Symantec™

How Protected Is Your Enterprise?

Next Gen thinking and technology to help strengthen and protect your critical business systems and data

Greg Belanger, CISSP

Symantec (Canada) Corporation - Security Practice

The Challenge of Securing the Data Centre

As we see more:

- Higher Density via Virtualisation
- Interconnection between Systems
- Hosted applications
- Data sharing
- Use of the Cloud

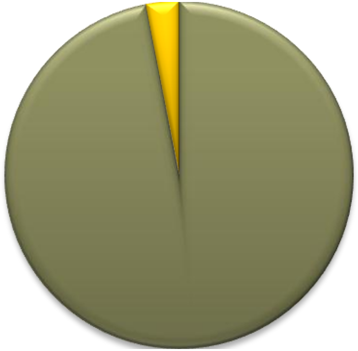
The criticality of the Data Centre increases

Servers Are The Primary Target

2012 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

97%

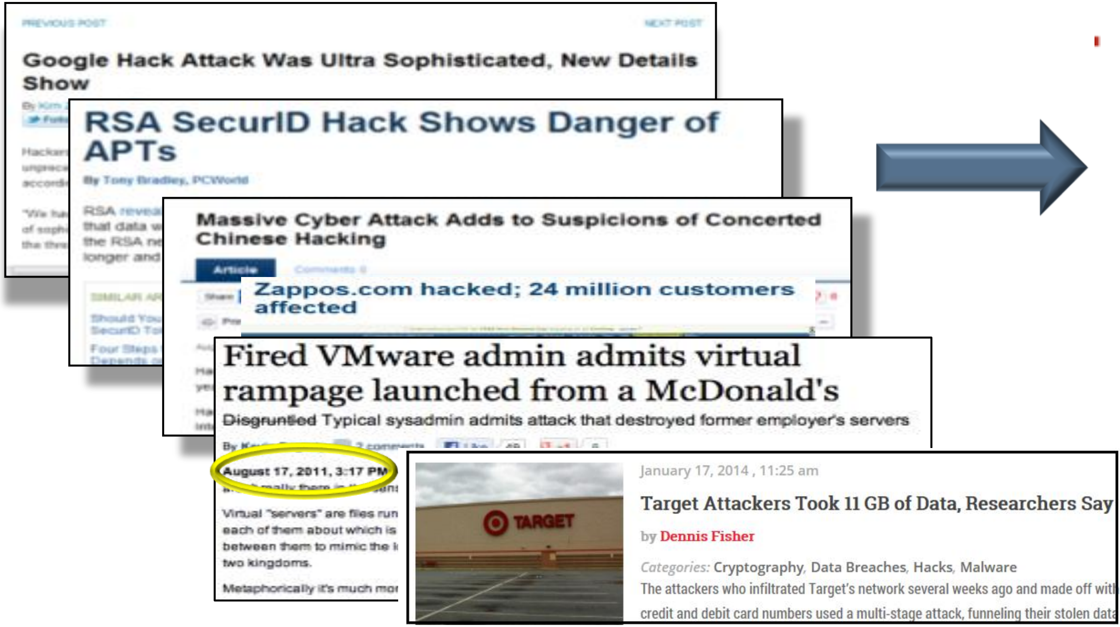


of stolen data is from servers

" …. More often endpoints / user devices simply provide an initial "foothold" into the organization, from which the intruder stages the rest of their attack."

Hackers Target Servers

Breaches



PREVIOUS POST

NEXT POST

Google Hack Attack Was Ultra Sophisticated, New Details Show

RSA SecurID Hack Shows Danger of APTs

By Tony Bradley, PCWorld

Massive Cyber Attack Adds to Suspicions of Concerted Chinese Hacking

Article

Zappos.com hacked; 24 million customers affected

Fired VMware admin admits virtual rampage launched from a McDonald's

Disgruntled Typical sysadmin admits attack that destroyed former employer's servers

August 17, 2011, 3:17 PM

Virtual "servers" are files run each of them about which is between them to mimic the i two kingdoms.

Metaphorically it's much mor

January 17, 2014 , 11:25 am

Target Attackers Took 11 GB of Data, Researchers Say

by Dennis Fisher

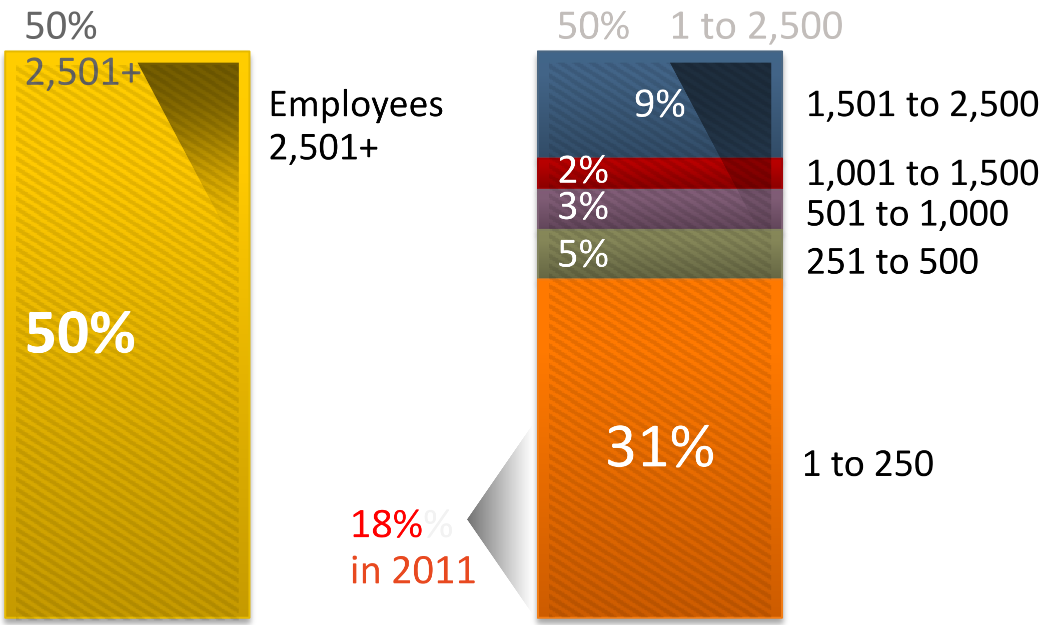
Categories: Cryptography, Data Breaches, Hacks, Malware

The attackers who infiltrated Target's network several weeks ago and made off wit credit and debit card numbers used a multi-stage attack, funneling their stolen data

67% of Breaches occur on servers

97% of Records stolen were on servers

The Changing Target Of Attacks: Not Just Large DCs

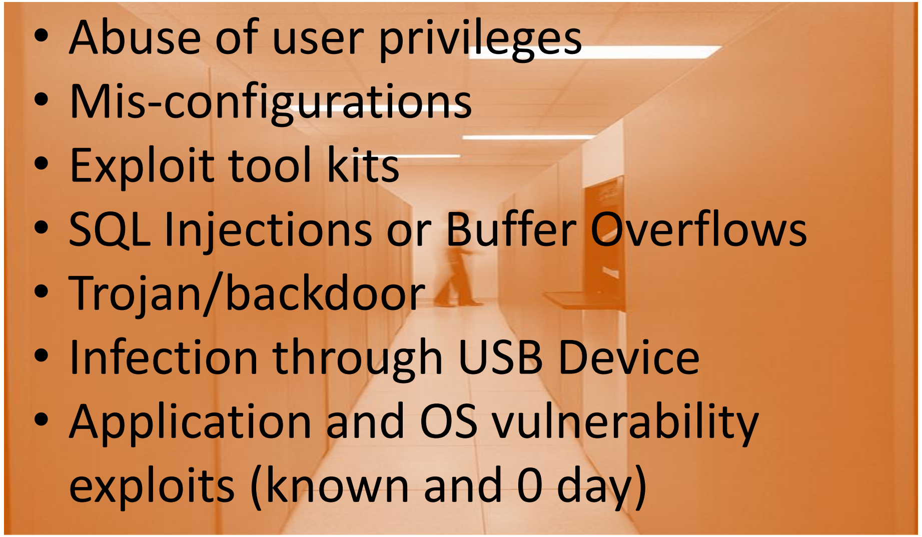


Source:

Symantec Internet Security Threat Report vol. 18

Servers Are Different To Laptops!

- Mail-based – Spam/phishing/social engineering
- Browser and app based – known and zero day vulnerabilities
- Peer to peer file sharing

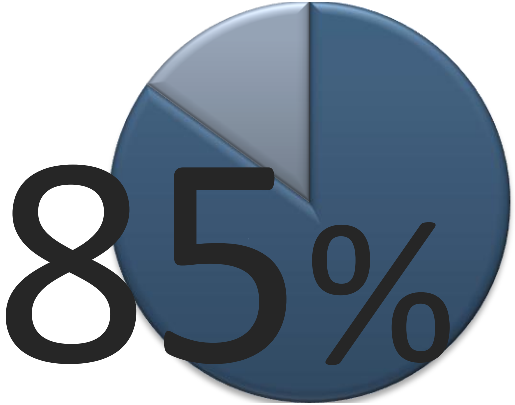


- Abuse of user privileges
- Mis-configurations
- Exploit tool kits
- SQL Injections or Buffer Overflows
- Trojan/backdoor
- Infection through USB Device
- Application and OS vulnerability exploits (known and 0 day)

Key and Important Challenges in Today's Datacentre

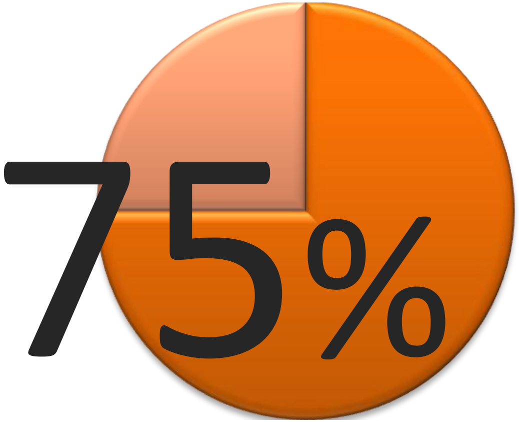
- Virtualisation
- Securing Legacy Platforms
- The Shifting Gateway
- Managing Compliance
- Securing Information, not just Systems

Challenge: The Data Center is Being Virtualised



85%

planning to adopt x86 virtualisation

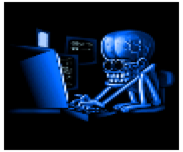


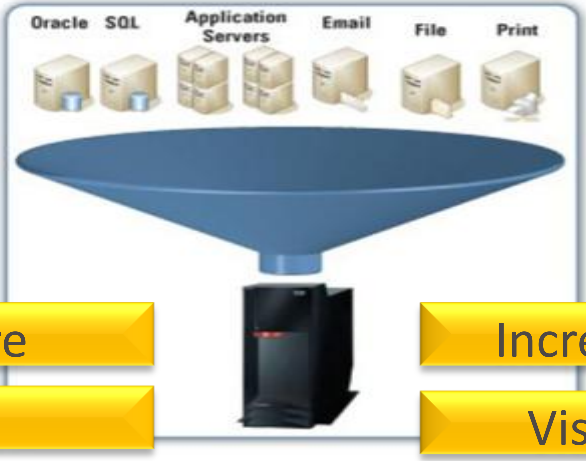
75%

of x86 servers will be virtual in 2 years

Source: Forrester: CISO's Guide To Virtualization Security

The Challenges of Virtualisation Security

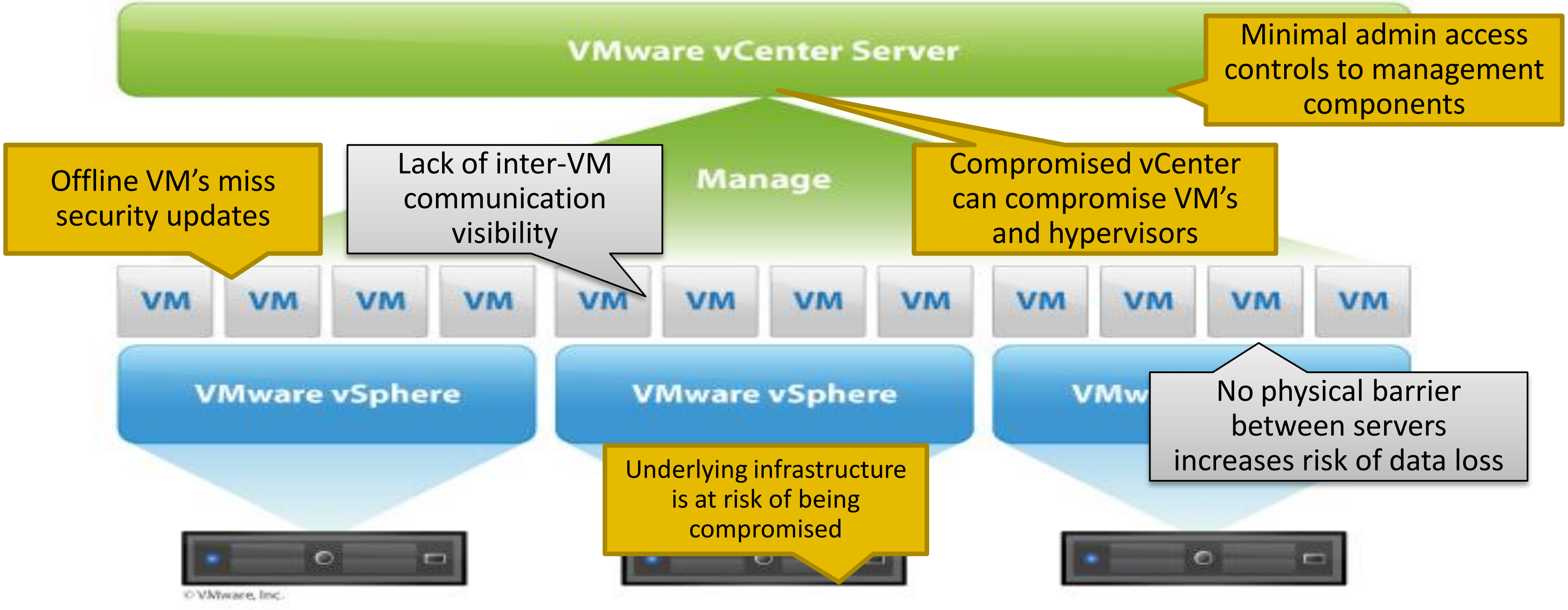




- Ethereal Infrastructure
- Targeted Malware
- Virtual Sprawl
- Misconfiguations
- System Tracking

- Increase Compliance Needs
- Visibility and Monitoring
- Rogue\Non-Compliant Systems
- Overlapping Responsibilities
- Access Control

Protecting Virtual Infrastructure: New Areas Of Risk



Minimal admin access controls to management components

Offline VM's miss security updates

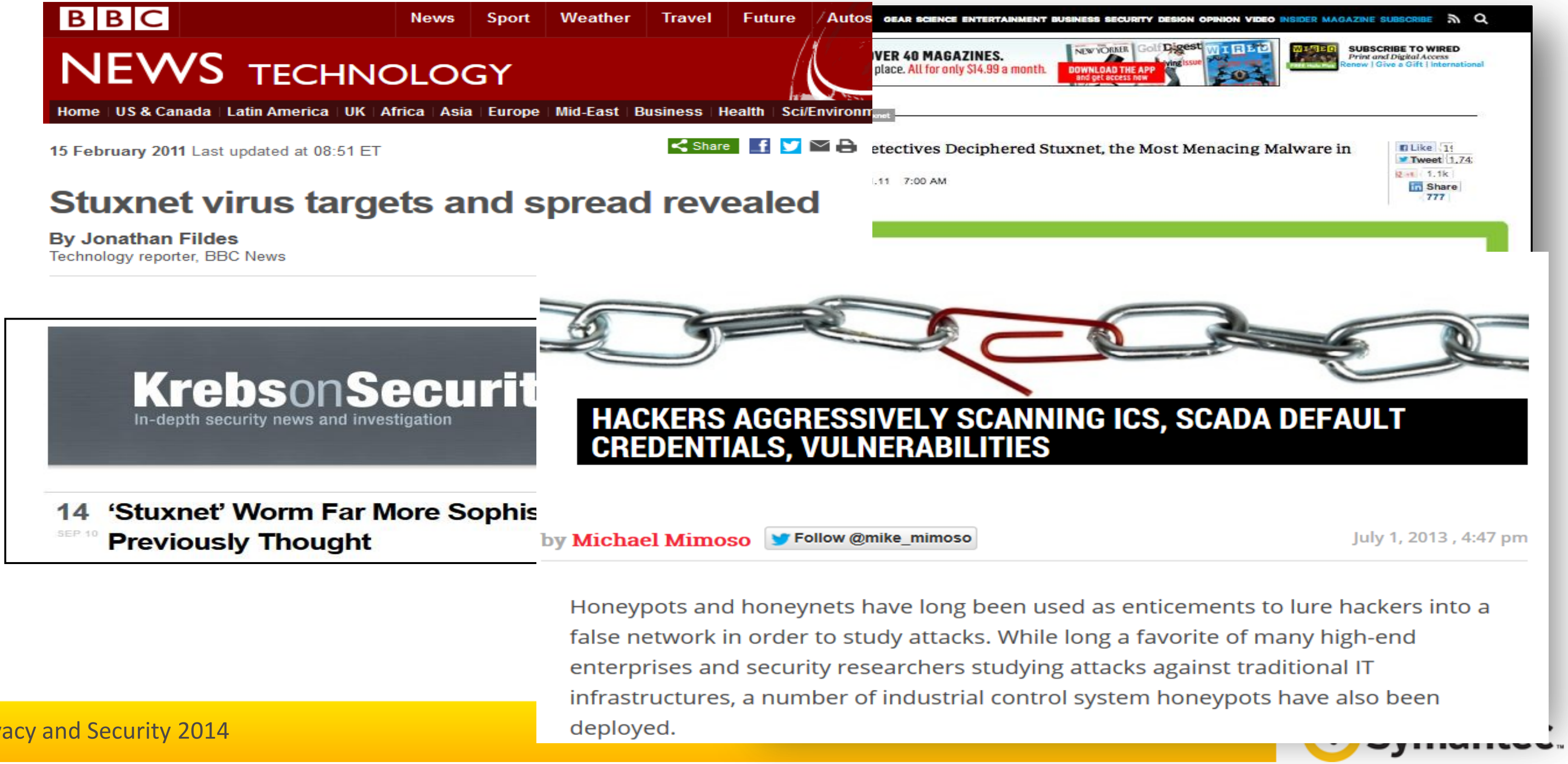
Lack of inter-VM communication visibility

Compromised vCenter can compromise VM's and hypervisors

No physical barrier between servers increases risk of data loss

Underlying infrastructure is at risk of being compromised

Beyond the “Traditional” Datacentre: Industrial Systems



BBC
News | Sport | Weather | Travel | Future | Autos
NEWS TECHNOLOGY
Home | US & Canada | Latin America | UK | Africa | Asia | Europe | Mid-East | Business | Health | Sci/Environm
Share

15 February 2011 Last updated at 08:51 ET

Stuxnet virus targets and spread revealed

By Jonathan Fildes
Technology reporter, BBC News

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO INSIDER MAGAZINE SUBSCRIBE
VER 40 MAGAZINES.
place. All for only $14.99 a month.
DOWNLOAD THE APP
SUBSCRIBE TO WIRED
Print and Digital Access
Renew | Give a Gift | International
Like
Tweet
Share
777

etectives Deciphered Stuxnet, the Most Menacing Malware in

.11 7:00 AM

KrebsonSecurit
In-depth security news and investigation

14 SEP 10 ‘Stuxnet’ Worm Far More Sophis Previously Thought

HACKERS AGGRESSIVELY SCANNING ICS, SCADA DEFAULT CREDENTIALS, VULNERABILITIES

by Michael Mimoso July 1, 2013 , 4:47 pm

Honeypots and honeynets have long been used as enticements to lure hackers into a false network in order to study attacks. While long a favorite of many high-end enterprises and security researchers studying attacks against traditional IT infrastructures, a number of industrial control system honeypots have also been deployed.

Challenge: The Gateway and Identity

- The "Front Door" is becoming Harder to Police!
- Bad Guys:
  - SPAM accounts for more than 2/3 of all email
  - Malicious Websites have increased four fold
  - Complexity of attacks have increased
- Good Guys
  - With more mobile users and platforms, how can I assure identity?

Challenge: Managing Compliance and Security

Looking at Webservers as a Microcosm of the state of Security Management

53%

of legitimate websites have unpatched vulnerabilities

61%

of web sites serving malware are legitimate sites

25%

have critical vulnerabilities unpatched

Challenge: Securing Information, not just Equipment

50%

email business documents using personal accounts

37%

use file-sharing apps – like Dropbox – without permission

41%

download intellectual property to personal mobile devices

Symantec in the Datacentre

- Jobs that need to be done:
  - Secure the Servers, including the Virtual ones
  - Protect the Gateway
  - Strengthen Identity
  - Secure the Information
  - Keep it that way!

Job: Securing Servers in the Data Centre

Need a server specific approach:

Symantec Data Center Security Advanced Edition

(Formerly known as Critical System Protection)

Principle of Least Privilege

“The principle of least privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.”

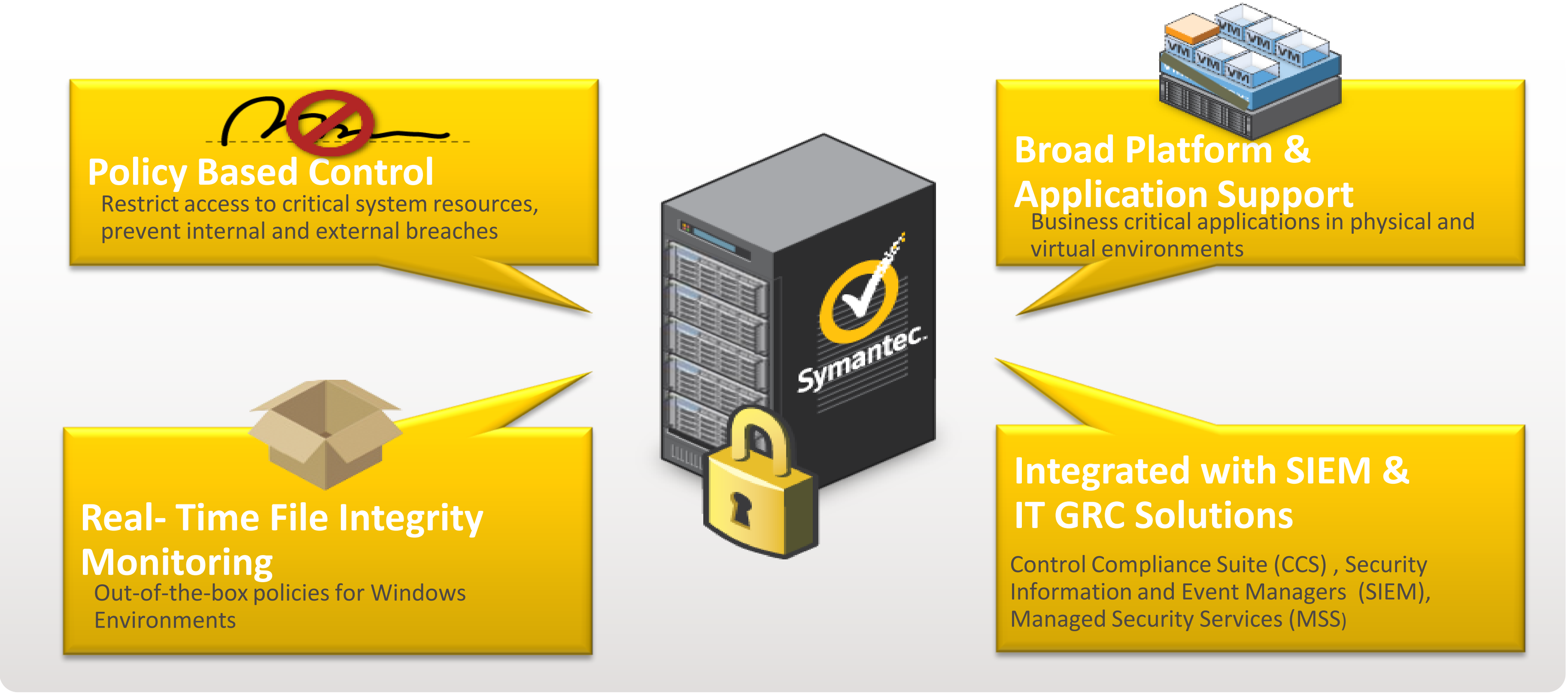
Securing Servers with SDCS

- Allows only approved process to execute on

  servers *without the use of signatures*.

- Policy-based protection to detect and protect against external malware, penetration-oriented threats and abuse of user privileges.
  - Monitors activity and change
  - De-escalates user privileges
  - Blocks active threats
  - Latent threats are neutralized and left on filesystem

How DCS Protects the Data Centre



Policy Based Control

Restrict access to critical system resources, prevent internal and external breaches

Broad Platform & Application Support

Business critical applications in physical and virtual environments

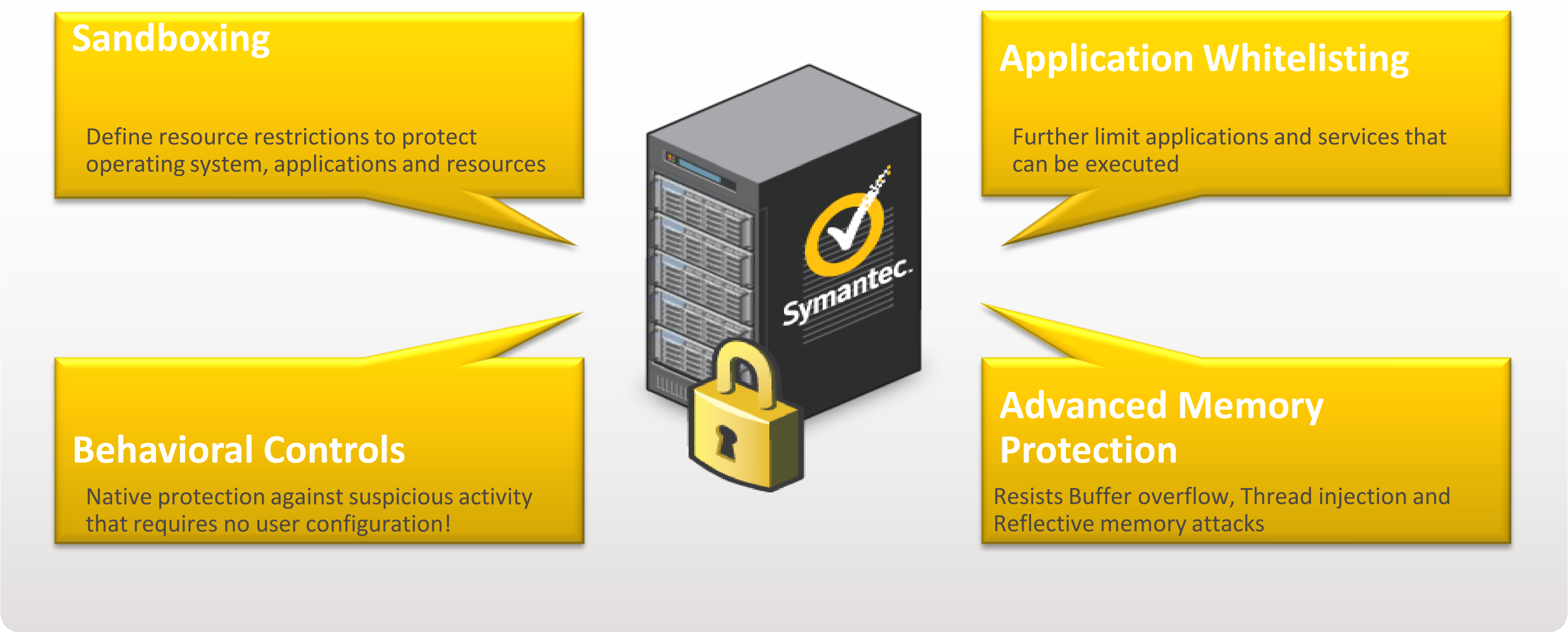
Real- Time File Integrity Monitoring

Out-of-the-box policies for Windows Environments

Integrated with SIEM & IT GRC Solutions

Control Compliance Suite (CCS) , Security Information and Event Managers (SIEM), Managed Security Services (MSS)

Multiple Technology Layers



Sandboxing

Define resource restrictions to protect operating system, applications and resources

Application Whitelisting

Further limit applications and services that can be executed

Behavioral Controls

Native protection against suspicious activity that requires no user configuration!

Advanced Memory Protection

Resists Buffer overflow, Thread injection and Reflective memory attacks

Symantec DCS: Protecting Virtualisation

Comprehensive Protection for VSphere

VMware Management Server

- Enforce Policies that adhere to VMware’s hardening guidelines
- Real-time monitoring and intrusion detection across vCenter

VMware Hypervisor Protection

- Monitor and protect VMware ESXi hypervisors

VMware Guest Protection

- Protect guests with policy-based controls
- Limiting VM Communication
- Hardening Applications
- Hardening Operating Systems
- Agentless Protection

Example of Protecting Systems

- Capture The Flag Challenge: Black Hat Conference 2011, 2012 and 2013.
- **Challenge:**
  - ‘Flag’ hidden on an un-patched **XP** workstation
  - Server protected with CSP out-of-the box windows strict prevention policy
  - Pen-testers from DoD, NSA, DISA, Anonymous asked to “Capture the flag”
- **Attacks Techniques used:**
  - Buffer overflow and thread injection

Example of Protecting Systems

- Capture The Flag Challenge: Black Hat Conference 2011, 2012 and 2013!

- **Outcome:**
  - No one was able to capture the flag!
  - Last hacker wanted physical access to the system ☺
  - Nexpose found 10+ exploited vulnerabilities

Disclaimer: As a security vendor, Symantec recognises that no solution will ever provide 100% protection, and we would never make that claim for Data Center Security. However, we believe that this exercise has demonstrated the capabilities of this solution to help customers lock down, protect and monitor their critical systems to a very secure level. Effective security not only involves technology, but a well-defined set of policies and procedures to ensure any risks are limited and mitigated.

Protect The Gateway

- Web and Email Protection
  - Deployed via on-premise software or via the Cloud
- Use Anti-Virus, heuristics and **up-to-the-second Intelligence** to filter traffic
- Ability to enforce policies on acceptable content
- Cloud-deployed offerings provide SLAs on capture rates and 100% availability

How Symantec can Authenticate Users

Tokens

Device Identity

Norton by Symantec

intel

Device Reputation

Norton by Symantec

User Behaviour

Symantec Security: Protecting the Information, Not Just Equipment

Set Policy

Use templates to develop and set protection policy

Discover

Find Sensitive Data on the Network via Data Insight

Monitor

Monitor Endpoints AND Network

Inspect Data Being sent

Protect

Block, remove or Encrypt

Notify and Coach

Manage

Report and Remediate

Maintain Protection and Control

Symantec Control and Compliance Suite (CCS)

- A suite of modules to identify, present and manage risk across the organisation – from systems and devices to people and processes.

Symantec Managed Security Services

- A Security Operations Centre as a service to provide 24x7 monitoring, assessment and alerts across any or all of your security perimeter and endpoints.

In Summary

- The Data Centre IS being targeted by malicious parties (Risk)
- Security in the Data Centre is more than simply Antivirus and Firewalls
- With virtualisation, expansion of storage, the interconnection of systems and the increased management requirements, securing the Data Centre is more difficult than ever
- Symantec is your partner in securing your Data Centre

Additional Assistance and Information

- ***Symantec DLP Risk Assessments*** – Identify at Risk Data
- ***Symantec Health Checks*** – Endpoint, Messaging, Web and other Symantec Security Solutions
- ***Symantec Security Program Review*** – “outside” view of your Organisational security
- ***Whitepapers and Information Sites:***
  - ➢ http://go.symantec.com/apt - Advanced Persistent Threats VS Targeted Attacks
  - ➢ www.threatexpert.com – Advanced Automated Threat Analysis
  - ➢ http://www.symantec.com/security_response/publications/threatreport.jsp - Internet Security Threat Report

Please drop by our booth!

Thank you!

Greg Belanger

Greg_belanger@symantec.com

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.