Dell SecureWorks

Counter Threat Unit Research Team

- Elite cyber intelligence talent focuses on threat actors, tradecraft and countermeasures

Counter Threat Platform

- Next generation technology applies intelligence to protect thousands of customers worldwide

Certified Security and Compliance Experts

- 1,000+ security and compliance professionals deliver award-winning services and customer satisfaction

Global Security Operations Centers

- 7 resilient, high-security facilities provide vendor-neutral, in-region service delivery 24x7x365

We help **thousands** of organizations **protect against cyber threats, simplify regulatory compliance** and **embrace innovation securely**.

• Classification: //De

SecureWorks

GLBA
FFIEC
NCUA
PCI
HIPAA
NERC CIP
FISMA

700+
Federal and state security-related laws

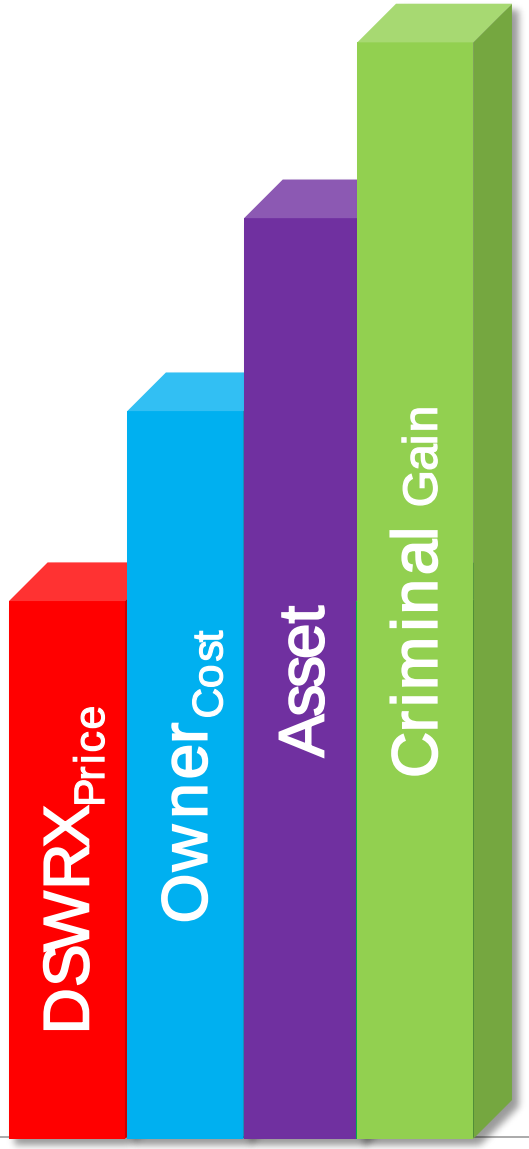
50
U.S. states with varying data breach laws

8,000
Security-related software vulnerabilities publicly disclosed

76%
IT staffs report being buried in basic daily activities with little time to focus on security & other projects

Role of a managed security service provider

Increase risk
Reduce reward
Increase effort



• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

SecureWorks

An integrated approach to security

Core Assets	CTU Intelligence	Flexible Approach	Vertical Expertise	Purpose-built Technology	Scalable Security Operations	Certified Security Experts
Services	Threat Intelligence	Managed Security	Security & Risk Consulting	Incident Response & Digital Forensics		
Business Value	Threat Mitigation	Visibility	Flexibility	Cost Control	Compliance	Rapid Response

Dell SecureWorks delivers a comprehensive suite of information security services powered by our proprietary technology, global threat visibility and deep security expertise

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Information Security Leader

XCHANGE events
MES XCellence Awards 2012

Gartner

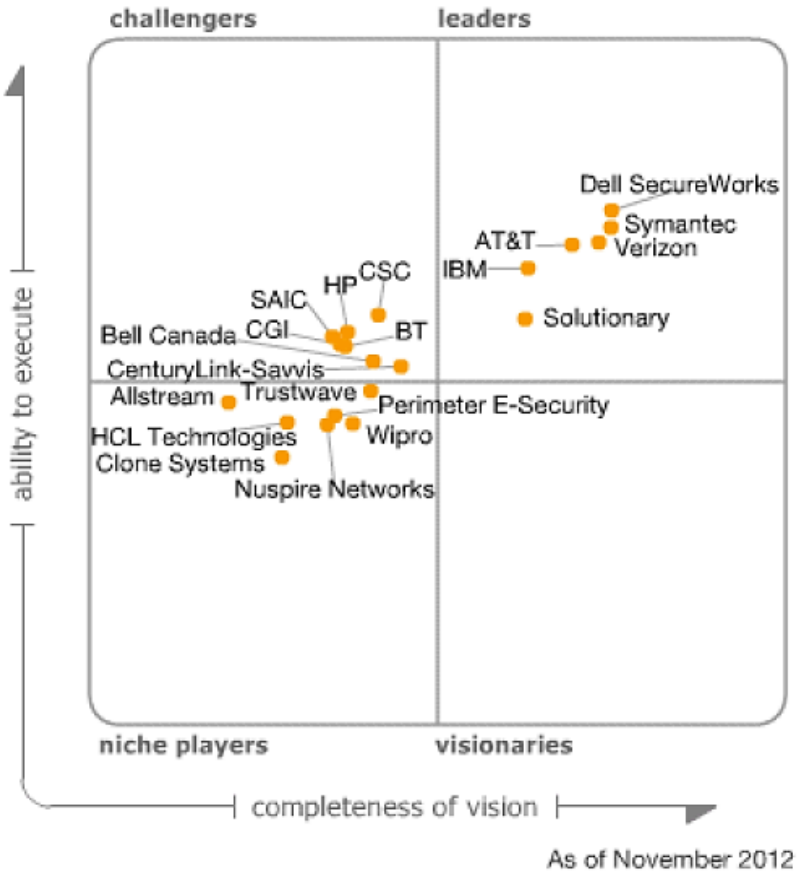
FORRESTER

MIDSIZE ENTERPRISE INNOVATION AWARDS 2011
Everything CHANNEL events

SC MAGAZINE AWARDS 2006 WINNER
SC MAGAZINE AWARDS 2007 WINNER
SC MAGAZINE AWARDS 2008 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2009 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2011 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2012 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2011 EUROPE WINNER

Dell SecureWorks positioned as a Leader in the Magic Quadrant for MSSPs, North America

"Gartner sees continued expectations to reduce operational costs and capital expenditures, and avoid staffing increases, while maintaining a sufficient security posture and meeting compliance mandates."



Source: Gartner "Magic Quadrant for MSSPs, North America" by Kelly M. Kavanagh, 15 November 2012.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Dell SecureWorks

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Dell. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Industry stats

Doubling each year

New pieces of malicious code found daily
- 2011: 150,000 daily
- 2010: 75,000 daily
- 2009: 37,500 daily

1 of 6

SMBs has experienced an IT security breach (1 million+ U.S. companies)

71%

Mobile devices in SMB environment found to have high severity operating system and application vulnerabilities

$11.3 million

Estimated sales/revenue opportunities lost by U.S. SMBs as a result of IT security breaches in the past year

$5.6 million

Estimated spend by U.S. SMBs to replace damaged hardware as a result of IT security breaches in the past year

22 million

Estimated staff-hours that U.S. SMBs have lost handling security breaches in the past year

40%

Of all targeted attacks during past two years directed at companies with fewer than 500 employees

96%

Of breached companies subject to PCI DSS had not achieved compliance status

92%

Of breach incidents were discovered by a third party

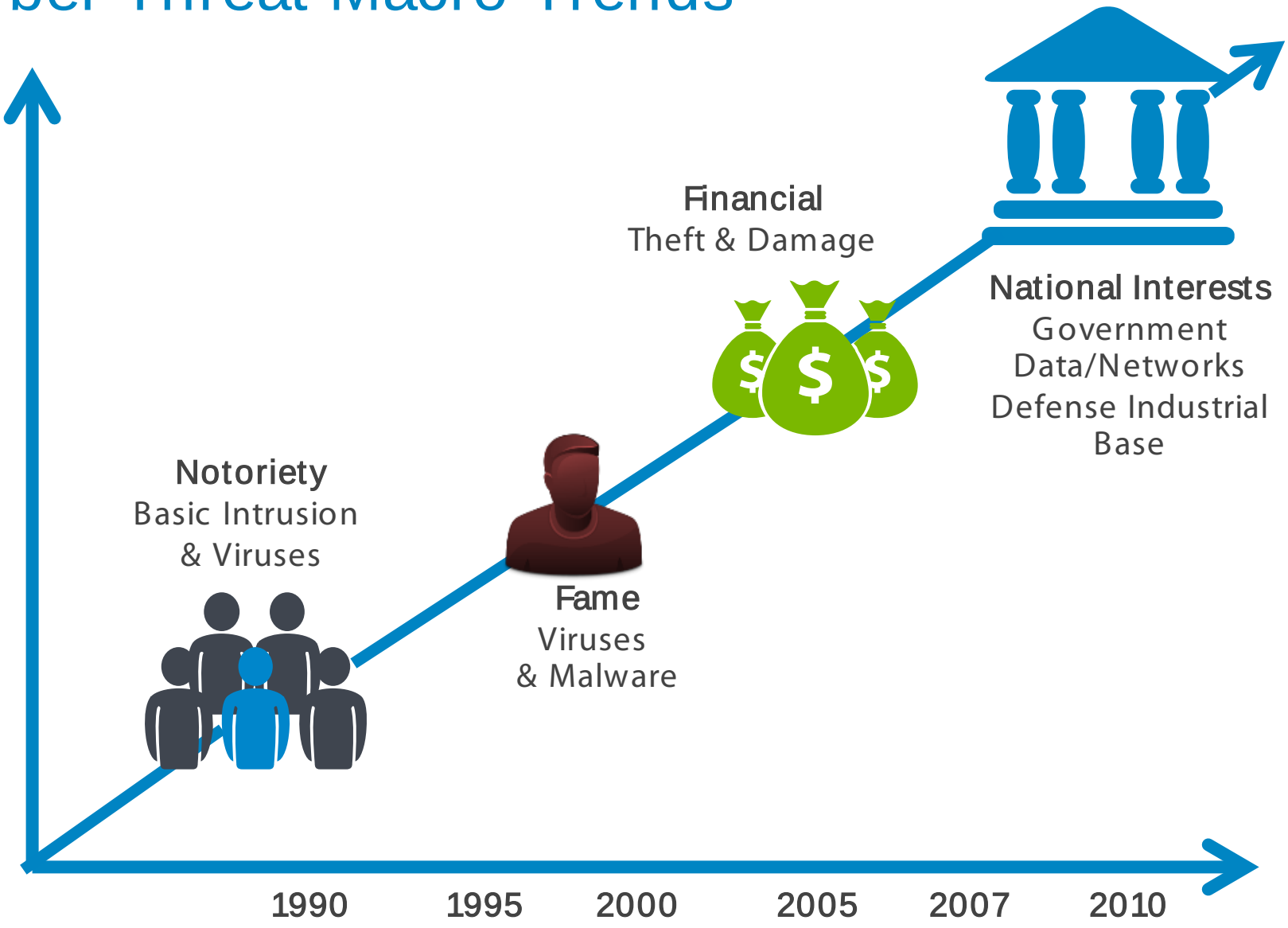
DELL SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Current Threat Landscape

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Cyber Threat Macro Trends



Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

The threat landscape

Malware

Malicious software that disrupts computer operation, gather sensitive information, or gain unauthorized access to computers

Computer viruses, worms, trojan horses, spyware, adware

Advanced Threats

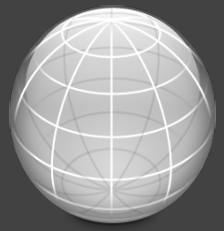
A sophisticated and organized cyber attack to access and steal information from compromised computers

DoS & DDoS

Denial-of-Service

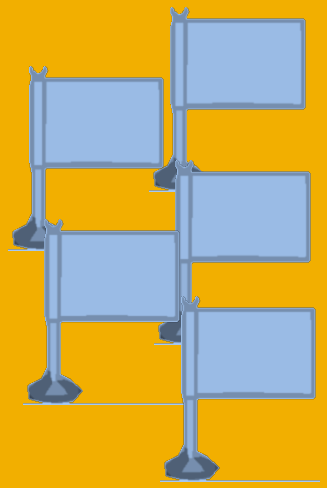
Distributed Denial-of-Service

An attempt to make a computer or network resource unavailable to its intended users



Cyber Warfare

Politically motivated hacking to conduct sabotage and espionage



SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Cyber attacks edging out terrorism as No. 1 threat to U.S.

"In the not too distant future, we anticipate that the cyberthreat will pose the No. 1 threat to our country."

"No company is immune, from the Fortune 500 corporation to the neighborhood 'mom and pop' business."

"I am convinced there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Source: FBI Director Robert Mueller
Speaking at 2012 RSA Conference

DELL SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

According to top cyber security experts

Companies need to do more than just *react* to intrusions

Companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking – or the costs they may have already suffered.

He doesn't believe there is a single secure, unclassified computer network in the U.S.

FBI agents are increasingly coming across data stolen from companies whose executives had no idea their systems had been accessed.

In cases handled by one computer security firm where intrusions were traced back to China, 94% of the targeted companies didn't realize they had been breached until someone else told them.

"In many cases, the skills of the adversaries are so substantial that they just leap right over the fence and you don't even hear an alarm go off."

Source: "U.S. Outgunned in Hacker War"
The Wall Street Journal, March 28, 2012

DELL SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Motivations Behind Cyber Crime

- Gain financial advantage
- Intelligence gathering
- Gain competitive advantage
- Damage organizations' brand, reputation and systems
- Obtain indirect access to a targeted business partner

Project "Scareware". Defrauded consumers of $100 million dollars

Co-conspirators are wanted by FBI and Interpol

DELL SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Criminal to Criminal

Increase in criminal-to-criminal activity

- Exploit auction houses (WabiSabiLabi)
- Forums and IRC (# Vxers, cybermafia.cc)
- Distribution service (IFRAMES.BIZ)
- Botnet rental (5Socks.net)
- Licensing model (storm worm)
- Identity auctions (76service)
- Social networks (ranking and escrow)

Fourth generation

SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

What If Hackers Inc. Were a Company?

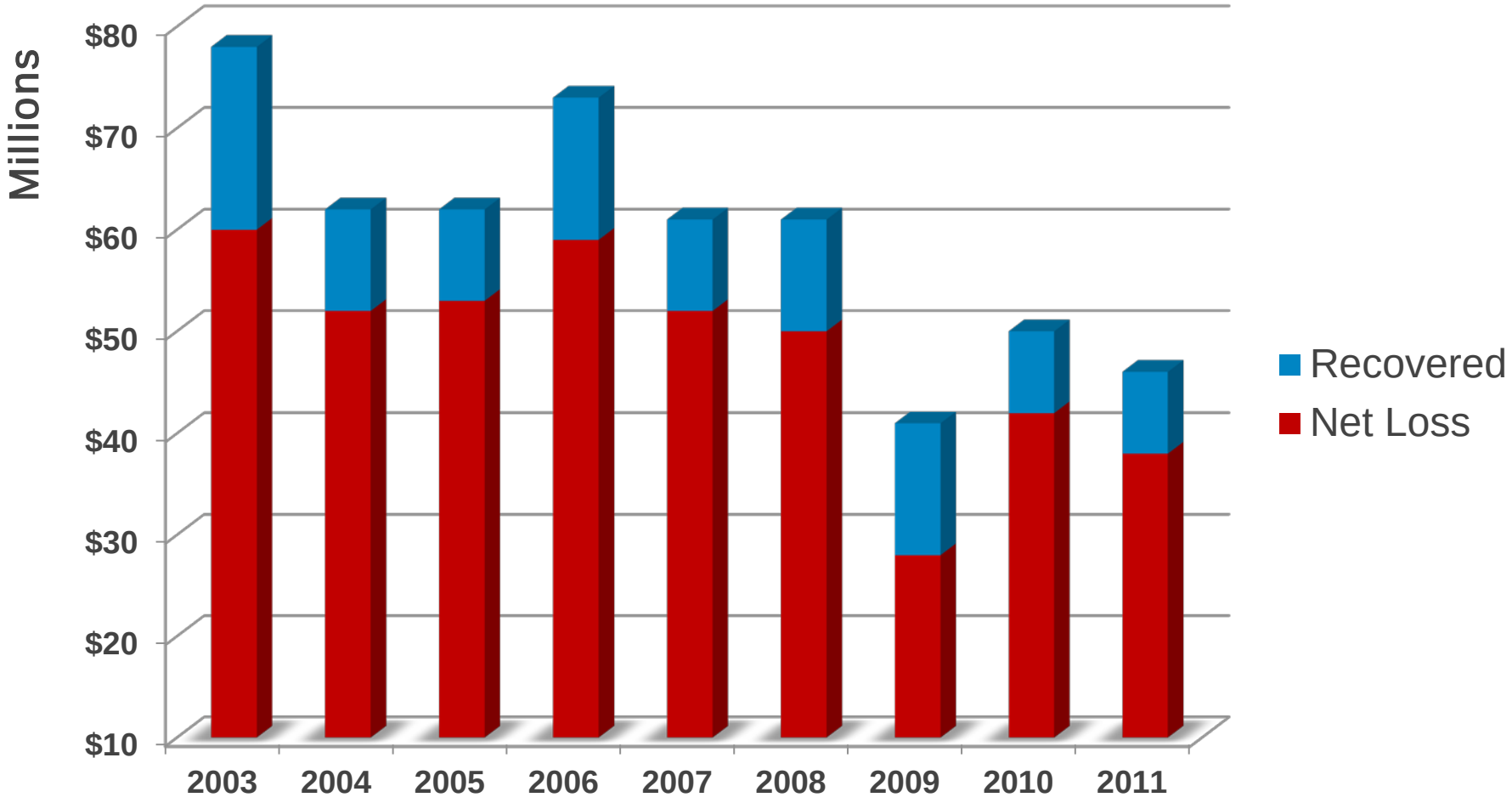
Rank	Company	Revenues ($ millions)	Profits ($ millions)
1	Wal-Mart Stores	421,849.0	16,389.0
2	Exxon Mobil	354,674.0	30,460.0
3	Chevron	196,337.0	19,024.0
4	ConocoPhillips	184,966.0	11,358.0
5	Fannie Mae	153,825.0	-14,014.0
6	General Electric	151,628.0	11,644.0
7	Berkshire Hathaway	136,185.0	12,967.0
8	General Motors	135,592.0	6,172.0
9	Bank of America Corp.	134,194.0	-2,238.0
10	Ford Motor	128,954.0	6,561.0
11	Hewlett-Packard	126,033.0	8,761.0
12	AT&T	124,629.0	19,864.0
13	J.P. Morgan Chase & Co.	115,475.0	17,370.0
14	Citigroup	111,055.0	10,602.0

#1

74x > Walmart

FORTUNE 500

Losses due to “traditional" crimes

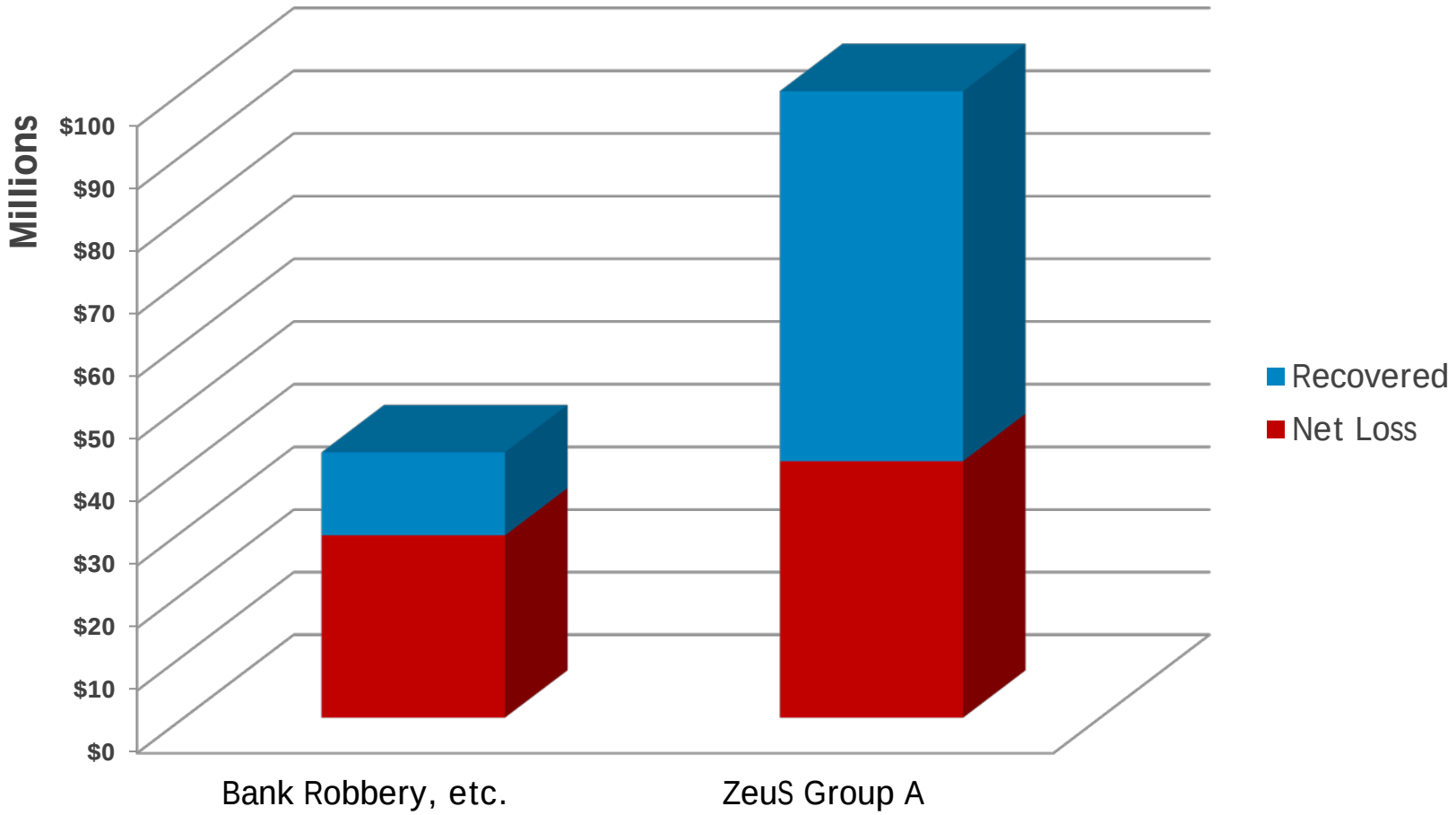


Source: FBI Bank Crime Statistics (BCS) Federally Insured Financial Institutions January 1, 2003- December 31, 2011

SecureWorks

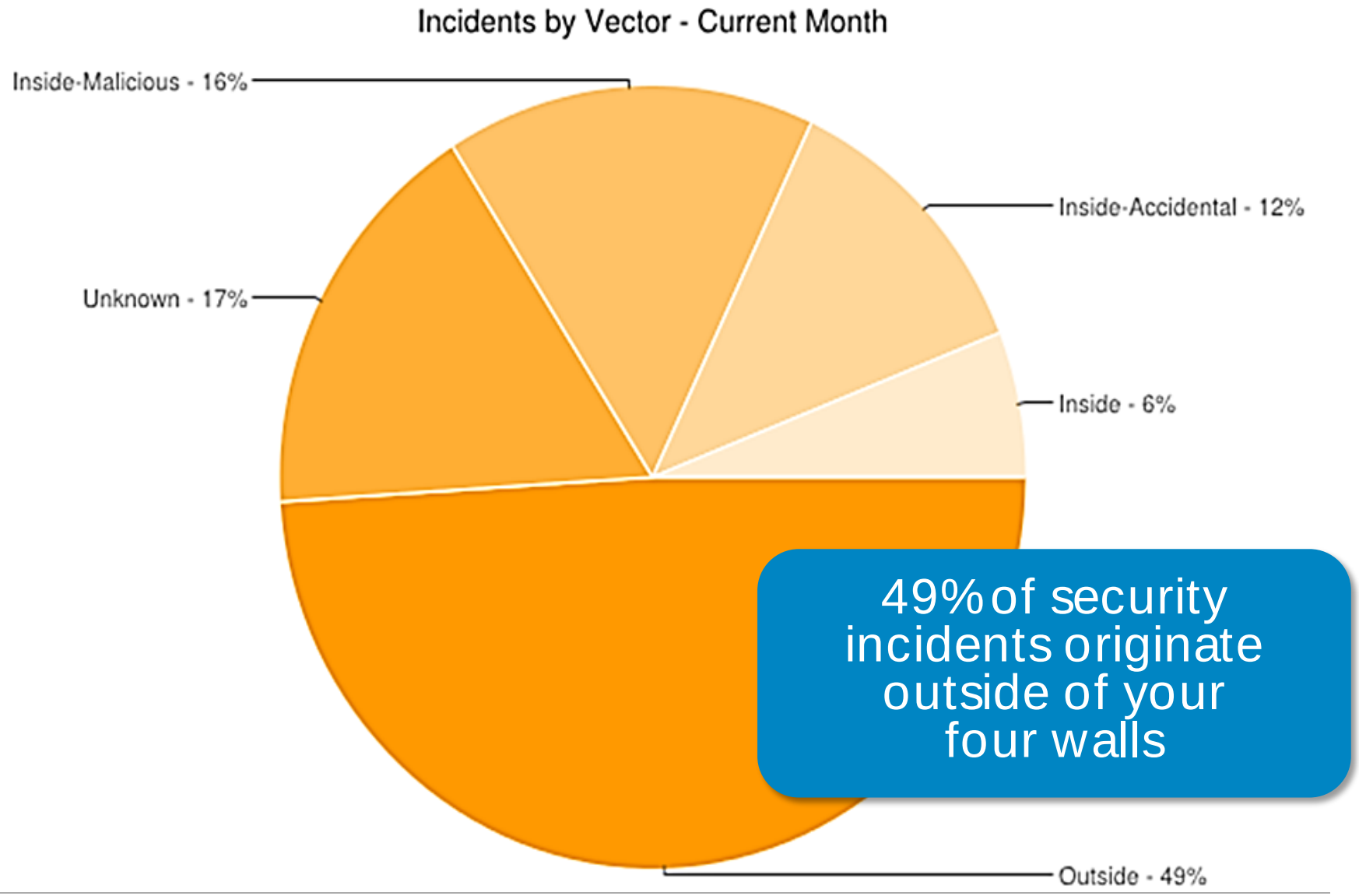
- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Cybercrime vs. traditional crime



• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Incident Source Trend March 2013

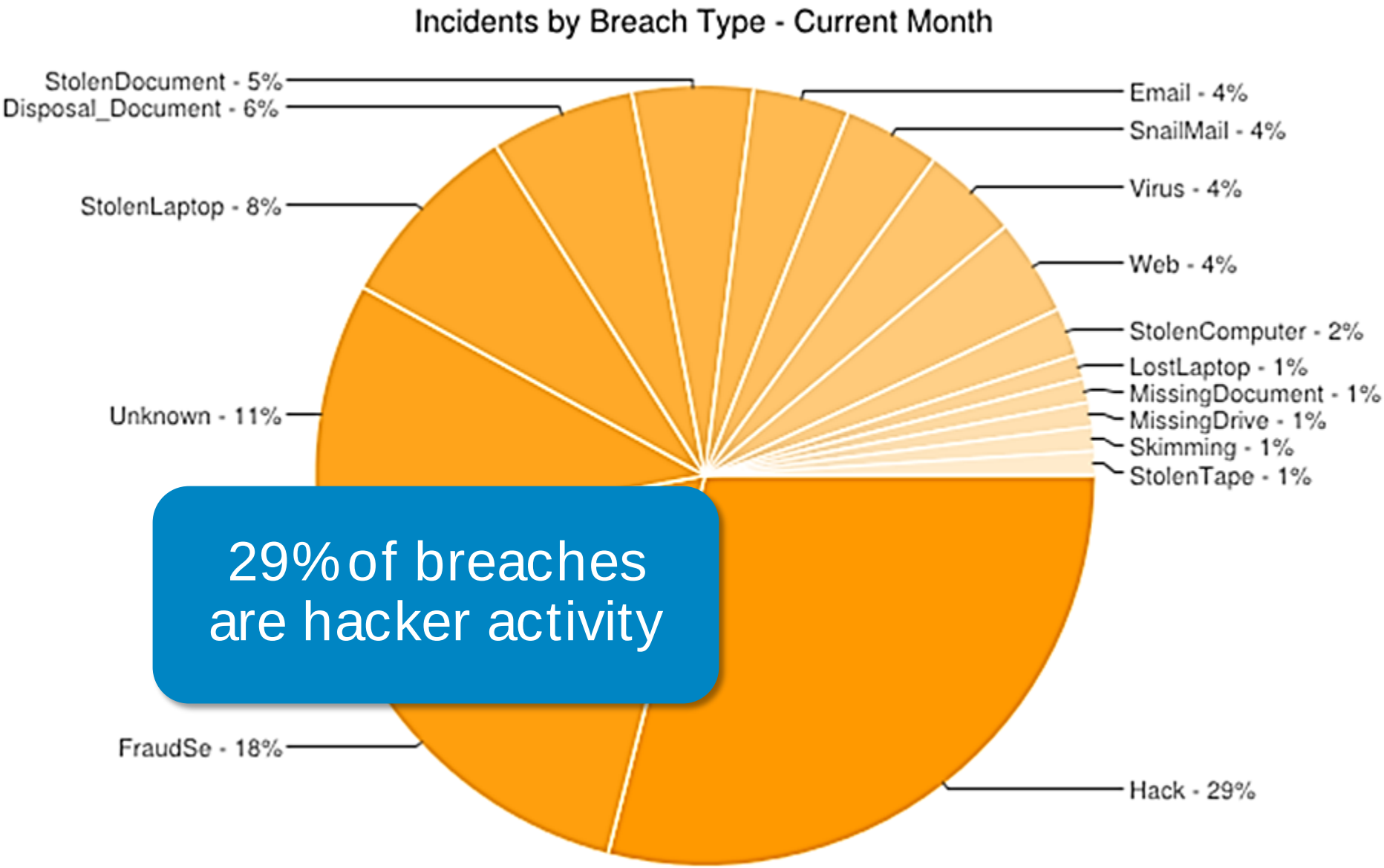


49% of security incidents originate outside of your four walls

Source: OSF DataLossDB

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Breach Trend March 2013

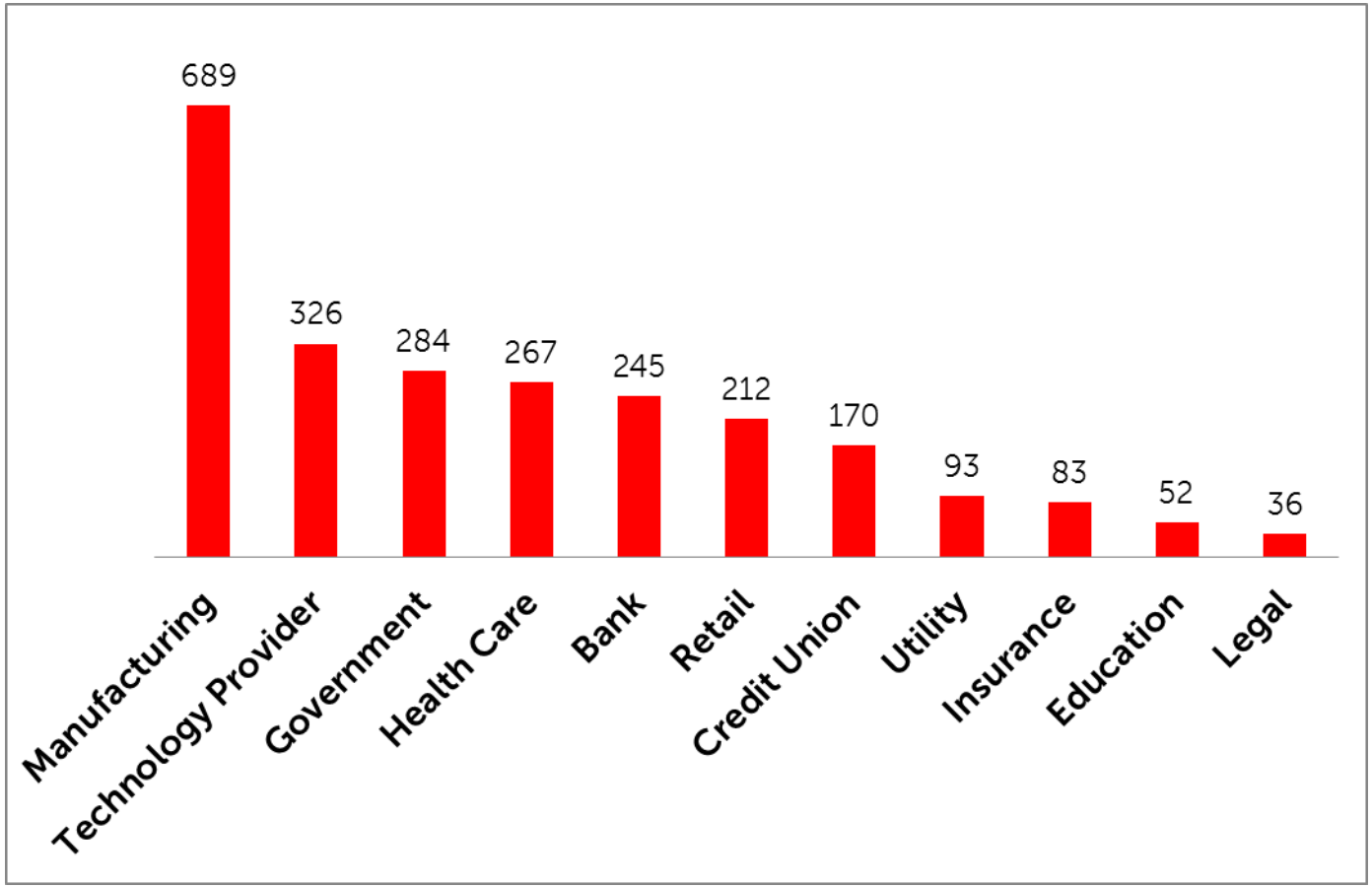


29% of breaches are hacker activity

Source: OSF DataLossDB

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Attacks per month, per customer (Q1/2012)



Source: Dell SescureWorks Counter Threat Unit Intelligence

SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Hacker Activity is Global

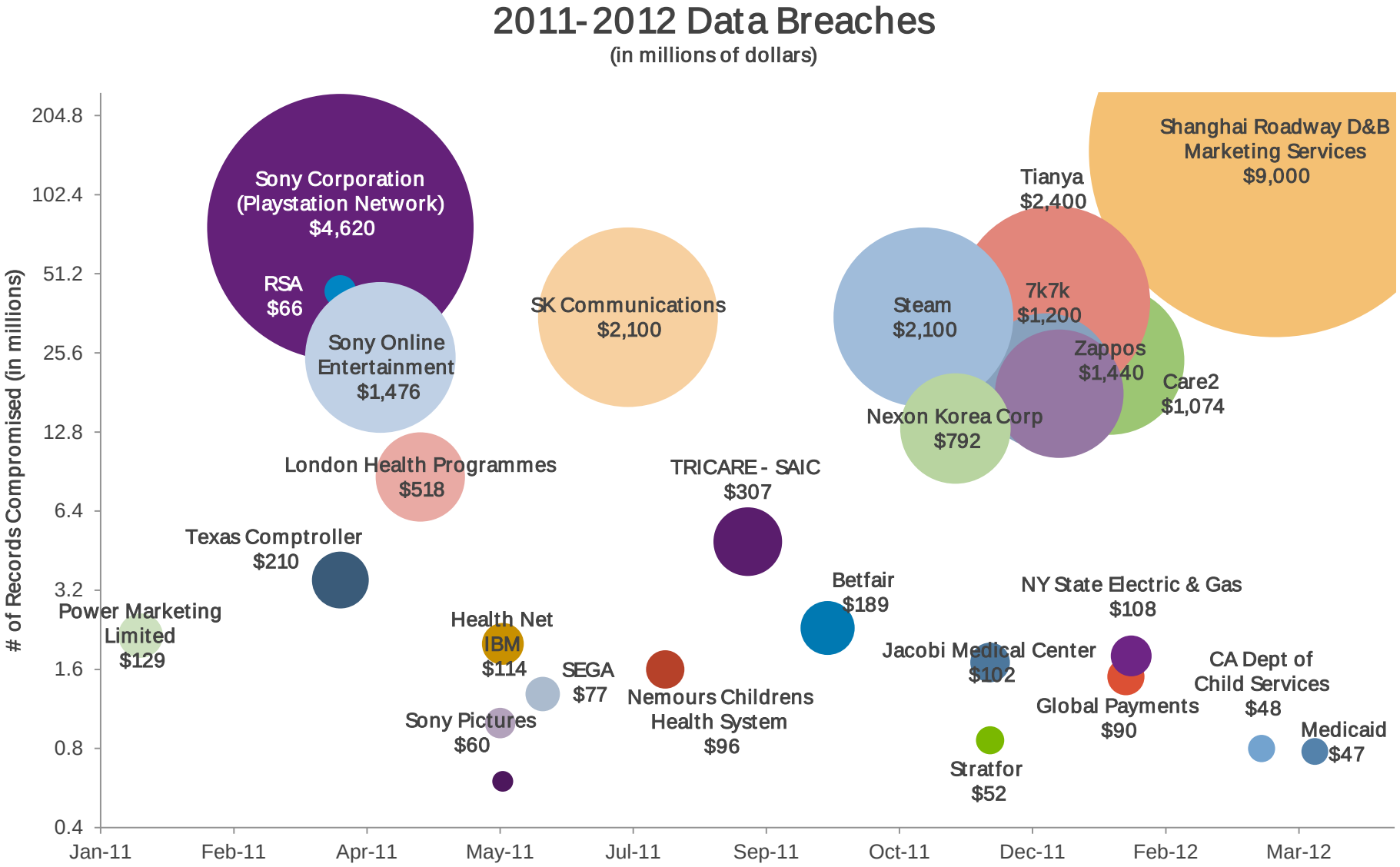
1. China
2. India
3. Vietnam
4. Russia
5. US
6. Ireland
7. Poland
8. Belarus
9. Mexico
10. Ukraine

Source:Team Cymru

SecureWorks

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Data Breaches are costly



Breaches and estimated costs retrieved from datalossdb.org, and idtheftcenter.org
Sony's records and costs reduced to fit on the map. Records exceeded 77m, and est. cost exceeds $4bln
RSA records reduced to fit on the map. Actual records compromised was approx. 40m.

- Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

DELL SecureWorks

High profile compromises, Q4 2012

2012

October

11 — **Florida College**
(300,000 PII. Identity theft)

24 — **Barnes & Noble**
(PoS PII)

29 — **South Carolina Dept. of Revenue**
(3.6M tax records)

30 — **Experian**
(17,000 credit reports)

November

5 — **Coca-Cola**
(Chinese APT, cyberespionage)

2 — **Russian Government**
(Team GhostShell, 2.5M accounts)

14 — **NASA**
(Employee PII)

26 — **Greece**
(9M citizen records, suspect arrested)

December

3 — **China/QQ Messenger**
(1 Billion PII, suspect arrested)

3 — **Nationwide**
(1M PII)

26 — **Council on Foreign Relations**
(APT, IE 0-day)

28 — **Verizon**
(300K PII, third party leak by TibitXimer)

Threat Intelligence

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

The Counter Threat Unit

Top security talent in the industry

- Former CERT, Army Global NOSC, USCYBERCOM, DoD, Natl. Labs, CISOs and SANS instructors

Highly regarded in the security community

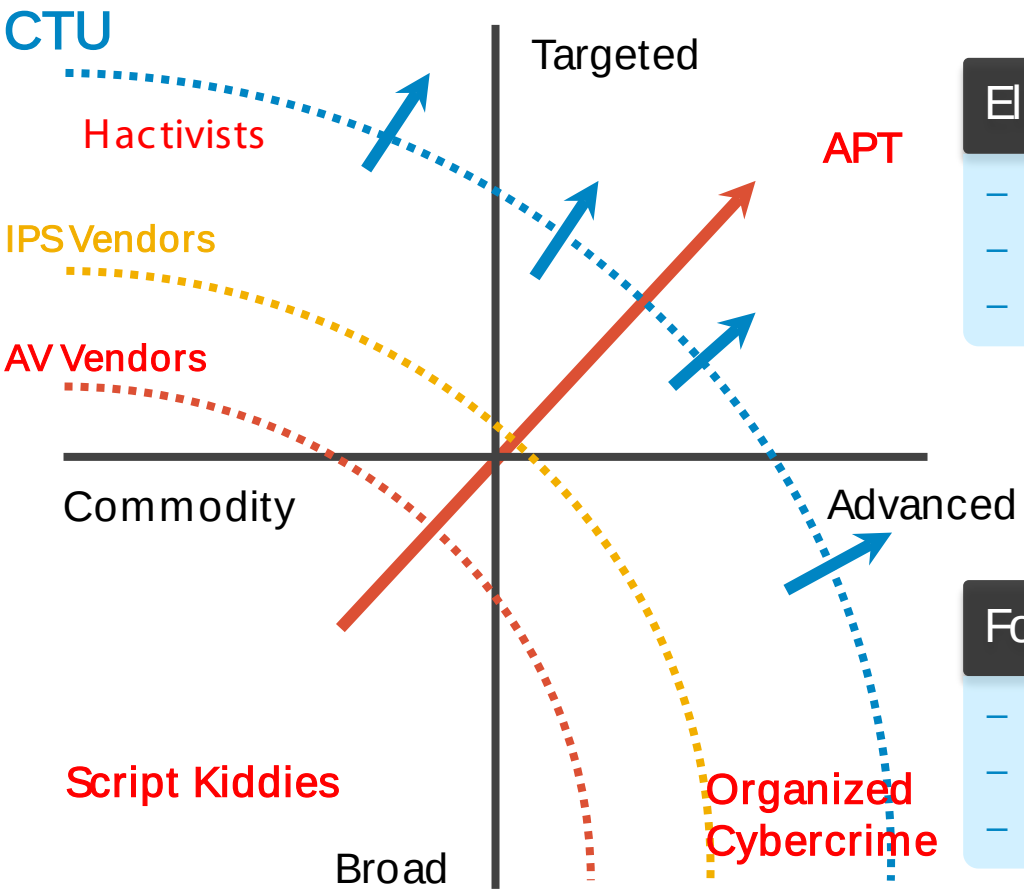
- Black Hat, DEFCON, ShmooCon, ToorCon, DeepSec, U.S. DoD Cyber Crime Conference, CERT-EE, AusCERT, Hacker Halted, RECON, APWG

1,000+ security and compliance experts

- CISSP
- INFOSEC
- CISA
- GIAC GCIA
- GIAC GSEC
- GIAC GCFW
- GIAC GCIH
- GIAC GCFA
- GIAC GCWN
- GIAC GPEN
- CCDP
- CCNA
- CCSE
- CSPFA
- CSVPN
- CSIDS
- CCSP
- CCIE
- CCSA
- CCDA
- CCNP
- INFOSEC
- MCSA
- MCSE
- MCP+I
- MCSE+I
- PMP
- NCSA
- CFE
- CCSI
- CEH
- NOP

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

CTU's strategic focus



Elite cyber-intelligence experts

- Current and historical rich attack data
- World-class intelligence platform and tools
- Industry and law enforcement relationships

Focused on "who" and "how"

- Threat actors and their missions
- Tradecraft used in attacks
- "Kill chain" – how to disrupt attack process

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Global threat visibility

70+	3K+	1K+	24x7 x365	~38B	2K+
Countries	Customers	Security Pros		Daily Events	Daily Escalations

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Real Life Examples

- Flame Malware
- Gameover Zeus Trojan Horse
- Searchhereonline downloader
- Blackhole Exploit Kit
- Targeted Exploit - CVE-2012-4681

Dell SecureWorks CTU deploys 161 countermeasures to protect customers.

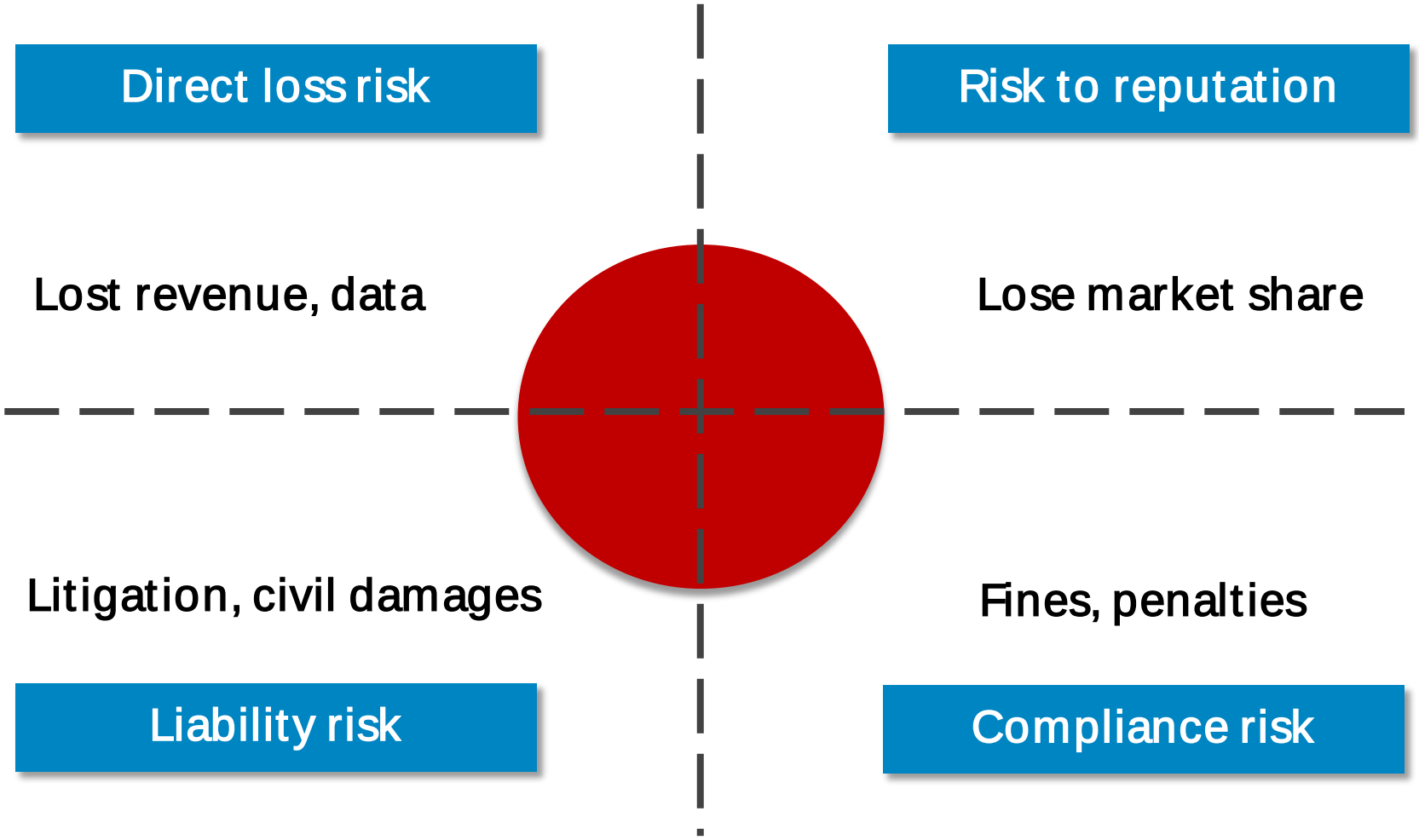
Existing countermeasures already in place to detect and block Pony downloader activity.

Existing countermeasures already in place to detect activity associated with this downloader trojan.

CTU already has countermeasures in place to detect and block Blackhole Exploit Kit

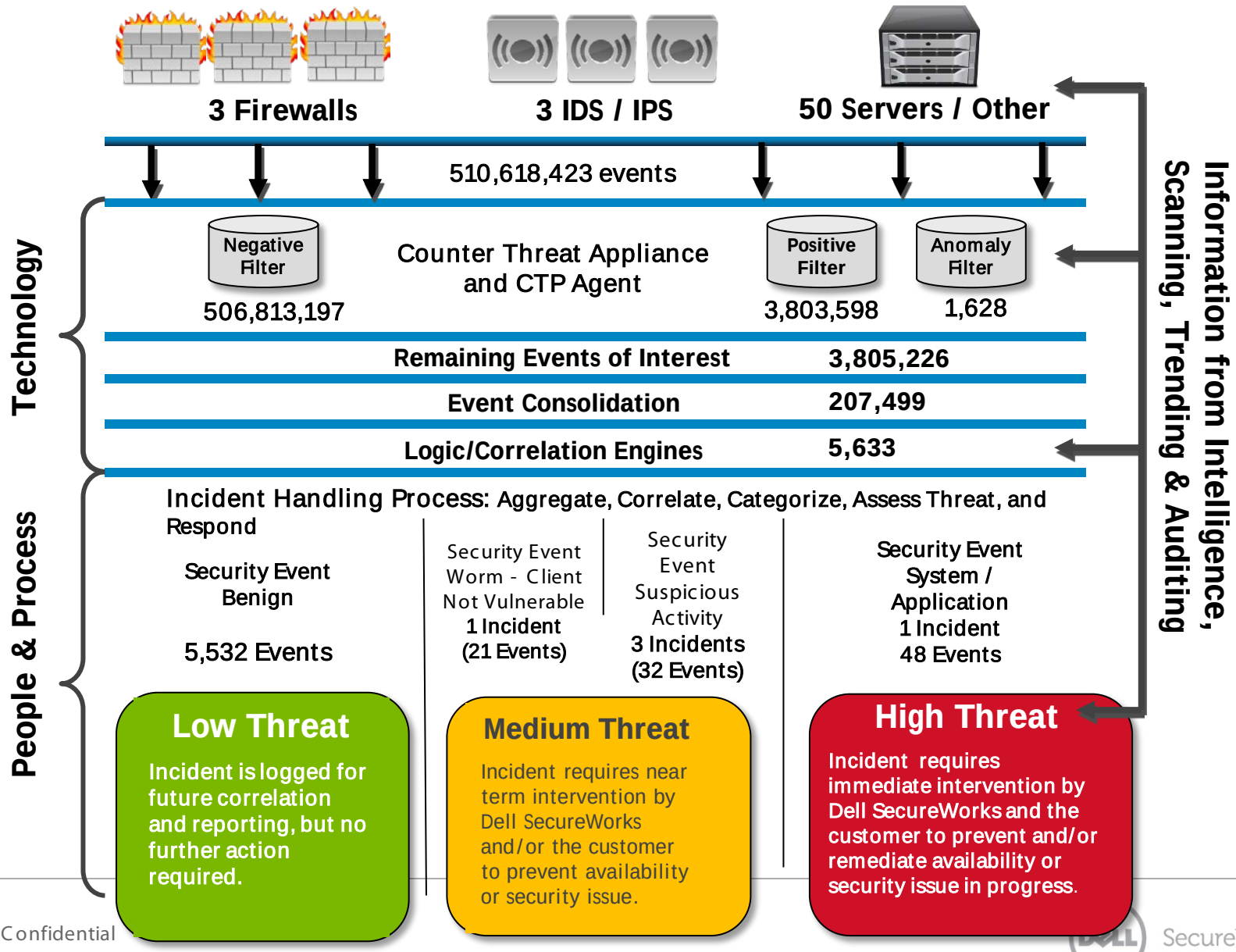
CTU developed iSensor countermeasures to detect and block traffic associated with this exploit

Risk-based approach



• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Real-time monitoring and analysis



SecureWorks

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Be proactive

- Invest in prevention
- Educate your employees
- Protect IT assets
- Reduce security costs
- Enable compliance
- Around-the-clock protection
- Layered security – (50/30/20 Rule)

• Classification: //Dell SecureWorks/Confidential - Limited External Distribution:

Dell SecureWorks

Counter Threat Unit Research Team

- Elite cyber intelligence talent focuses on threat actors, tradecraft and countermeasures

Counter Threat Platform

- Next generation technology applies intelligence to protect thousands of customers worldwide

Certified Security and Compliance Experts

- 1,000+ security and compliance professionals deliver award-winning services and customer satisfaction

Global Security Operations Centers

- 7 resilient, high-security facilities provide vendor-neutral, in-region service delivery 24x7x365

We help **thousands** of organizations **protect against cyber threats, simplify regulatory compliance** and **embrace innovation securely**.

• Classification: //De

SecureWorks

Questions?

Jeff Multz, Dell SecureWorks
Director, North America Medium Business Sales