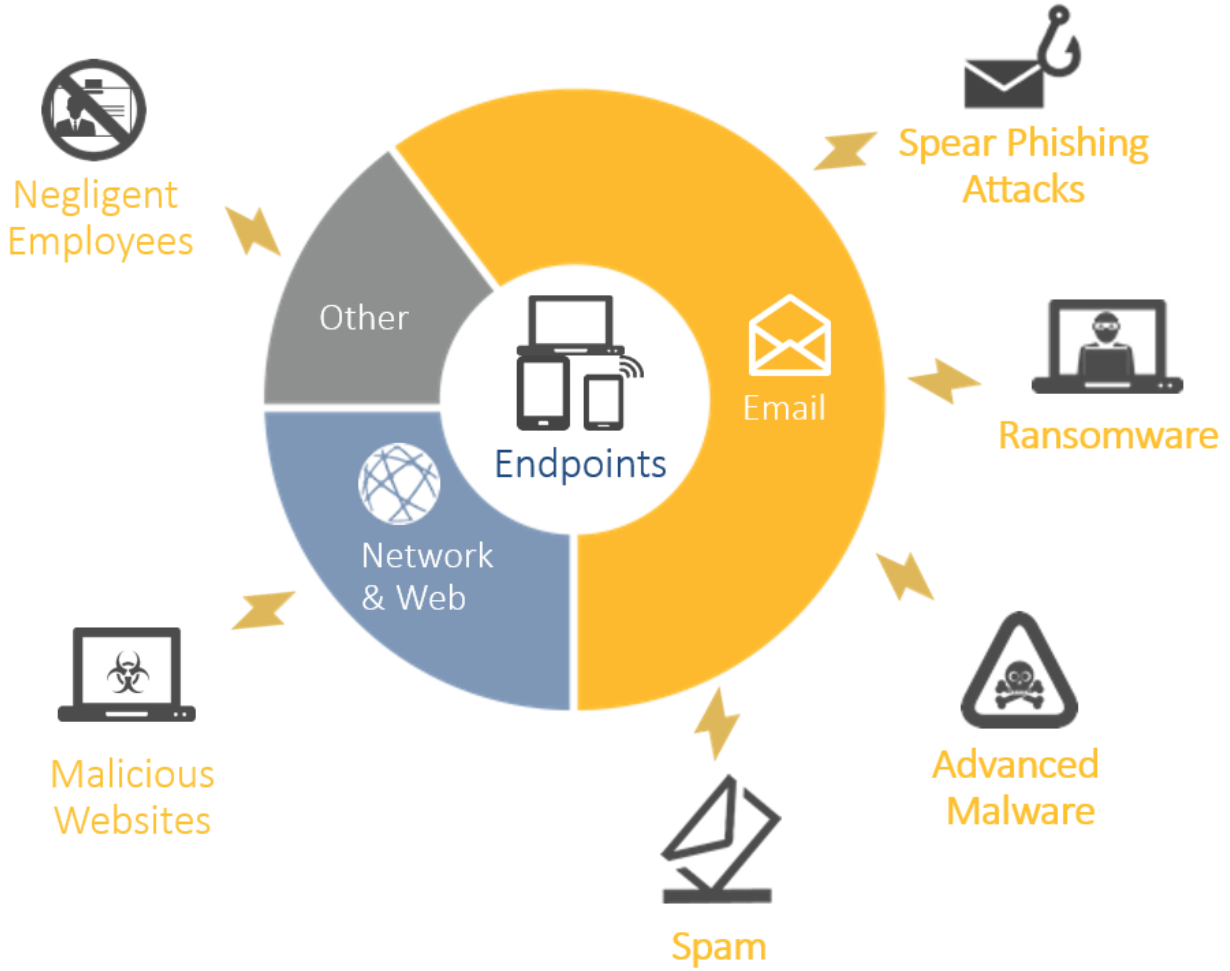
Symantec Messaging Gateway

Presenter
Hackim Farrell

Date
July 24th

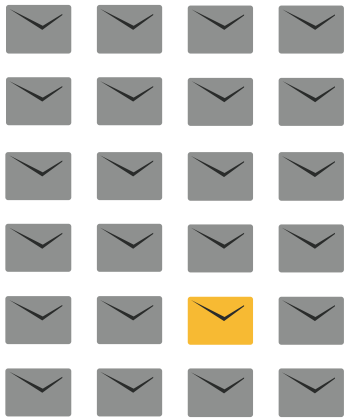
Email Continues To Be The Attack Vector Of Choice



Copyright © 2017 Symantec Corporation

Malicious Emails Hit the Highest Rate in Five Years

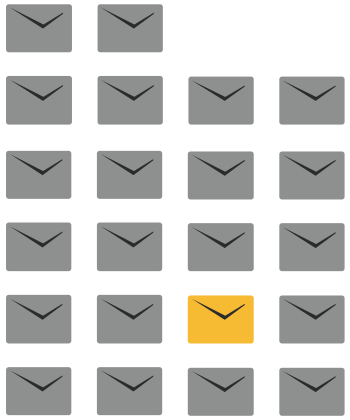
2014



1 out of

244

2015



1 out of

220

2016

1 out of

131

Copyright © 2017 Symantec Corporation

Email Attacks Are Becoming More Sophisticated

$5B

Lost to **Business Email Compromise** scams over last 3 years

55%

Increase in **spear phishing** attacks

61%

of organizations hit by a **ransomware** attack in 2016

Copyright © 2017 Symantec Corporation

Symantec Email Security Solutions

ON-PREMISES APPLIANCE

MULTI-TENANT CLOUD

Protect against spear phishing, ransomware, and BEC attacks

Quickly respond to targeted & advanced email attacks

Keep your emails secure and confidential

Copyright © 2017 Symantec Corporation

Messaging Gateway Solution Overview

MULTI-LAYER SPAM & MALWARE FILTERING

Block unwanted email & prevent delivery of email containing malicious links & attachments

TARGETED ATTACK PROTECTION

Strong protection against spear phishing , ransomware & BEC attacks

RICH THREAT INTELLIGENCE

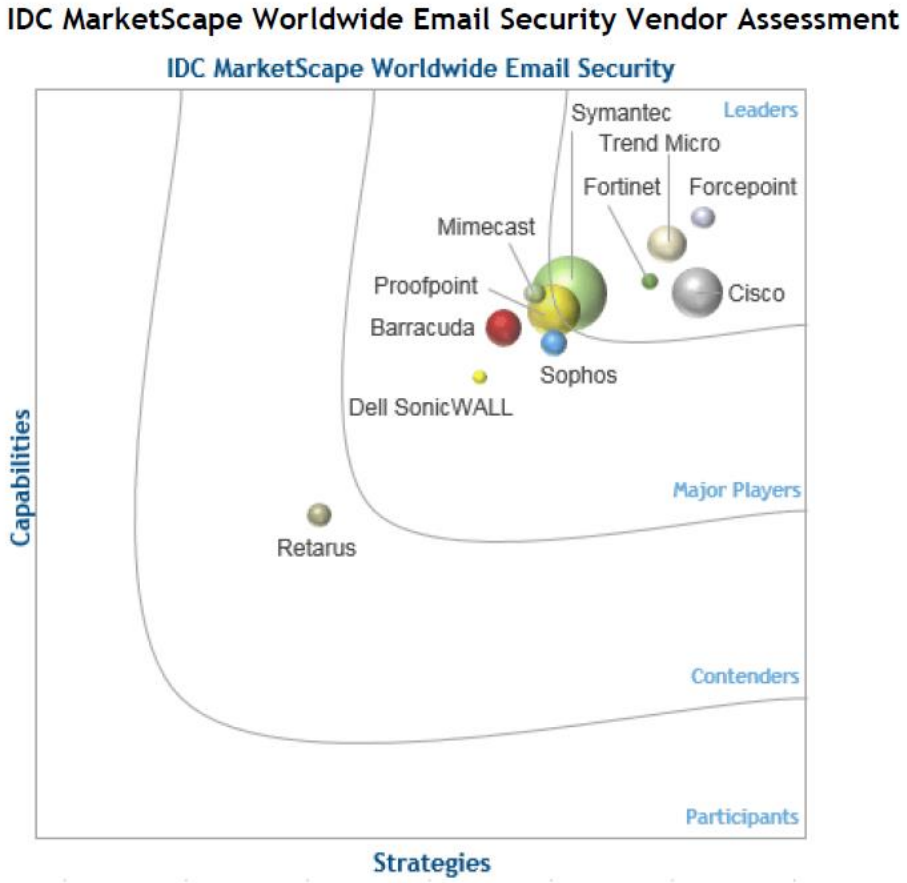
Provide detailed threat analysis & risk scoring to accelerate remediation

POLICY-BASED DATA PROTECTION & ENCRYPTION

Prevent leakage of sensitive company information

Copyright © 2017 Symantec Corporation

Named A Leader By IDC MarketScape



A **Leader** in the IDC MarketScape: Worldwide Email Security 2016 Vendor Assessment

"Symantec is the overall revenue leader in messaging security and in the software-as-a-service and software on-premises categories."

IDC MarketScape: Worldwide Email Security 2016 Vendor Assessment

Copyright © 2017 Symantec Corporation

Advanced Threat Protection & Visibility

I want to uncover & quickly respond to advanced threats

SYMANTEC MESSAGING GATEWAY

Protect Sensitive Data Shared Over Email

I want to prevent loss of sensitive data and keep emails confidential

Copyright © 2017 Symantec Corporation

Advanced Email Threat Protection And Visibility

Need

"Advanced threats including ransomware, spear-phishing & Business Email Compromise are getting through using basic email security tools."

Challenges

Traditional blocking tools failing to block advanced threats & need better visibility into targeted attacks for faster remediation

Product

- Messaging Gateway + Content & Malware Analysis

Capabilities

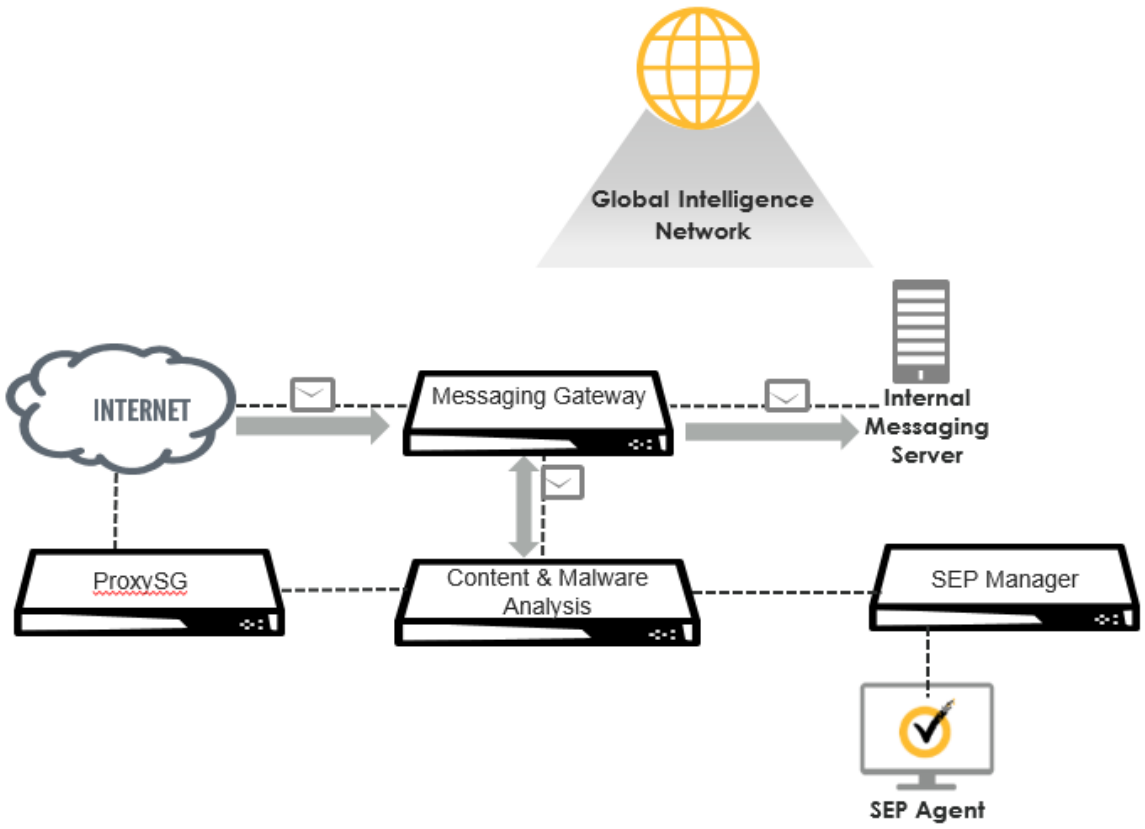
- Multi-layered technologies, Symantec GIN
- Cloud sandboxing, targeted & advanced attack visibility

Why Symantec

- Prevents stealthy targeted & advanced attacks
- Uncover threats with customizable sandbox
- Provides deep visibility into threat sources
- Tightly integrated with 3rd party SIEM

Copyright © 2017 Symantec Corporation

Advanced Threat Protection with Content & Malware Analysis



Blocks targeted attacks using advanced detection technologies - static, dynamic & behavior analysis

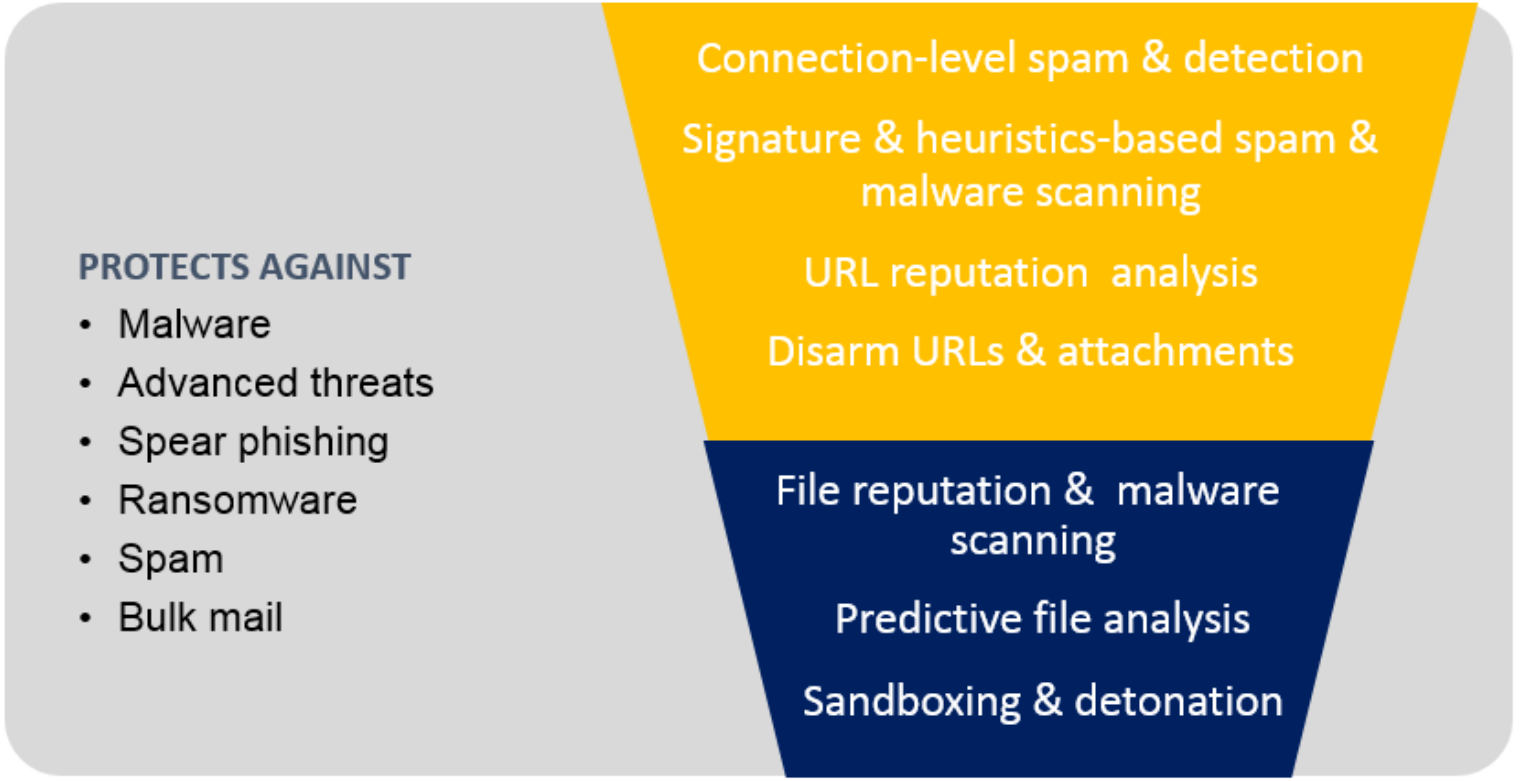
Provides rich threat intelligence including key malicious indicators, event timeline & threat risk score

Complete Cyber Defense Platform protects mail, web & endpoint channels

Rapid Remediation*:* Perform single-click remediation (blacklist, delete malware) of threats on endpoints

Copyright © 2017 Symantec Corporation

How the solution works

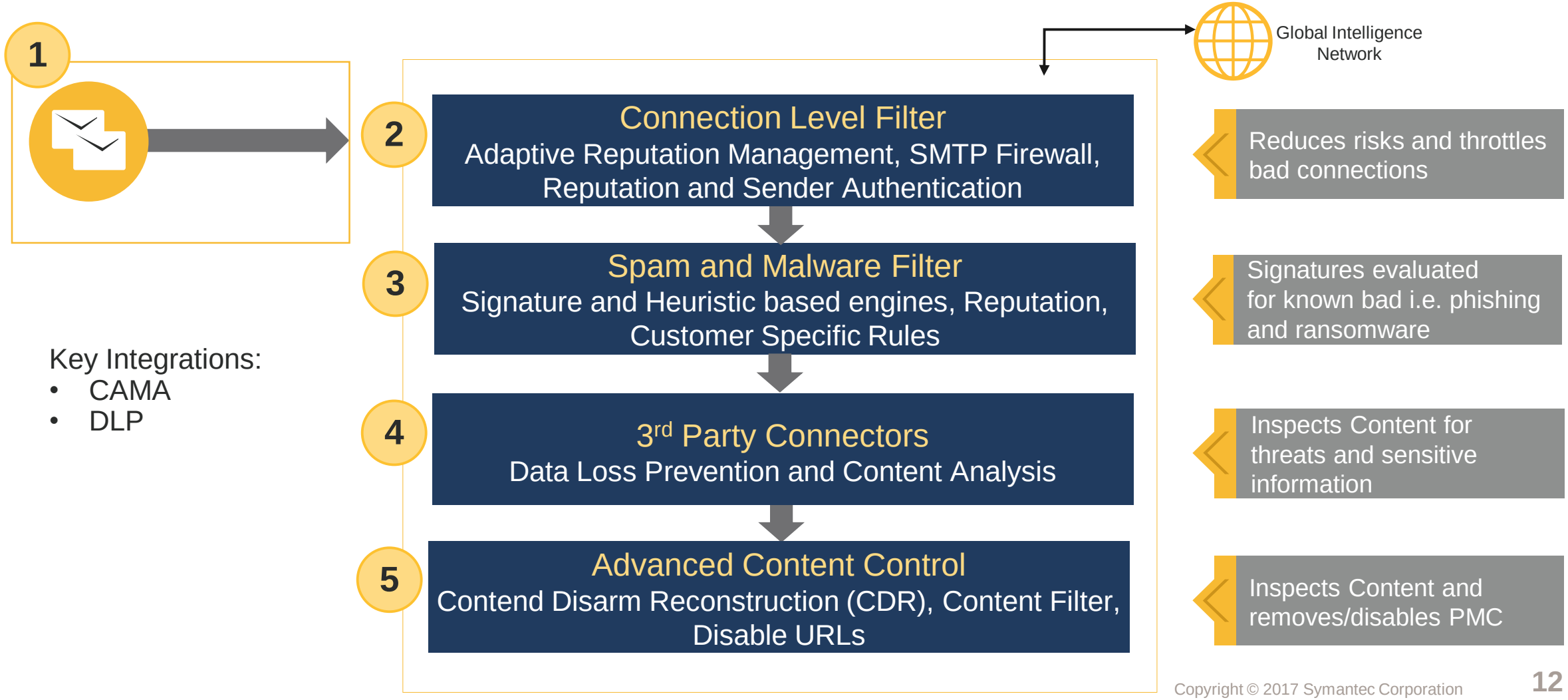


Symantec Messaging Gateway

Advanced Threat Protection (Content & Malware Analysis)

Copyright © 2017 Symantec Corporation

Messaging Gateway

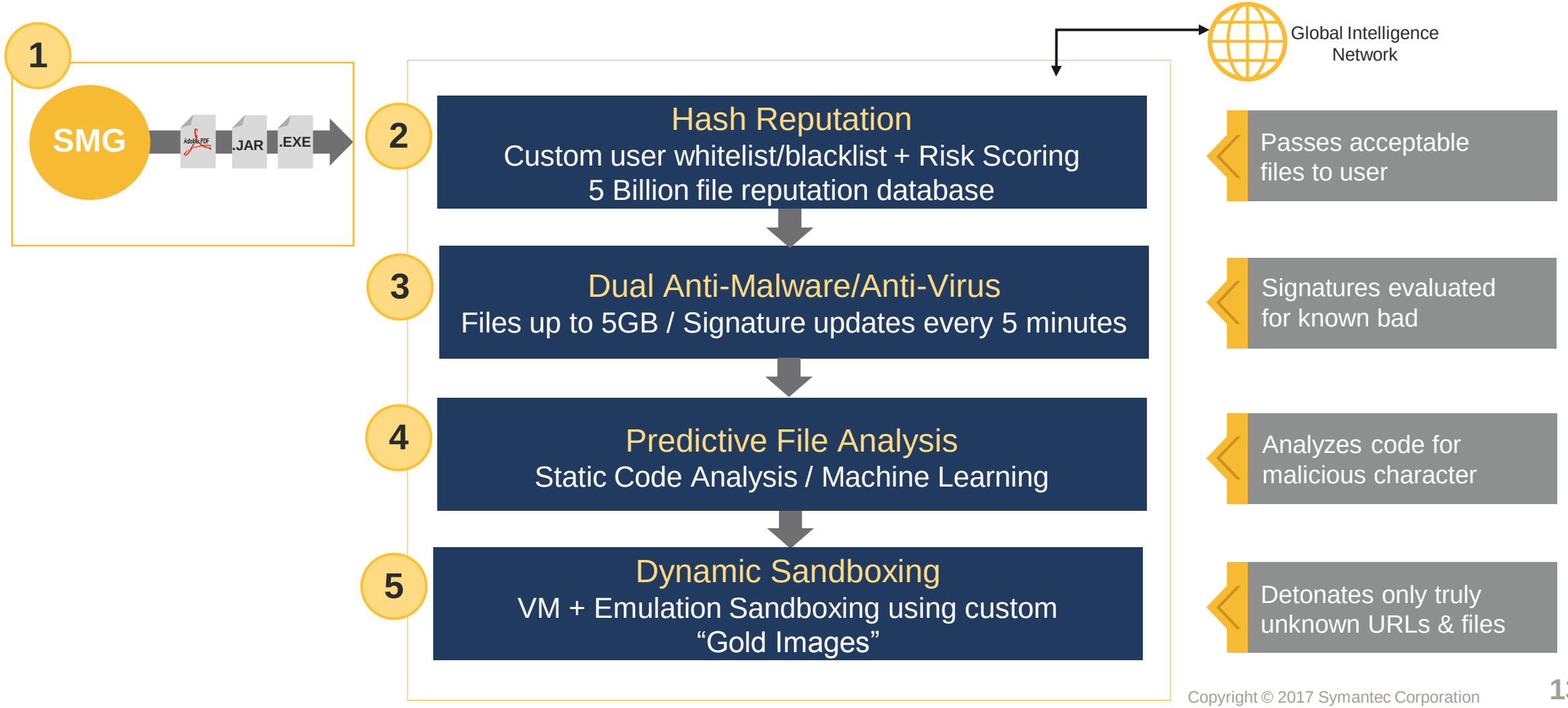


Key Integrations:

- CAMA
- DLP

Copyright © 2017 Symantec Corporation

Content And Malware Analysis



Copyright © 2017 Symantec Corporation

Addressing Targeted & Advanced Email Attacks Requires Rich Intelligence

Is This Targeted?

- Was this attack targeting specific users in my organization?
- If so, what type of targeted attack is this?
- Who's targeting me and where is it coming from?

Who's Targeted?

- Who in my organization was targeted?
- Was my network or endpoint security able to stop the attack?
- Were targeted users infected by the attack?

What's Used to Target?

- Were malicious file attachments used?
- Were malicious urls used? If so, was a payload downloaded?
- Can I block this attack on my endpoint or network?

Copyright © 2017 Symantec Corporation

Deep Visibility Into Targeted & Advanced Attacks

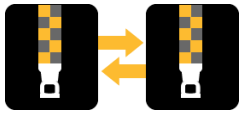
Rich Threat Intelligence

Malware Category

Detection Method

Attack Technology Used

Risk Scores


File Hashes

URL Information

Email Volume

Artifacts Analysis

Malicious Email Senders & Recipients

Correlation & Response

Export Intelligence

splunk>

APIs for 3rd party SIEM integration

Accelerate Threat Response

Benefits

- **Identify targeted attacks recipients**
- **Feed malicious URLs into web proxy**
- **Find patterns in threats**
- **Monitor email logs**

Copyright © 2017 Symantec Corporation

Protect Sensitive Data Shared Over Email

Need

"We have to prevent leakage of sensitive company data for business & compliance reasons."

Challenges

Relying on employees to prevent data leakage is not foolproof.

Product

- Messaging Gateway + Content Encryption
- Messaging Gateway + DLP + Content Encryption

Capabilities

- Provide DLP & policy-based encryption controls to block, quarantine, or encrypt sensitive emails.

Why Symantec

- Built-in content filtering & DLP controls
- Integration with Symantec DLP & Encryption provides email channel enforcement point & data security

Copyright © 2017 Symantec Corporation

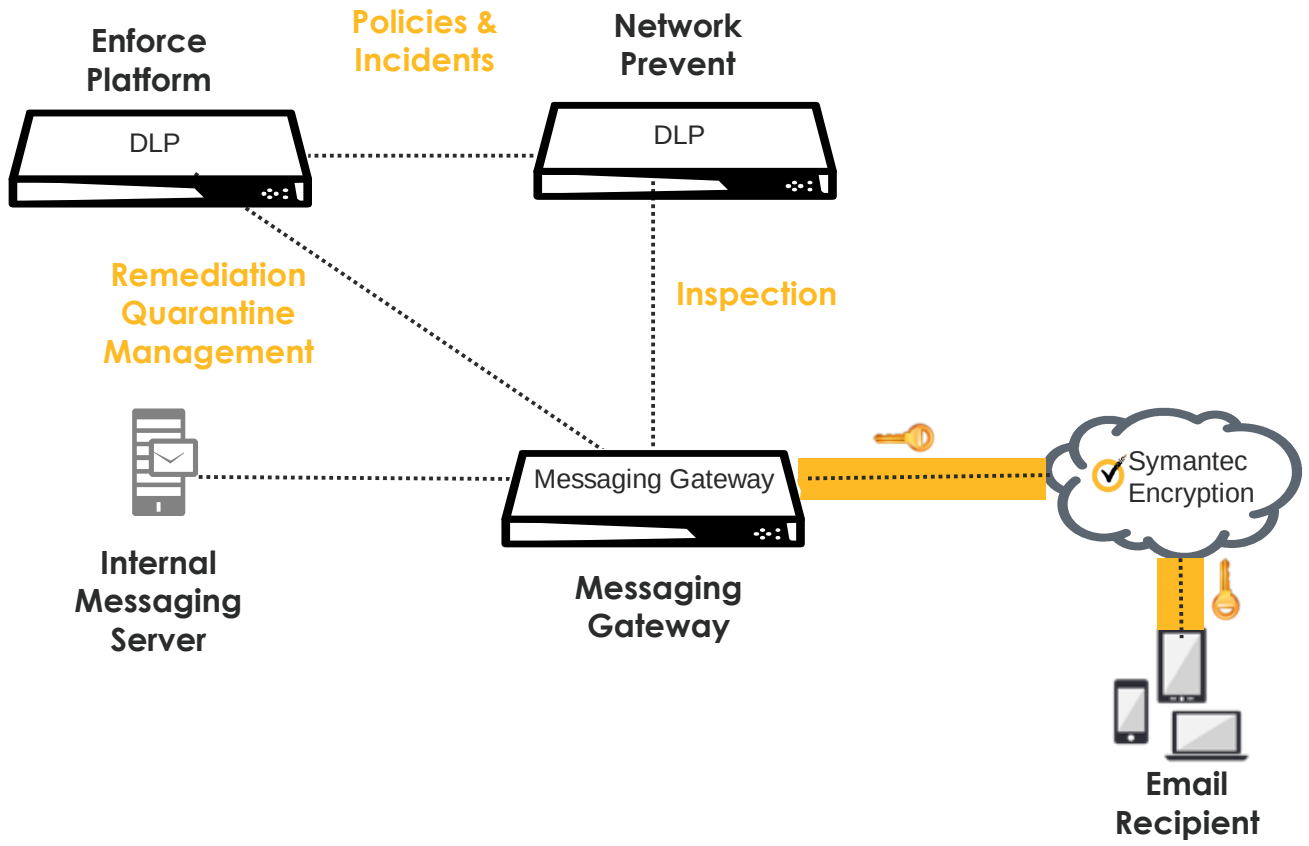
Protect Sensitive Data Shared Over Email

BUILT-IN DATA LOSS PREVENTION

Over 100 pre-built dictionaries, patterns, and policy templates	→	Protect PCI, HIPAA & sensitive business data
Workflow and remediation tools	→	Enforce business transactions & non-business related transactions
Violations & incident management	→	Visibility & control with audit reports & incident tracking

Copyright © 2017 Symantec Corporation

Symantec DLP & Encryption Integration



Monitoring & enforcement point for sensitive information shared over email

Policy-based data encryption from cloud service or on-premises appliance

Copyright © 2017 Symantec Corporation

Email Security Platform – Flexible Deployment

Virtual Appliance	• VMWare • Microsoft Hyper-V
Physical Appliance	• 8340 Appliance • 8380 Appliance
Hybrid Deployment	• Combination of Email Security.Cloud and Messaging Gateway

Copyright © 2017 Symantec Corporation

Key Takeaways

1. **A powerful and accurate email security solution**
   Stop new and sophisticated threats in their tracks using advanced multi-layered detection technologies such as machine learning and behavior analysis, and the world's largest GIN (Catches 99 percent of Spam with 1 in 1 million false positive)

2. **Provides in-depth threat analysis to reduce response time**
   Quickly respond to targeted and advanced threats with deep visibility and rich analysis of leading Indicators of Compromise

3. **Includes strong Data Protection Controls**
   Prevent data leakage and ensure compliance with regulations such as HIPAA, PCI-DSS, and ITAR with granular DLP and encryption controls

Copyright © 2017 Symantec Corporation

Thank You!

Presenter
Email
Phone

Copyright © 2017 Symantec Corporation