Messaging security deployment options - which is really best for you?

Duncan Mills, Stuart Jones, Amanda Grady
1. The threat landscape
2. Why Symantec messaging security
3. Generic differences to consider when choosing a platform
4. Why there are functionality differences across platforms
5. Driving priorities to obtain feature parity where possible
Threat landscape continues to worsen

Malware Attacks Rising
Targeted Attacks Expand
Mobile Threats Expose All
Data Breaches Rising
The Changing face of spam and inbound threats

**The good**

Percentage of Email Identified As Spam, 2011

- JAN 2010
- DEC JAN 2011
- DEC 2011

**The bad**

Ratio of Malware In Email Traffic, 2011

Source: Symantec cloud

**The ugly**

- Botnets
- Targeted Email Attacks
- Phishing Attacks
- Social Network Tie-ins

Messaging Security Deployment Options
Symantec is the market leader in messaging security


Symantec 17%
Trend Micro 11%
Cisco 8%
Microsoft 7%
McAfee 5%
Google 4%
Sophos 3%
Barracuda 3%
Websense 1%
Proofpoint 3%
Other 38%

Worldwide Messaging Security SaaS Revenue by Vendor, 2011

Symantec 25%
Google 16%
Microsoft 13%
Proofpoint 3%
Mimecast 4%
McAfee 4%
Perimeter 5%
Trend Micro 4%
Others 26%

### Symantec Global Intelligence Network

**Turning intelligence into protection**

<table>
<thead>
<tr>
<th>Power of the Cloud</th>
<th>Advanced Malware Detection</th>
<th>Strongest Email Security</th>
<th>Strongest Web Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time analysis of spam and malware traffic in the cloud with Skeptic</td>
<td>Malware intelligence from &gt; 130M systems</td>
<td>&gt; 99.85% effectiveness</td>
<td>Insight protects against new, mutated, &amp; targeted malware</td>
</tr>
<tr>
<td>Drives enhanced heuristic and signatures</td>
<td>Heuristics examine file attributes and vulnerability exploit attempts</td>
<td>&lt; 1 in a million false positives</td>
<td>Insight is powered by 210M users, 3.1B files</td>
</tr>
<tr>
<td>Drives global intelligence across products</td>
<td>Blocks new and unknown threats</td>
<td>400 million IPs - known spam and safe senders</td>
<td>Botnet and infected client protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stop marketing email</td>
<td>Block connections to Malicious IPs &amp; URLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Machine learning &amp; URL intelligence prevent phishing</td>
<td></td>
</tr>
</tbody>
</table>

**Block connections to Malicious IPs & URLs**
Symantec Global Intelligence Network
Turning intelligence into protection

Virtual appliance growing strongly, SaaS and hardware keeping up


IDC nomenclature for on premises software
Many of the differences between cloud-based and on-premises messaging security platforms are generic and not vendor specific.
Map your business requirements to your messaging security deployment platform

<table>
<thead>
<tr>
<th>Areas of consideration when choosing a messaging security deployment platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility and total cost of ownership</td>
</tr>
<tr>
<td>Current and future IT environment</td>
</tr>
<tr>
<td>Security and regulatory requirements</td>
</tr>
<tr>
<td>Key functionality</td>
</tr>
</tbody>
</table>
Map your business requirements to your messaging security deployment platform

Flexibility and total cost of ownership

<table>
<thead>
<tr>
<th>Organisation Requirement</th>
<th>Hardware appliance</th>
<th>Virtual appliance</th>
<th>Cloud SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital or operational expenditure</td>
<td>Capex</td>
<td>Both</td>
<td>Opex</td>
</tr>
<tr>
<td>Predictable per-user costs</td>
<td></td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Easily scales to accommodate additional load</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Fast implementation</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Easy to maintain</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Free up staff to focus on core business activities</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Minimal additional cost of HA and DR</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
</tbody>
</table>

Messing Security Deployment Options
Map your business requirements to your messaging security deployment platform

IT environment

<table>
<thead>
<tr>
<th>Organisation Requirement</th>
<th>Hardware appliance</th>
<th>Virtual appliance</th>
<th>Cloud SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce organisation’s data centre costs</td>
<td>☐</td>
<td>☐</td>
<td>☀</td>
</tr>
<tr>
<td>Multiple Internet gateways</td>
<td>☐</td>
<td>☦</td>
<td>☀</td>
</tr>
<tr>
<td>Policy and audit log backup</td>
<td>☐</td>
<td>☦</td>
<td>☀</td>
</tr>
<tr>
<td>Increase ROI of existing virtual infrastructure</td>
<td>N/A</td>
<td>☦</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Map your business requirements to your messaging security deployment platform

Security and regulatory

<table>
<thead>
<tr>
<th>Organisation Requirement</th>
<th>Hardware appliance</th>
<th>Virtual appliance</th>
<th>Cloud SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quickly address all privacy concerns</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>All data must be stored in a specified country</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Guarantee the security posture of the platform</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Enforce DLP policy before data leaves the network</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Service level agreements</td>
<td>N/A</td>
<td>N/A</td>
<td>○</td>
</tr>
<tr>
<td>Provider has local legal jurisdiction</td>
<td>N/A</td>
<td>N/A</td>
<td>○</td>
</tr>
</tbody>
</table>
Products evolve to meet customer requirements
Broad messaging & web portfolio

SMTP, HTTP

Internet

SMTP

Web Gateway
Hardware or virtual

Messaging Gateway
Hardware or virtual

HTTP / HTTPS and all other ports and protocols

Data Loss Prevention

Content Encryption

PGP Universal Gateway Email

Mail Security for Groupware

Email AntiSpam .cloud
Email AntiVirus .cloud
Email Image Control .cloud
Email Content Control .cloud
Email Boundary Encryption .cloud
Policy Based Encryption .cloud
Web Security .cloud
Instant Messaging Security .cloud

Symantec Message Security Deployment Options
Map your business requirements to your messaging security deployment platform

Functionality

<table>
<thead>
<tr>
<th>.cloud email security</th>
<th>Symantec Messaging Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image control</td>
<td>Self service TLS encryption deployment</td>
</tr>
<tr>
<td>Email continuity</td>
<td>Integration with enterprise DLP</td>
</tr>
<tr>
<td>Inbound email queuing</td>
<td>On-premises DLP incident management</td>
</tr>
<tr>
<td>Content control using DLP</td>
<td>Rich LDAP integration (auth and routing)</td>
</tr>
<tr>
<td></td>
<td>IP V6 support</td>
</tr>
<tr>
<td></td>
<td>Sender authentication</td>
</tr>
<tr>
<td></td>
<td>Long term log retention</td>
</tr>
</tbody>
</table>
Development themes drive feature parity between .cloud and on-premises products

**Protection**
- Effective protection is the primary driver for messaging security
- Email is main entry for botnets, APTs and other threats
- Phishing rate = 1 in every 299 emails

**Control**
- Email primary vector for data loss
- 35% of data loss incidents traced back to email
- Only 10% of organizations address outbound threats from well-meaning or malicious insiders

**Management & Platform**
- Visibility and control of the operating environment, configuration and reporting
- Compatibility with hardware/software components, network protocols, external product integrations, etc.
Recent enhancements were driven by customer requirements and feature parity
Recent enhancements address customer requirements and drive feature parity

<table>
<thead>
<tr>
<th>Protection</th>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection and filtering of bulk email / marketing newsletters by group</td>
<td>Spam submissions via management console</td>
<td></td>
</tr>
<tr>
<td>Customer specific spam rules</td>
<td>Not a customer priority</td>
<td></td>
</tr>
<tr>
<td>Spam submissions feedback</td>
<td>Real-time link following for phishing protection</td>
<td></td>
</tr>
<tr>
<td>Future</td>
<td>Insight reputation data for file whitelisting</td>
<td></td>
</tr>
<tr>
<td>Future</td>
<td>Backend phishing improvements</td>
<td></td>
</tr>
</tbody>
</table>
Submissions feedback and customer-specific rules

- Three core concepts:
  - Streamline and drive customer submissions of missed spam or false positives to Symantec
  - Integrate submissions into custom rules to improve local effectiveness without impacting global accuracy
  - Provide end-to-end visibility into submissions and their impact
Back-end anti-phishing improvements
Universal link following (cloud)

Inbound email

Email scanning towers

Extract URLs

Link-following Infrastructure

Data store

Analyze URLs

Symantec GIN

http://online.lloysdtsb-bank.co.uk/customer.htm

Signature created by Symantec GIN

Messaging Security Deployment Options
Recent enhancements address customer requirements and drive feature parity

### Control

<table>
<thead>
<tr>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available already</td>
<td>Disclaimers by user group</td>
</tr>
<tr>
<td>Available already</td>
<td>Policy-based routing</td>
</tr>
<tr>
<td>Available already</td>
<td>Enhanced Content Control templates and new actions</td>
</tr>
<tr>
<td>Enterprise DLP integration</td>
<td>N/A</td>
</tr>
</tbody>
</table>
DLP integration

• Problem:
  – DLP administrator needs single view of incidents
  – Enforcement of separation of duties

• Incident management from Messaging Gateway
  – Rights based administration & the ability to track the lifecycle of quarantined incident

• Incident management from DLP console (Enforce)
  – Synchronized message status & incident correlation across DLP and SMG
  – Leverage email based remediation in Messaging Gateway
Recent enhancements address customer requirements and drive feature parity

<table>
<thead>
<tr>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Audit Log enhancements</td>
<td>Track &amp; Trace enhancements</td>
</tr>
<tr>
<td>N/A</td>
<td>Reduced latency/propagation for Track &amp; Trace and policy config</td>
</tr>
<tr>
<td>TLS certificate management</td>
<td>Future</td>
</tr>
<tr>
<td>Improved in-product software update</td>
<td>N/A</td>
</tr>
<tr>
<td>FIPS 140-2 validation and Common Criteria update</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Track & Trace enhancements

Advanced data in results

- SMTP response code
- SMTP start/finish time
- No of delivery attempts
- UI and CSV contains new data
- New “Log view”
- Details of all delivery attempts shown as new back end mta rolls out
Future priorities driven by customer requirements and feature parity

Disclaimer

Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.
Future development will address customer requirements and drive feature parity

<table>
<thead>
<tr>
<th>Protection</th>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Targeted attack prevention with attachment cleanser</td>
<td>Under consideration</td>
</tr>
<tr>
<td></td>
<td>Full .cloud link following feed</td>
<td>Available already</td>
</tr>
<tr>
<td></td>
<td>Skeptic integration</td>
<td>Available already</td>
</tr>
<tr>
<td></td>
<td>Available already</td>
<td>Sender authentication</td>
</tr>
</tbody>
</table>
Stop targeted attacks with new attachment cleanser

• Problem:
  – Spear phishing emails with malicious attachments
  – Advanced Persistent Threat (APT) entry
  – Zero-day attacks

• Symantec Solution:
  – Remove all potentially malicious content including
    • Macros
    • Scripts
    • Unrecognized file types
  – Deliver cleansed copy of attachment to recipient
Future development will address customer requirements and drive feature parity.

Control

<table>
<thead>
<tr>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available already</td>
<td>Data loss prevention .cloud</td>
</tr>
</tbody>
</table>
Email Security.cloud - Data Loss Prevention

- Multiple rules in a single policy
- Enhanced Boolean capabilities
- Thresholds
- Unique match count option
- Case sensitivity of keywords
- Custom regular expressions
Future development will address customer requirements and drive feature parity

### Management and platform

<table>
<thead>
<tr>
<th>Symantec Messaging Gateway</th>
<th>Email Security .cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid log search</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Outbound email support for Office 365 / Google Apps Mail</td>
</tr>
<tr>
<td>N/A</td>
<td>Reduce configuration propagation times</td>
</tr>
<tr>
<td>Available already</td>
<td>Self service domain provisioning</td>
</tr>
<tr>
<td>Available already</td>
<td>Self service TLS management</td>
</tr>
</tbody>
</table>
Hybrid log search

- Addressing customer requirements for joint deployments of Symantec Messaging Gateway and Symantec.cloud
  - SaaS-based inbound filtering and on-prem outbound filtering
  - Dual-layer bi-directional filtering
- Priority use case on single interface for searching through logs during an investigation
Things to consider when choosing the right deployment platform for email security

**TCO Flexibility**
- Opex or capex and budget constraints
- Resources to maintain and manage on-premise products
- Amount of change happening within your organisation

**Environment**
- Investment in virtualisation
- Number of Internet connections

**Security Regulatory**
- Regulatory compliance
- Importance of SLAs

**Functionality**
- Choice of form factor – map to your requirements
- Assess individual products to determine which meets your needs
Other sessions of interest

• ISB09 (114, tomorrow 9:00)
  – SONAR, Insight, Skeptic and GIN - The Symantec secret sauce

• ISB13/14 (This room, this afternoon)
  – Web security deployment options - which is really best for you?
  – Are You Getting the Most From Symantec Protection Suite?

• ISB11 (114, tomorrow 11:45)
  – Demo: integrating Symantec products to get the ultimate protection

• ISB07 (114, tomorrow 13:45)
  – The roadmap for Symantec infrastructure protection products
Thank you!