- the new dynamic landscape -

Cyber-warfare

Hacktivism
Advanced Persistent Threat

Further things to understand about “the APT”

• Compromised Game Networks

• Lulzec

• Anonymous/YamaTough

• WikiLeaks
- the new dynamic landscape -

Cyberwarfare

Hacktivism

Polymorphic Malware Saturation

Digital Natives
- the new dynamic landscape -

**SOCIAL ENGINEERING**

The clever manipulation of the natural human tendency to trust.
- the new dynamic landscape -
Preparing for Mandatory 2012 U.S. Benefits Open Enrollment

Employee Resources

Dear U.S. Employee:

U.S. Benefits Open Enrollment, which will be held October 31 through November 18, 2011, is the one time of the year that you can change your benefits for the 2012 calendar year. With health care costs continuing to rise, it is more important than ever to be a proactive health care consumer. I encourage everyone to become more informed about the benefits that are available by visiting www.symantecbenefits.com.

Our Total Rewards package — Symantec’s investment in our employees — includes competitive salaries, benefits, work-life...
- the new dynamic landscape -

Preparing for Mandatory 2012 U.S. Benefits Open Enrollment

Employee Resources

Dear U.S. Employee:

U.S. Benefits Open Enrollment is the time of year that you can change your benefits for the upcoming year. It is more important than ever to be as proactive as possible in this health care costs continuing to rise.

This year, you can choose from a variety of plans, including:

- Medical
- Dental
- Vision
- Life Insurance
- Disability

The Open Enrollment period runs from November 1 through November 18, 2011.

To learn more about the benefits that are available, please visit our website at www.symantecbenefits.com.

Our Total Rewards package includes competitive salaries, benefits, work-life opportunities, and professional development programs to help you achieve your career goals.

Thank you for your continued contributions to Symantec. We look forward to supporting you in the new year.

Symantec

http://www.you_are_powned.com

nice doing business with you

Ctrl+Click to follow link
Dear U.S. Employee:

U.S. Benefits Open Enrollment is the time to change your benefits for the coming year. Proactive health care costs are continuing to rise, it is more important than ever to be as informed as possible about the benefits that are available by visiting the following link:

http://www.you_are_powned.com/nice_doing_business_with_you

Ctrl+Click to follow link

www.symantecbenefits.com

Our Total Rewards package – Symantec’s investment in our employees – includes competitive salaries, benefits, work-life benefits.

Thanks,

[Signature]
Symantec Global Intelligence Network

Global Scope and Scale

Largest Security Footprint Worldwide

Instant Detection

24x7x365 Collection & Correlation

<table>
<thead>
<tr>
<th>Attack Activity</th>
<th>Malware Intelligence</th>
<th>Vulnerabilities</th>
<th>Spam/Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>240,000 sensors</td>
<td>250M* client, server, gateways monitored</td>
<td>32,000+ vulnerabilities</td>
<td>2.5M decoy accounts</td>
</tr>
<tr>
<td>200+ countries &amp; territories</td>
<td>• Global coverage</td>
<td>• 11,000 vendors</td>
<td>• 8B+ email messages/day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 72,000 technologies</td>
<td>• 1B+ web requests/day</td>
</tr>
</tbody>
</table>

Preemptive Security Alerts

Information Protection Network

Threat Triggered Actions
Protect Identity

- Authenticate to: Cloud Applications Enterprise Infrastructure
- Validate Identities: Enterprise Trusted Partners
- Detect & Prevent Anomalies
- Single instance Identity provisioning and de-provisioning: Internal/External Public/Private Cloud, SaaS & beyond.
Protect Infrastructure

- Compliance within enterprise and public sector governance standards
- Mitigate risk relative to infrastructure exposure potential; policy based & technology enforced
- Secure and Manage: Endpoints
  - Data Center
  - Critical Operations
  - Mobile devices
  - Virtual environment
- Correlate and assess events across the environment
- Business Continuity and Disaster Recovery:
  - Storage & Archiving
- Premise agnostic:
  - Physical/legacy
  - Virtual
  - Private/Public Cloud
Protect Information

- Protect Information according to its sensitivity:
  Encryption, Data Leakage Prevention
  Control of Access based on Identity

- Information Lifecycle tracking; relative to Identity

- Business Continuity and Disaster Recovery:
  Storage & Archiving

- eDiscovery reach across the environment

- Understand, inventory, and control your sensitive information;
  anytime, anywhere, any device; with 100% Confidence
Symantec Public Sector Security Strategy

Global Intelligence

Protect Infrastructure

Protect Identity

Protect Information

Visibility, Security, Control, & Agility
Endpoint/End-user Security over time...

Protect Infrastructure

Back in the Day

Antivirus

Antispyware

Today's SEP 12.1
Protect Infrastructure

- Leverages anonymous telemetry data from 250M+ machines to construct a massive nexus of files, machines and domains
- Tracks nearly every binary in the world
  - 4 billion files, adding 37 million every week
  - 1 Petabyte of statistical data
  - Uses age, prevalence, source and other attributes to assign a reputation rating to files
- Can accurately identify and block threats even if just a single Symantec user encounters them

**Symantec Insight**

Proactive Protection from New & Targeted Threats

- **Bad Safety Rating**
  - File is **blocked**
- **No Safety Rating Yet**
  - IT can set block/allow **thresholds**
- **Good Safety Rating**
  - File is **whitelisted**
Unfortunately neither technique works well for the tens of millions of files with low prevalence. (but this is precisely where the majority of today’s malware falls)

No existing protection addresses the “long tail”

Blacklisting works well here.

For this long tail a new technique is needed.

Whitelisting works well here.
Symantec Named as a Leader in 2012 Gartner Magic Quadrant for Endpoint Protection Platforms


This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our 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.
Symantec Protection Suite Enterprise Edition

Endpoint Protection
- Symantec™ Endpoint Protection
- Symantec™ System Recovery Desktop Edition

Messaging Protection
- Symantec™ Mail Security for Microsoft® Exchange
- Symantec™ Mail Security for Domino
- Symantec™ Messaging Gateway powered by Brightmail™

Web Protection
- Symantec™ Web Gateway

Symantec Protection Center
- Symantec™ Protection Center
Summer 2010:
Symantec completed acquisitions of:

GuardianEdge Technologies
PGP Encryption
Verisign Security Business

Fall of 2010, Symantec created:
Information & Identity Protection Business Unit
(encompassing Vontu DLP, GE, PGP & Verisign)
Encryption ... as part of Defense in Depth.

Risk-based deployment:

- Whole Disk Encryption
- Removable Media Encryption
- Device Control & Encryption
- Mobile & Tablet Encryption

Protect Information

- Insight Reputation
- Network Access Control
- Host Integrity Checking
- Heuristic Detection
- Location Awareness
- Application Control
- Device Control
- SONAR
- Firewall
- IPS
- Antispyware
- Antivirus
Protect Information

Laptops, Desktops, Windows Servers
- Symantec Endpoint Encryption Full Disk Ed.

USB Devices Optical Media
- Symantec Endpoint Encryption Removable Storage Ed.

Device Control
- Symantec Endpoint Encryption Device Control

Mobile & Tablet
- Symantec Endpoint Encryption Mobile
### Protect Information

**Integrated Encryption**
- Coverage – integrated endpoint, email and file encryption
- Combined Strength – stronger protection with the combination of PGP and GuardianEdge technologies
- Platforms – expanding SEE Full Disk to Mac OS X

**Centralized Management**
- Policy – unified policy driving deployment of encryption across multiple risk points
- Intelligence – automated actions based on context
- Risk Based – improved reporting helps gives greater visibility into risk posture

**Continued Innovation**
- Performance – integrated use of Intel AES-NI instruction set boosts 40%
- Theft-Deterrence – support for Intel Anti-Theft technology
- Leverage – better protection using DLP and Encryption

SEE has the widest range of integration encryption applications
SEE allows organizations to simplify encryption management and reduce risk
SEE continued investment to deliver information protection for today’s environment
Protect Information

SEE Whole Disk Encryption
Remote Disable And Destroy

Intel Anti-Theft

Theft Deterrence
Remote Deactivation
Reactivation & Recovery
Available as Annual Subscription

SEE Whole Disk Encryption

Data Protection
Remote Key Destruction
Pre-Boot Lockout

PGP Universal Server
Protect Information

### All Systems

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>Name</th>
<th>Status</th>
<th>Policy Group</th>
<th>Last Date Connected</th>
<th>Passphrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tough_Pana</td>
<td>rddtest2</td>
<td>Stolen</td>
<td>RDD</td>
<td>09/15/2010 1:22:25 PM</td>
<td></td>
</tr>
<tr>
<td>PanCF-52b</td>
<td>rddtest7</td>
<td>Stolen, Decommissioned</td>
<td>RDD</td>
<td>09/14/2010 10:25:28 AM</td>
<td></td>
</tr>
<tr>
<td>DemoHP-2</td>
<td>rddtest8</td>
<td>AT Activated</td>
<td>RDD</td>
<td>09/15/2010 1:22:26 PM</td>
<td></td>
</tr>
<tr>
<td>DemoHP-1</td>
<td>rddtest9</td>
<td>AT Activated</td>
<td>RDD</td>
<td>09/14/2010 1:43:29 PM</td>
<td></td>
</tr>
</tbody>
</table>
Disabled Stolen Laptop At Pre-Boot

Laptop displays Stolen status

Recovery options available for restoration
Data Loss Prevention
... as part of Defense in Depth.

Three different “Missions”
- DISCOVER
- MONITOR
- PROTECT

Three different “Theatres”
- ENDPOINT
- NETWORK
- STORAGE

![Diagram](image-url)
Data Loss Prevention
... as part of Defense in Depth.

**DISCOVER**
- Broad scan coverage
- High performance
- Identify data owners
- Extensive remediation options

**MONITOR**
- Cover all exit points and user activities
- Understand content and context
- Work with other security products

**PROTECT**
- Educate users in real time
- Prevent confidential data loss
- Enforce policies anywhere

Management Platform
Symantec™ Data Loss Prevention Enforce Platform
Data Loss Prevention
... as part of Defense in Depth.

Management Platform
Symantec™ Data Loss Prevention Enforce Platform
Lifecycle Management
... as part of Defense in Depth.

You can’t secure...
...what you can’t manage.

Asset Management

Patch Management

User & System Provisioning
Information & Identity Assurance

... as part of Defense in Depth.

2 Factor Authentication

Digital Identity

CAC/PIV

Anomaly Detection
Compliance, FISMA, FDCC, & CNCI

... as part of Defense in Depth.

FDCC/FISMA
NIST/SCAP
GLBA, SOX
HIPAA
FERPA, CIPA

Continuous Monitoring
Situational Awareness
Trusted Internet Connection (TIC)
Global Intelligence

Protect Infrastructure

Protect Identity

Protect Information
Thank you very much!