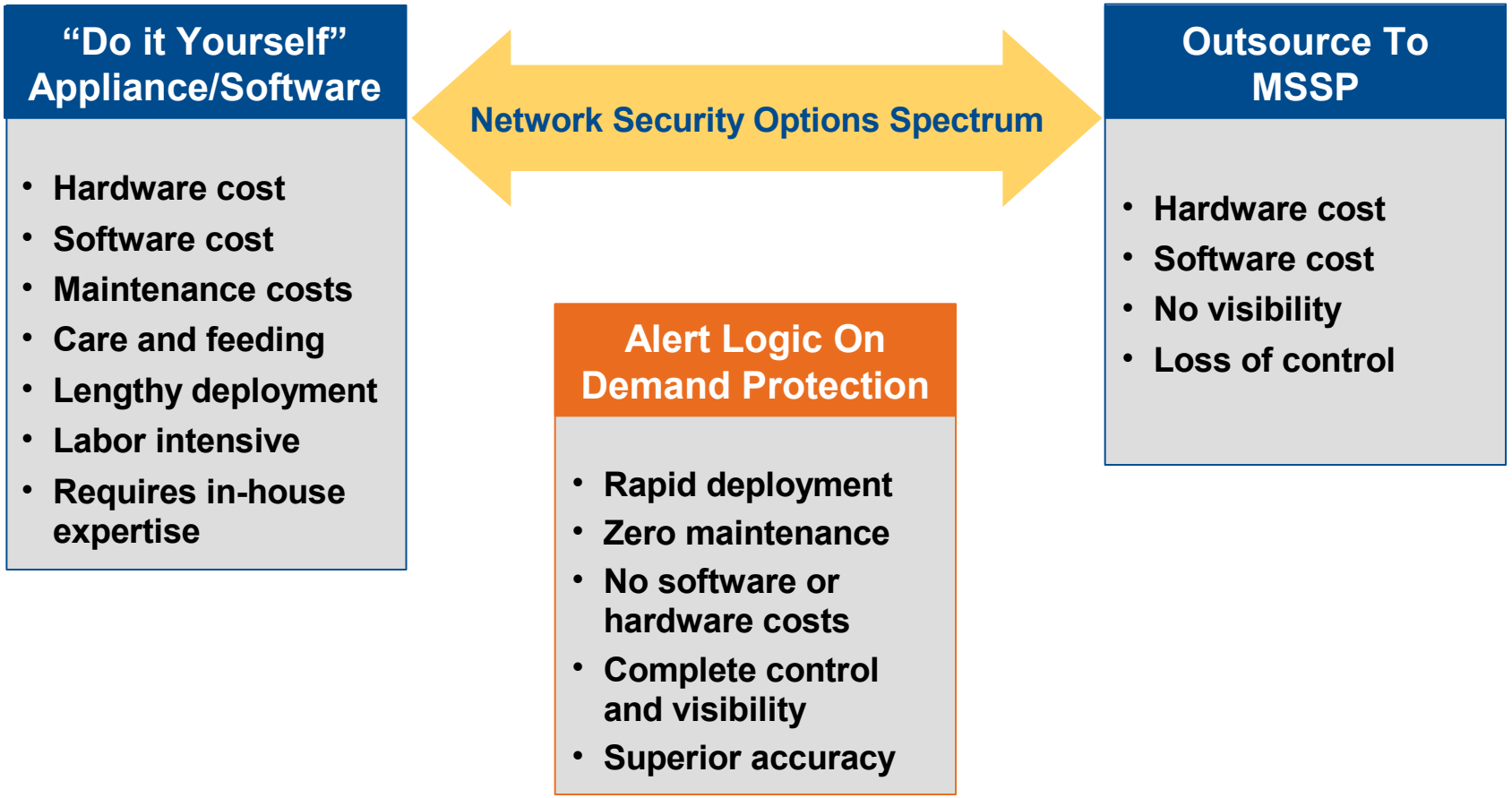
- Lack of visibility into network traffic
- No control mechanisms to stop threats once they begin to spread
- Insider threats attempting unauthorized access

Losing the Arms Race

- Most businesses ill equipped to effectively fight the bad guys
- Network security solutions complicated and difficult to deploy – “too many moving parts”

Why You Shouldn't "Do It Yourself"

How We Compare

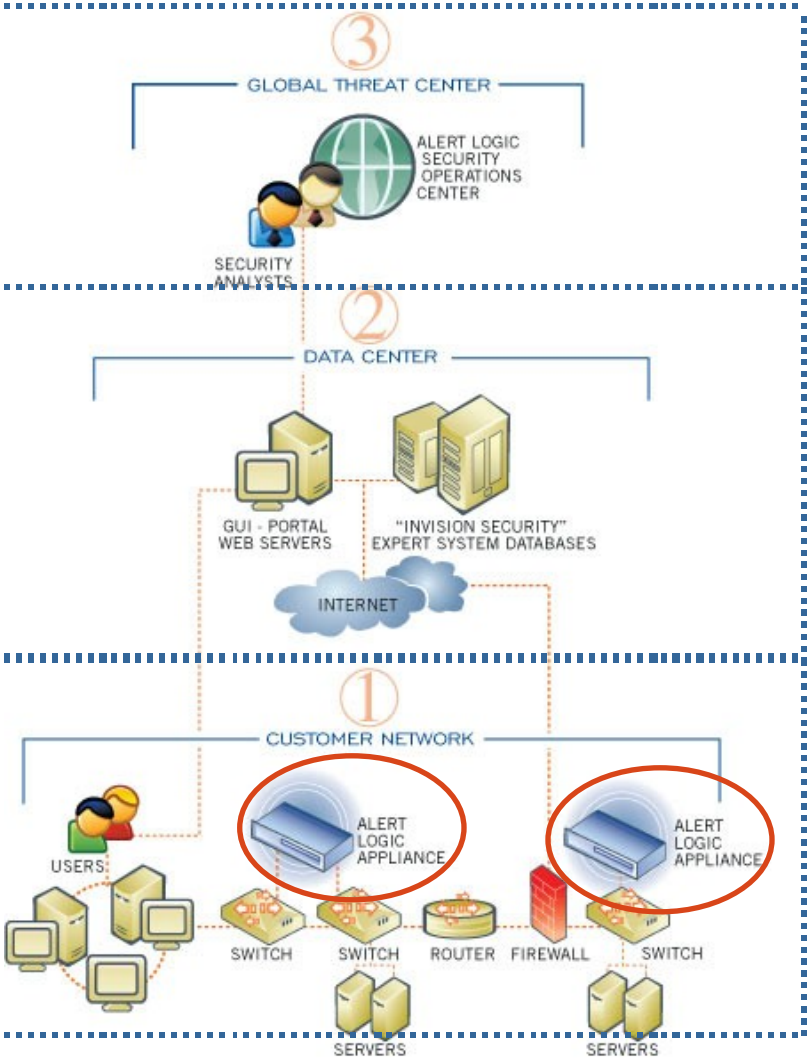


Layered “On-Demand” (SaaS) Model

Optional SOC Services

Moving Parts Are Hosted in Our Datacenter

Network Appliance(s)



Three Products in One

1

Intrusion Protection

- Leverages 8,000+ signatures
- Passive monitoring with optional blocking, containment, & quarantine defensive actions
- SSL embedded threat detection
- Incident resolution management

2

Vulnerability Management

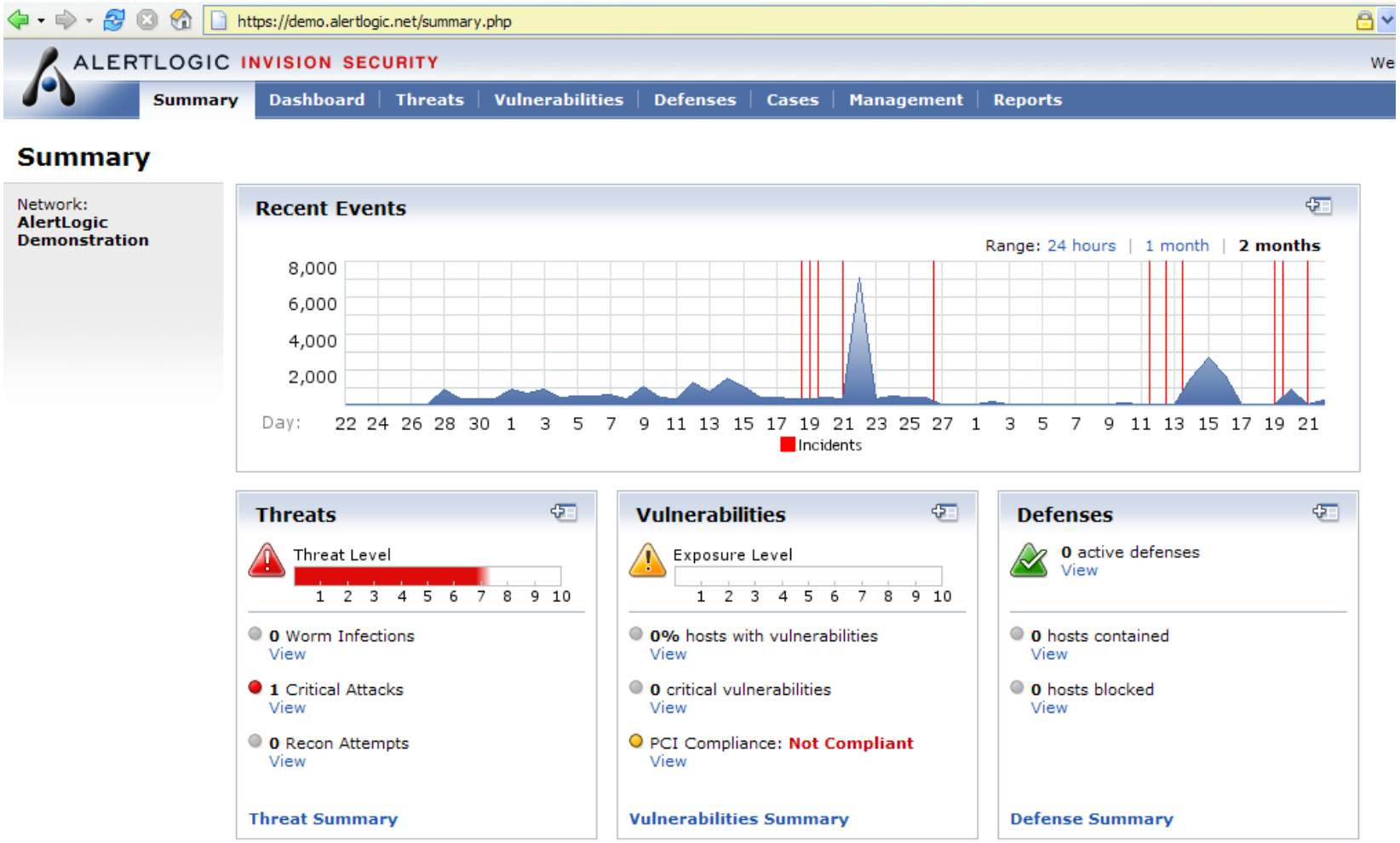
- PCI certified scanning (available in Q1 ’07)
- Automated scanning with 12,000+ vulnerabilities
- Network discovery and asset weighting
- On-Demand external and internal scanning (external available Q1 ’07)
- Exposure remediation resolution management

3

Compliance Reporting

- Compliance posture security Incident identification
- Compliance posture vulnerability identification
- Pre-built PCI, SOX, GLBA, and HIPAA reporting

Threat Manager in Action


https://demo.alertlogic.net/summary.php
ALERTLOGIC INVISION SECURITY
We
Summary
Dashboard
Threats
Vulnerabilities
Defenses
Cases
Management
Reports
Summary
Network:
AlertLogic
Demonstration
Recent Events
Range: 24 hours | 1 month | 2 months
8,000
6,000
4,000
2,000
Day:
22 24 26 28 30 1 3 5 7 9 11 13 15 17 19 21 23 25 27 1 3 5 7 9 11 13 15 17 19 21
Incidents
Threats
Threat Level
1 2 3 4 5 6 7 8 9 10
0 Worm Infections
View
1 Critical Attacks
View
0 Recon Attempts
View
Threat Summary
Vulnerabilities
Exposure Level
1 2 3 4 5 6 7 8 9 10
0% hosts with vulnerabilities
View
0 critical vulnerabilities
View
PCI Compliance: Not Compliant
View
Vulnerabilities Summary
Defenses
0 active defenses
View
0 hosts contained
View
0 hosts blocked
View
Defense Summary

https://demo.alertlogic.net/dashboard.php

Summary | Dashboard | Threats | Vulnerabilities | Defenses | Cases | Management | Reports

Dashboard (More Options)

Security Headlines

Edit |

[2/5] IBM Rational ClearQuest Web Attachments Script Insertion
Last updated on Mar 21, 2007 08:01 AM | Secunia

[2/5] Mandriva update for nas
Last updated on Mar 21, 2007 08:01 AM | Secunia

[3/5] NETxEIB OPC Server Improper Handle Validation
Last updated on Mar 21, 2007 08:01 AM | Secunia

[2/5] OpenAFS Spoofed "FetchStatus" Privilege Escalation
Last updated on Mar 21, 2007 08:01 AM | Secunia

[4/5] InterActual Player IASystemInfo.dll ActiveX Control Buffer Overflow
Last updated on Mar 21, 2007 08:01 AM | Secunia

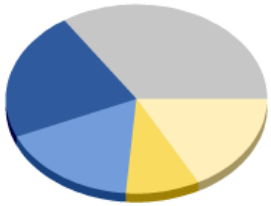
Top Incidents

Edit |

ID	Summary	Date	Threat	Events
34102	FTP brute force attempt from 172.20.2.243	Mar 13 2007 13:30:54	80	2,644
34103	Exploitation of a known vulnerability	Mar 13 2007 13:32:40	80	927
34075	Exploitation of a known vulnerability	Mar 12 2007 16:36:18	78	224
33469	Worm infected host at 10.0.2.2	Feb 21 2007 09:29:55	75	109
34030	Exploitation of a known vulnerability	Mar 11 2007 13:51:42	75	70

Top Event Sources

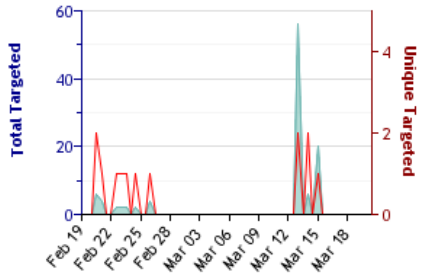
Edit |



Label	Address	Count	%
	172.20.2.243	1,952	34%
	172.20.2.244	1,303	22%
	0.0.0.0	1,009	17%
	10.0.2.2	506	9%
	All Others	982	17%

Targeted Vulnerabilities

Edit |



Vulnerability Name	Events	Risk Level	%
Microsoft Windows ASN.1 Library Integer Overflow	8	Critical	8
11032	78	Low	75
Microsoft IIS ISAPI .printer Extension	18	Medium	17

PCI Scorecard

Edit |

Current Status

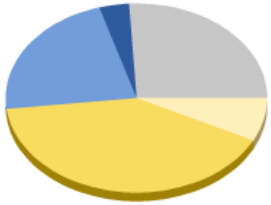
Non-Compliant
Last scan: N/A

Access

Inappropriate Access to Systems or Data	2 Items For Review
Buffer Overflows	1 Item For Review
Injection Flaws	176 Issues Require Action
Generic/Default User Accounts	176 Issues Require Action
Default Passwords	176 Issues Require Action

Incidents by Threat Level

Edit |



Label	Threat Level	Count	%
	Low	7	26%
	Medium	1	4%
	High	6	22%

https://demo.alertlogic.net/threats.php

ALERTLOGIC INVISION SECURITY

Summary | Dashboard | Threats | Vulnerabilities | Defenses | Cases | Management | Reports

Threats

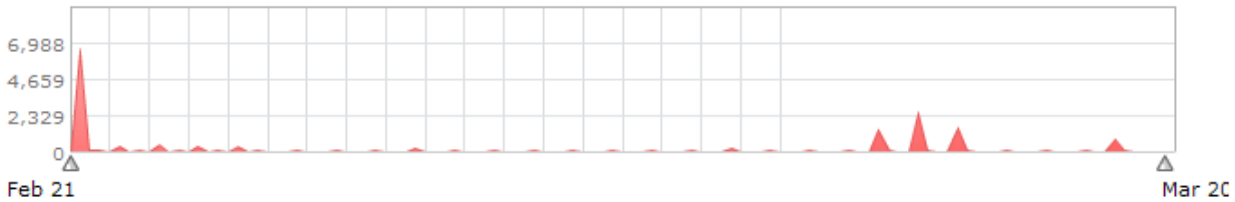
Search Incidents
View All Incidents
Search Events
View All Events

Configure Incident Monitor
Configure Event Monitor
Configure Alerts

Did you Know?

You can be automatically alerted of new threats. Configure your event alert rules to enable this feature.

Range: **Feb 21 2007 - Mar 20 2007** | Threats: **17,246**



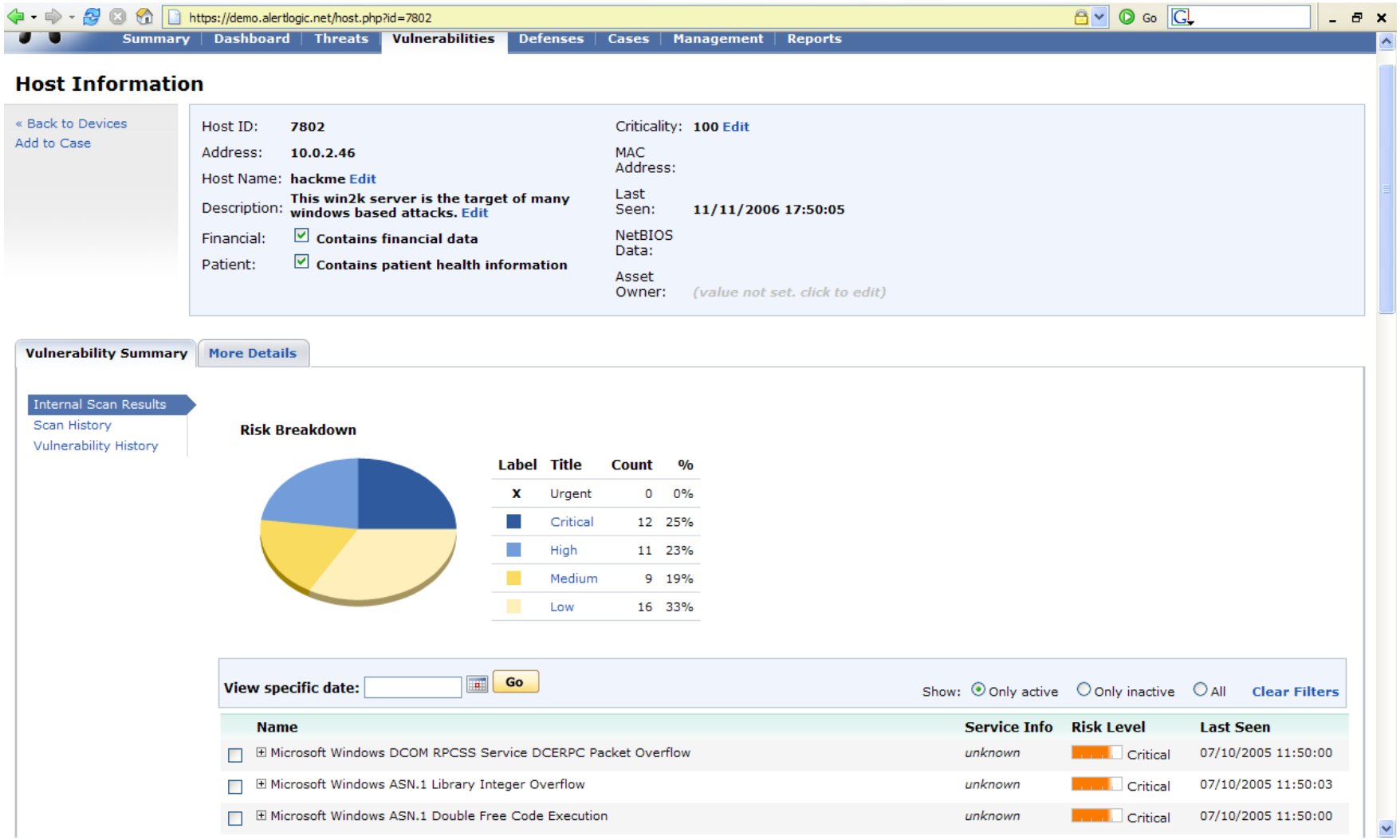
Incidents | Intrusion Events

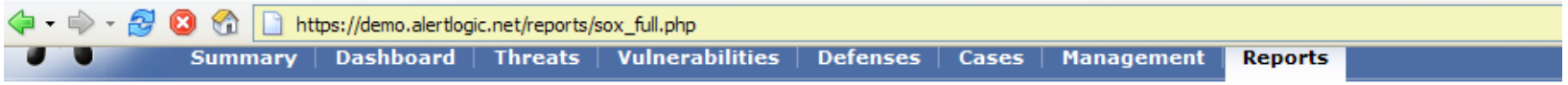
Latest Incidents
Top Incidents
By Threat
By Status
By Classification
Worms Spreading

View All Incidents

ID	Summary	Date	Threat	Events
27366	Webserver responded to a cmd.exe attack	Today 06:02:49	73	68
18002	Nikto vulnerability scan	Mar 19 2007 11:42:52	74	2
34120	Directory listing via PnP Exploit	Mar 13 2007 18:20:11	12	1
34107	PnP QueryResConfList exploit attempt from 10.0.2.2	Mar 13 2007 13:40:20	66	74
34105	Directory listing via PnP Exploit	Mar 13 2007 13:36:58	54	47

Home | My Account


https://demo.alertlogic.net/host.php?id=7802
Summary
Dashboard
Threats
Vulnerabilities
Defenses
Cases
Management
Reports
Host Information
« Back to Devices
Add to Case
Host ID: 7802
Address: 10.0.2.46
Host Name: hackme Edit
Description: This win2k server is the target of many windows based attacks. Edit
Financial: Contains financial data
Patient: Contains patient health information
Criticality: 100 Edit
MAC Address:
Last Seen: 11/11/2006 17:50:05
NetBIOS Data:
Asset Owner: (value not set. click to edit)
Vulnerability Summary
More Details
Internal Scan Results
Scan History
Vulnerability History
Risk Breakdown
Label Title Count %
X Urgent 0 0%
Critical 12 25%
High 11 23%
Medium 9 19%
Low 16 33%
View specific date:
Go
Show: Only active Only inactive All
Clear Filters
Name
Service Info
Risk Level
Last Seen
Microsoft Windows DCOM RPCSS Service DCERPC Packet Overflow unknown Critical 07/10/2005 11:50:00
Microsoft Windows ASN.1 Library Integer Overflow unknown Critical 07/10/2005 11:50:03
Microsoft Windows ASN.1 Double Free Code Execution unknown Critical 07/10/2005 11:50:00



SOX - Full Report

« Back to Reports

PDF Version

Excel Version

Company:	**AlertLogic Demonstration**	Date Range:	**February 19 2007 12:00am to March 21 2007 11:49am**
Customers:	**AlertLogic Demonstration**	Generated:	**Wednesday, March 21 2007**
User:	**demo1**		

This report only includes data related to hosts with the financial flag set. For the purposes of this report, the included hosts are:

10.0.2.2	10.0.2.254	10.0.2.41	10.0.2.3
10.0.2.46	10.0.2.47	10.0.2.43	10.0.2.11
10.0.2.47	10.0.2.42	10.0.2.48	

Executive Summary

The SOX Executive Summary lists specific of security controls that relate to data collected by Invision Security. For each general category, the specific of controls are listed, with their respective issue counts. If any category has issues present, the number of issues will be listed and clicking on that category title will provide further information about the issues affecting it.

Access

Unauthorized Access to Financial Systems	7 Items For Review
Weak Passwords	176 Issues Require Action
Default User Accounts	176 Issues Require Action

Configuration Management

Latest Patches Not Installed	43 Issues Require Action

Incidents

Feature/Benefit Summary

- 3-in-1 Solution
  - –Fully integrated solution eliminates the difficult task of correlating data from multiple sources to get a comprehensive picture of the security posture of your network.
- 24x7 Monitoring
  - –Alert Logic is always keeping an eye on your network, even when you can't. This ensures threats are addressed in the timeliest fashion to secure your network before damage can occur, freeing your staff to perform other high-priority tasks.
- Co-Managed w/ Full Visibility
  - –Alert Logic's On-Demand model means that we do it all for you. But you maintain full visibility and control over network security using the same GUI as the Alert Logic 24x7 monitoring team.
- Blocking and Containment
  - –We can terminate communication to/from a threatened asset at the firewall and either contain or quarantine at the switch, thereby eliminating threats before they harm your network.
- Extensive compliance reports
  - –Comprehensive reporting includes detailed and executive-level reports, providing easy communication of network security posture and helping to satisfy compliance requirements.
- No Maintenance Required
  - –Alert Logic manages all upgrades, updates, and maintenance of the application, freeing your staff from this expensive and time consuming task.
- Simple one-day installation
  - –Alert Logic's On-Demand solution eliminates the implementation burden associated with do-it-yourself solutions. This ensures a successful one-day installation and frees your staff from the expensive and time-consuming task of setting up hardware, loading software, network rollout, QA, and testing.

What should you do?

- Stop thinking of network threats as a nuisance
- Stop focusing exclusively on the perimeter
  - Inside of firewalls networks are wide open today
  - Businesses continuously spend 80% of their budget to fix 20% of their problem
- Automate incident investigation and response
  - Defense today is shrouded in uncertainty and reliant on manual decisions
  - Few businesses have situational awareness that allows them to identify complex threat scenarios
  - Network security has to become automated to be effective

In Summary

- Security issues are much more prevalent but rarely get the appropriate attention
- Perimeter security is limited in it's ability to prevent Network Threats
- Attackers and their exploits may take multiple vectors to achieve their goals
- Additional layers of defense should reduce burden on you, not be a burden