Symantec™

Email Security for the Cloud Generation

Davor Perat

Senior Technology Consultant

Evolving Email Threat Landscape

Symantec

Email is the #1

Delivery mechanism for malware

36%

Increase in **ransomware**

8,000

Businesses targeted each month by **BEC scams**

55%

Increase in **spear phishing** campaigns

30%

Users opened **phishing** emails

72%

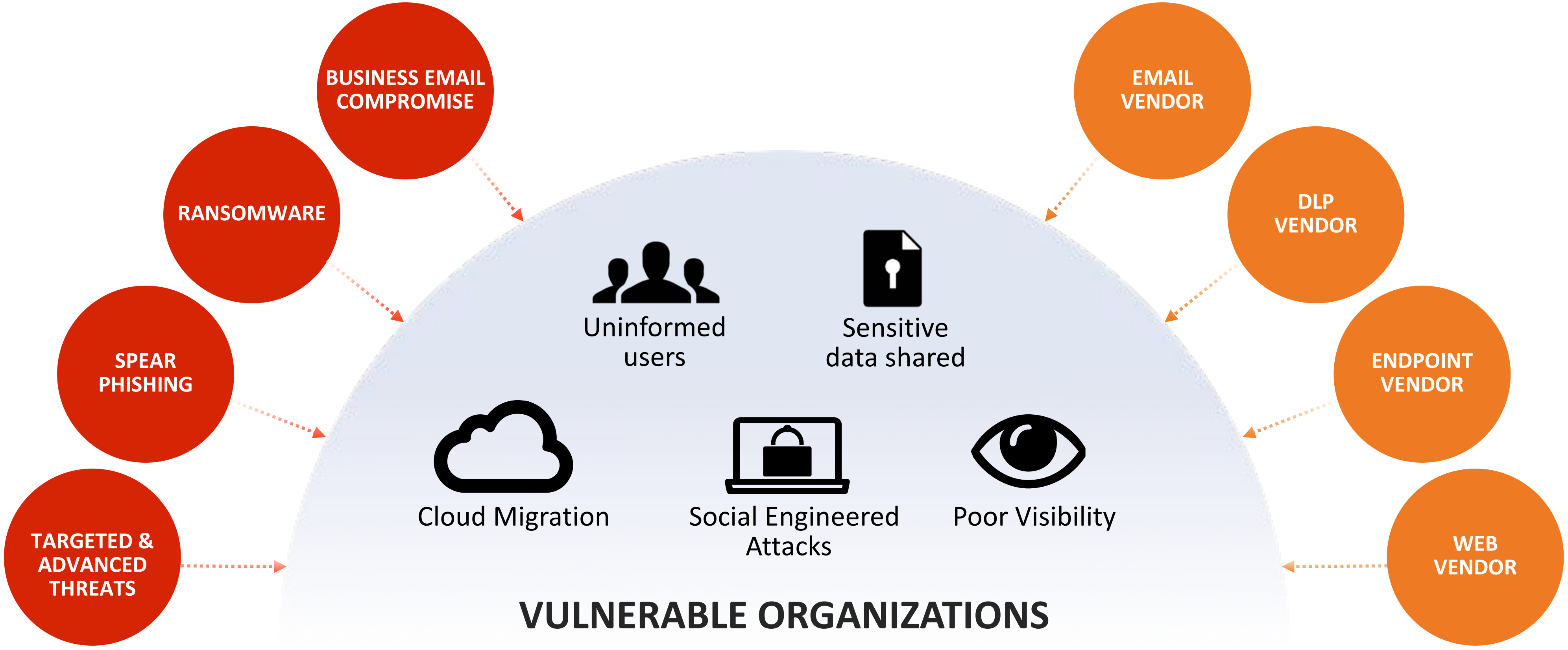
Incident responders use **security analytics** to speed detection & response

Source: ISTR Report 2017, Email ISTR Report 2017, ISTR Report 2016, Verizon DBIR 2016, 2016 SANS Incident Response Survey

Email Security Challenges / Chaos

SHORTAGE OF SECURITY PERSONNEL

EVOLVING THREAT LANDSCAPE



BUSINESS EMAIL COMPROMISE

RANSOMWARE

SPEAR PHISHING

TARGETED & ADVANCED THREATS

Uninformed users

Sensitive data shared

Cloud Migration

Social Engineered Attacks

Poor Visibility

VULNERABLE ORGANIZATIONS

EMAIL VENDOR

DLP VENDOR

ENDPOINT VENDOR

WEB VENDOR

POINT PRODUCTS = DISJOINTED SECURITY

OPERATIONAL COMPLEXITY

What Is Cloud Generation Email?

CLOUD GENERATION EMAIL

SECURE CLOUD & ON-PREMISES EMAIL

- Office 365 and G Suite cloud email
- Exchange and other on-premises email
- Seamless migration to the cloud

COMPLETE EMAIL SECURITY STACK

- Multi-layered with advanced threat protection
- Strong threat isolation prevents sophisticated attacks
- Deep visibility via advanced analytics
- Comprehensive impersonation defense and security awareness

EMAIL WITH INTEGRATED CYBER DEFENSE PLATFORM

- Integrated with endpoint, web security and DLP
- Holistic messaging security via CASB add-on
- Open APIs for SOC automation, ticketing systems integration, and orchestrated response

OPERATIONAL EFFICIENCY AT LOW TCO

- Single, strategic vendor
- Industry-leading SLAs
- Highest efficacy and accuracy

Cloud Generation Email Security Portfolio

BLOCK COMMON THREATS

- Heuristics
- Reputation Analysis
- Connection-level Detection
- AV Engine

STOP PHISHING ATTACKS

- Link Protection
- Impersonation Controls
- Phishing Variant Detection
- Behavioral Analysis

PROTECT AGAINST EMERGING THREATS

- Machine Learning & Sandboxing
- Click-Time Protection
- Advanced Email Security Analytics
- SOC Integration
- Threat Remediation

ISOLATE DANGEROUS THREATS

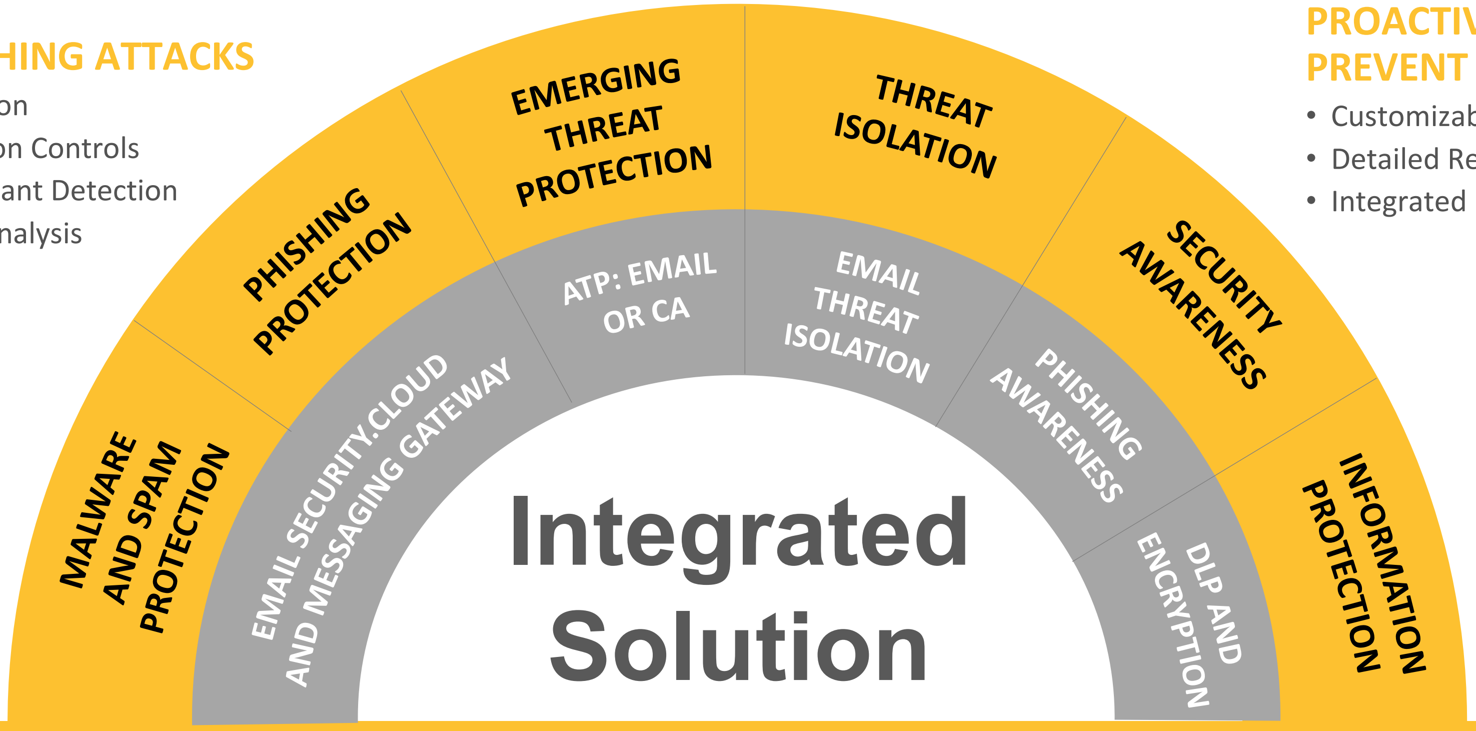
- Malicious URL Isolation
- Attachment Isolation
- Credential Theft Protection

PROACTIVELY PREVENT ATTACKS

- Customizable Security Assessments
- Detailed Reporting & Visibility
- Integrated User Education

PREVENT DATA LEAKAGE

- Advanced Detection Technologies
- Multi-Channel Data Protection
- Policy-Driven Controls
- Push & Pull Encryption



MALWARE AND SPAM PROTECTION

PHISHING PROTECTION

EMERGING THREAT PROTECTION

THREAT ISOLATION

SECURITY AWARENESS

INFORMATION PROTECTION

EMAIL SECURITY.CLOUD AND MESSAGING GATEWAY

ATP: EMAIL OR CA

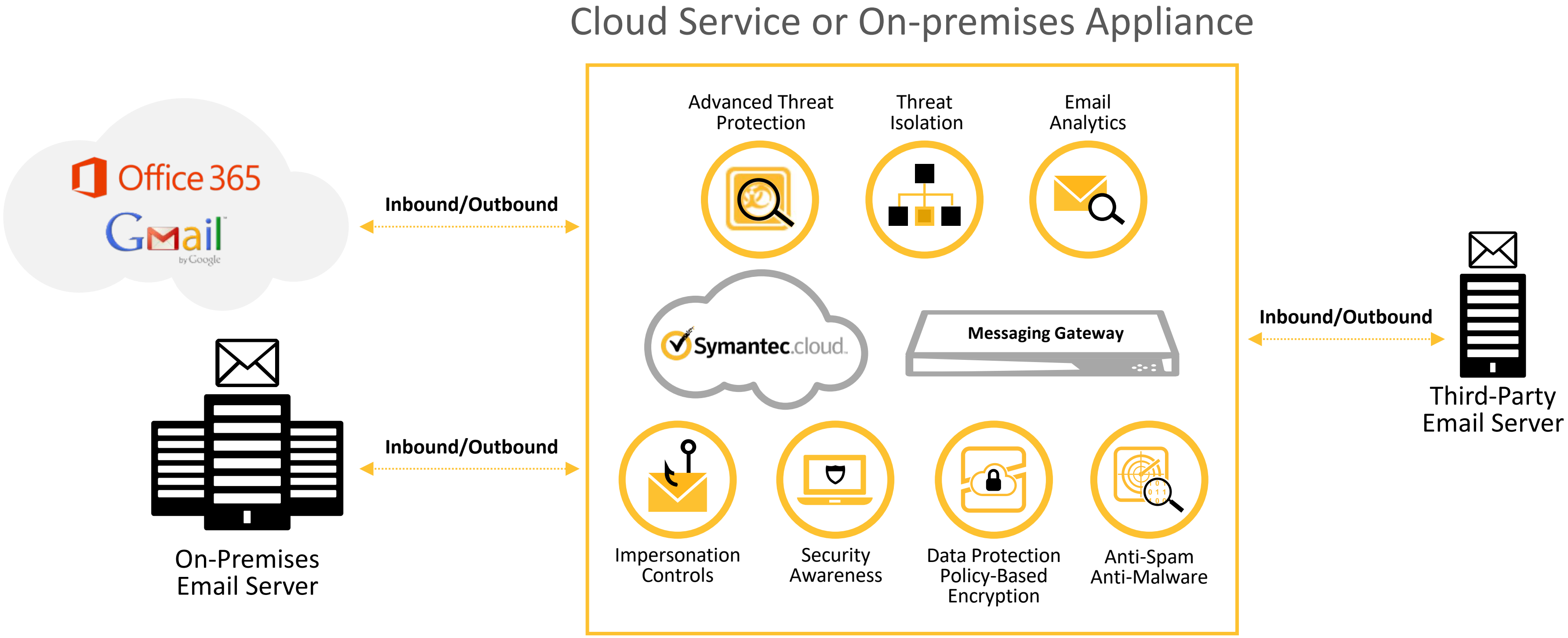
EMAIL THREAT ISOLATION

PHISHING AWARENESS

DLP AND ENCRYPTION

Integrated Solution

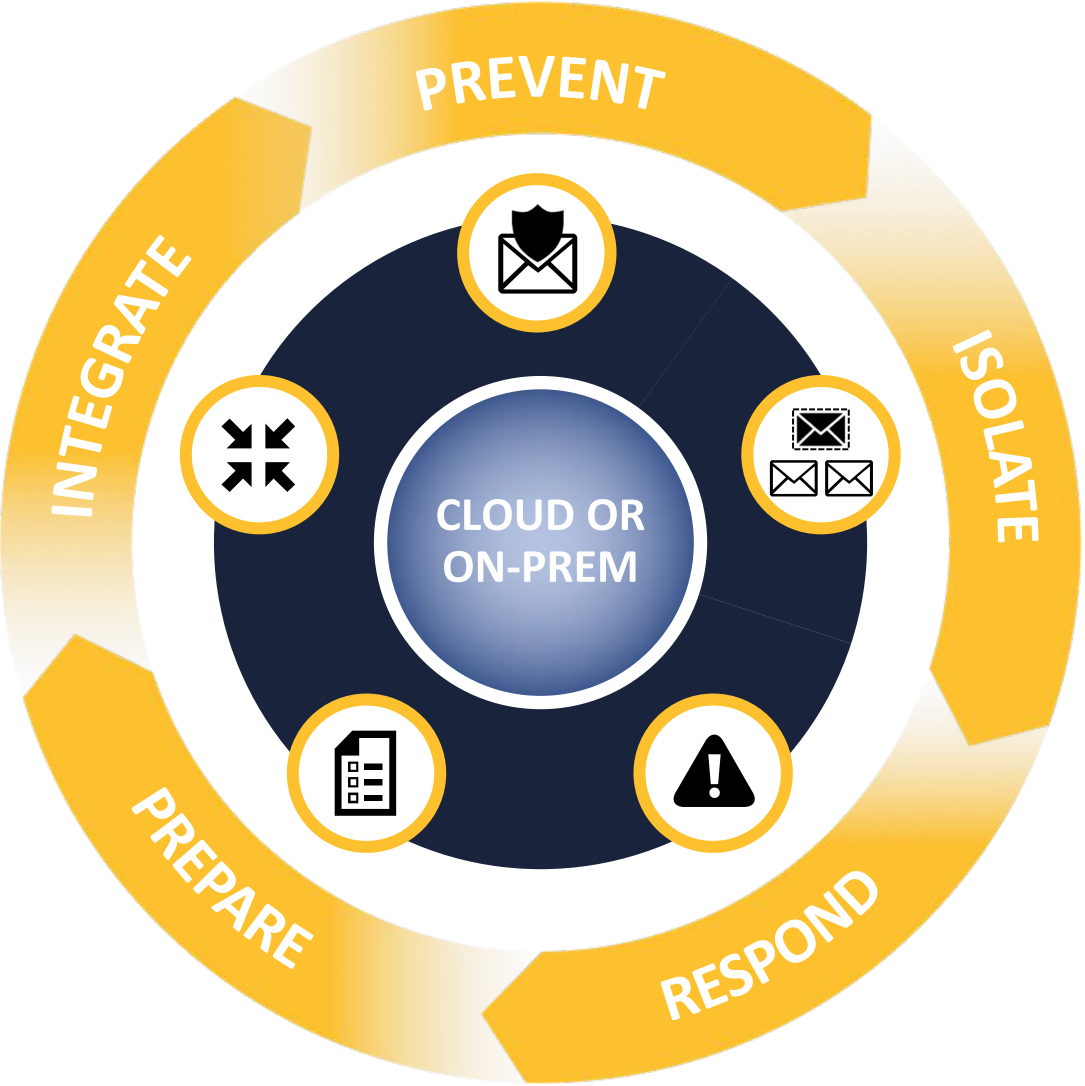
The Cloud Generation Email Security Solution



Solution Overview

- Protects against targeted attacks, ransomware, spear phishing & business email compromise
- Gives deep visibility into advanced attacks and accelerates threat response
- Controls sensitive data and helps meet compliance & privacy requirements
- Reduces business risks by training employees to recognize & report email attacks

Email Security Framework



PREVENT

ISOLATE

RESPOND

PREPARE

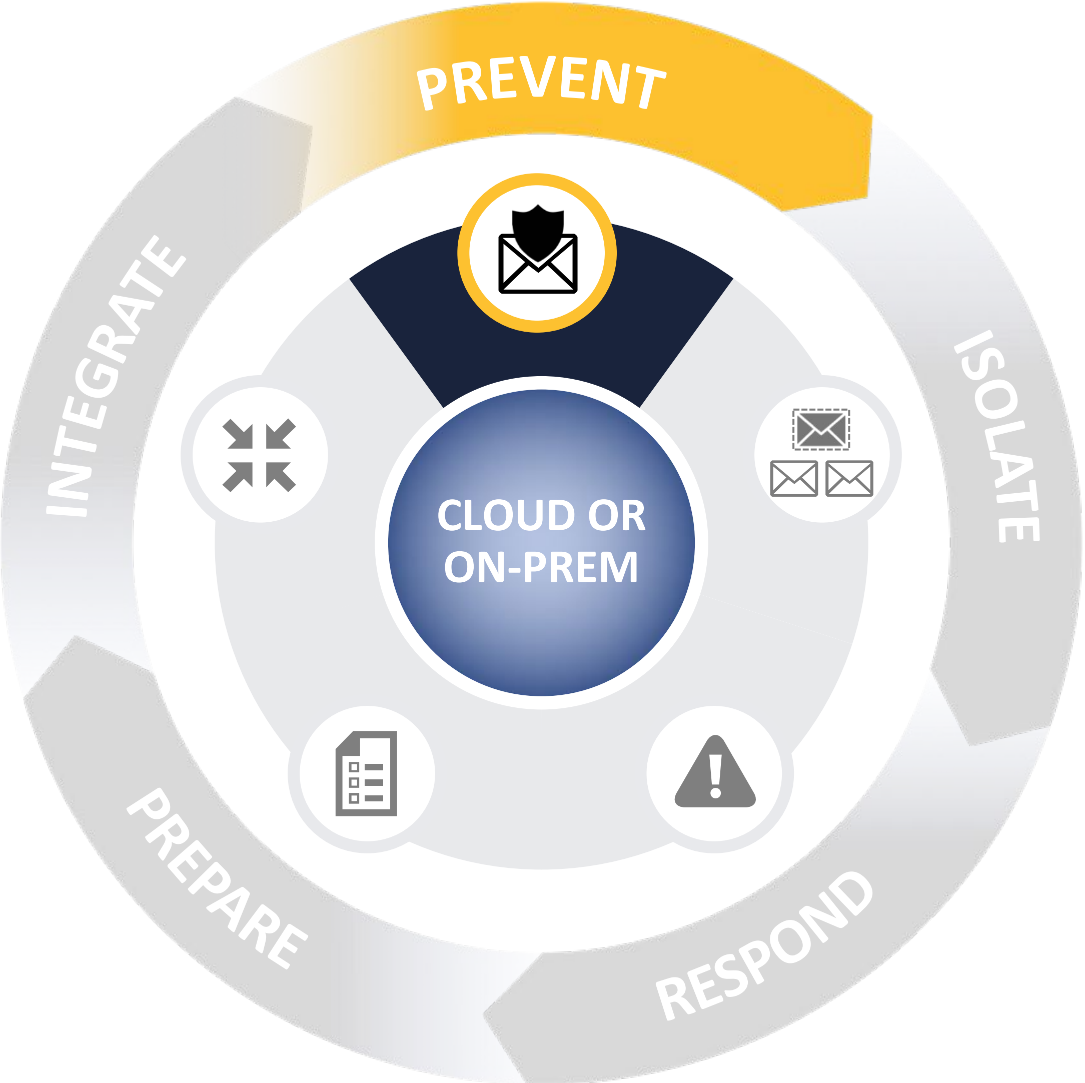
INTEGRATE

CLOUD OR ON-PREM

Email Security Framework

Email Security.cloud Messaging Gateway:

- DISCOVER
- BLOCK
- REPORT



Prevent Overview

USE CASE #1

Ransomware

“I need to prevent ransomware threats from reaching my endpoints.”

USE CASE #2

Impersonation

“I need to protect specific executives or all users from attacks impersonating a user.”

USE CASE #3

Spam & Bulk Mail

“I want to eliminate spam and bulk mail, which hamper user productivity.”

Strong prevention technologies lower security risk and improve productivity

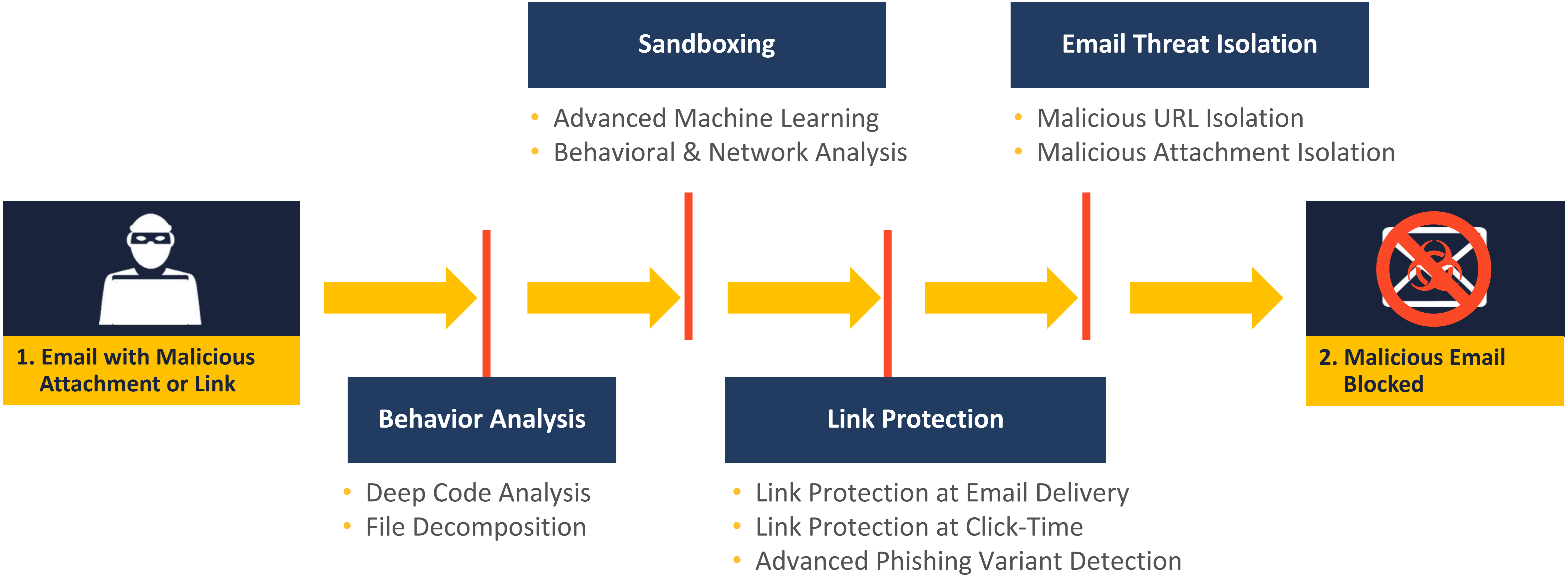
Symantec: Most Complete Protection in the Industry

Symantec

Global Intelligence Network

CONNECTION LEVEL	MALWARE & SPAM DEFENSE	LINK PROTECTION	IMPERSONATION CONTROL	BEHAVIOR ANALYSIS	ADVANCED MACHINE LEARNING	SANDBOXING
SMTP firewall, sender reputation and authentication reduce risks and throttle bad connections	Heuristics, reputation, and signature based engines evaluate files and URLs for email malware & spam	Evaluates malicious links at email delivery and time of click with advanced phishing variant detection	Blocks Business Email Compromise and other spoofing attacks	Identifies new, crafted, and hidden malware by examining the behavior of suspicious email	Analyzes code for malicious characteristics	Detonates only truly unknown files in both physical and virtual environments
MALWARE & SPAM PROTECTION		PHISHING DEFENSE		EMERGING THREAT PREVENTION		

Gain Comprehensive Protection Against Evolving Ransomware



1. Email with Malicious Attachment or Link

Behavior Analysis

- Deep Code Analysis
- File Decomposition

Sandboxing

- Advanced Machine Learning
- Behavioral & Network Analysis

Link Protection

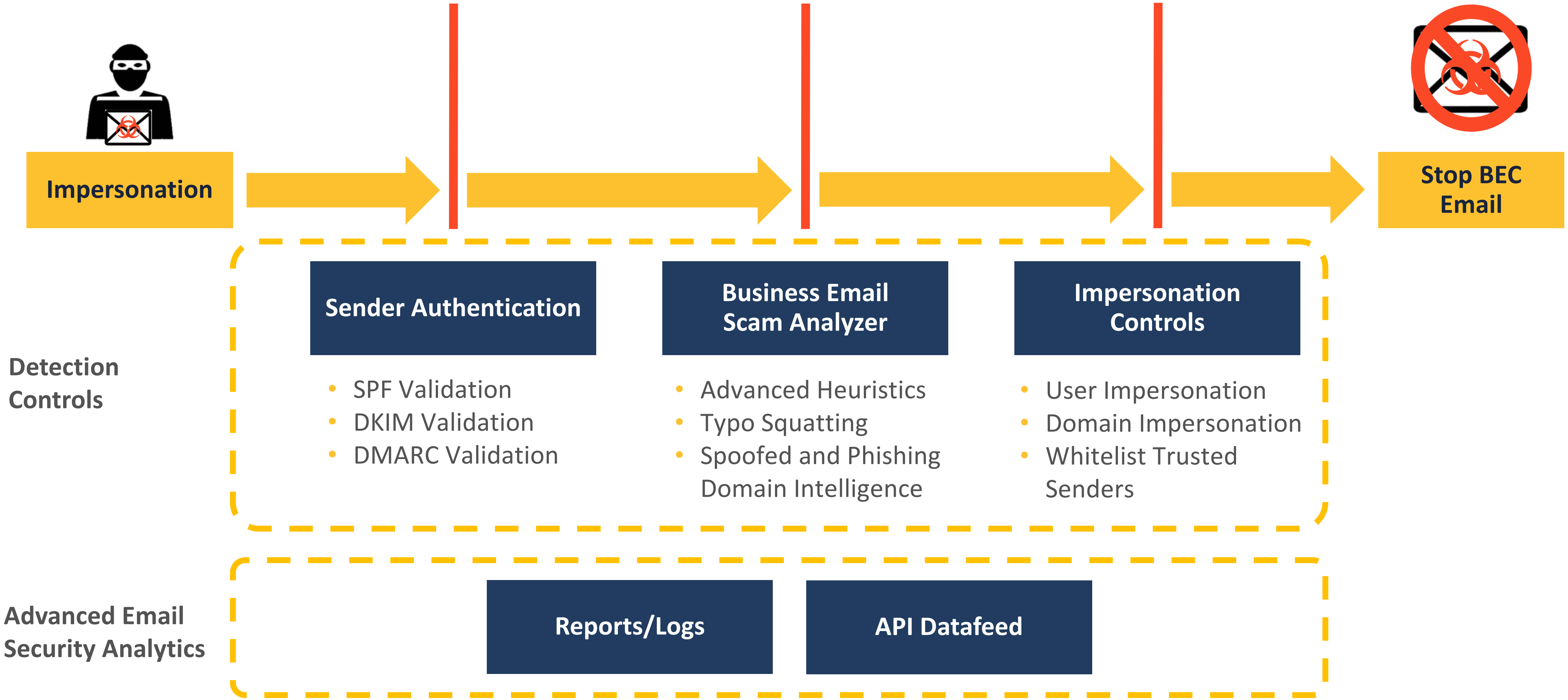
- Link Protection at Email Delivery
- Link Protection at Click-Time
- Advanced Phishing Variant Detection

Email Threat Isolation

- Malicious URL Isolation
- Malicious Attachment Isolation

2. Malicious Email Blocked

Strongest Protection Against Impersonation Attacks



Impersonation

Stop BEC Email

Detection Controls

Sender Authentication

- SPF Validation
- DKIM Validation
- DMARC Validation

Business Email Scam Analyzer

- Advanced Heuristics
- Typo Squatting
- Spoofed and Phishing Domain Intelligence

Impersonation Controls

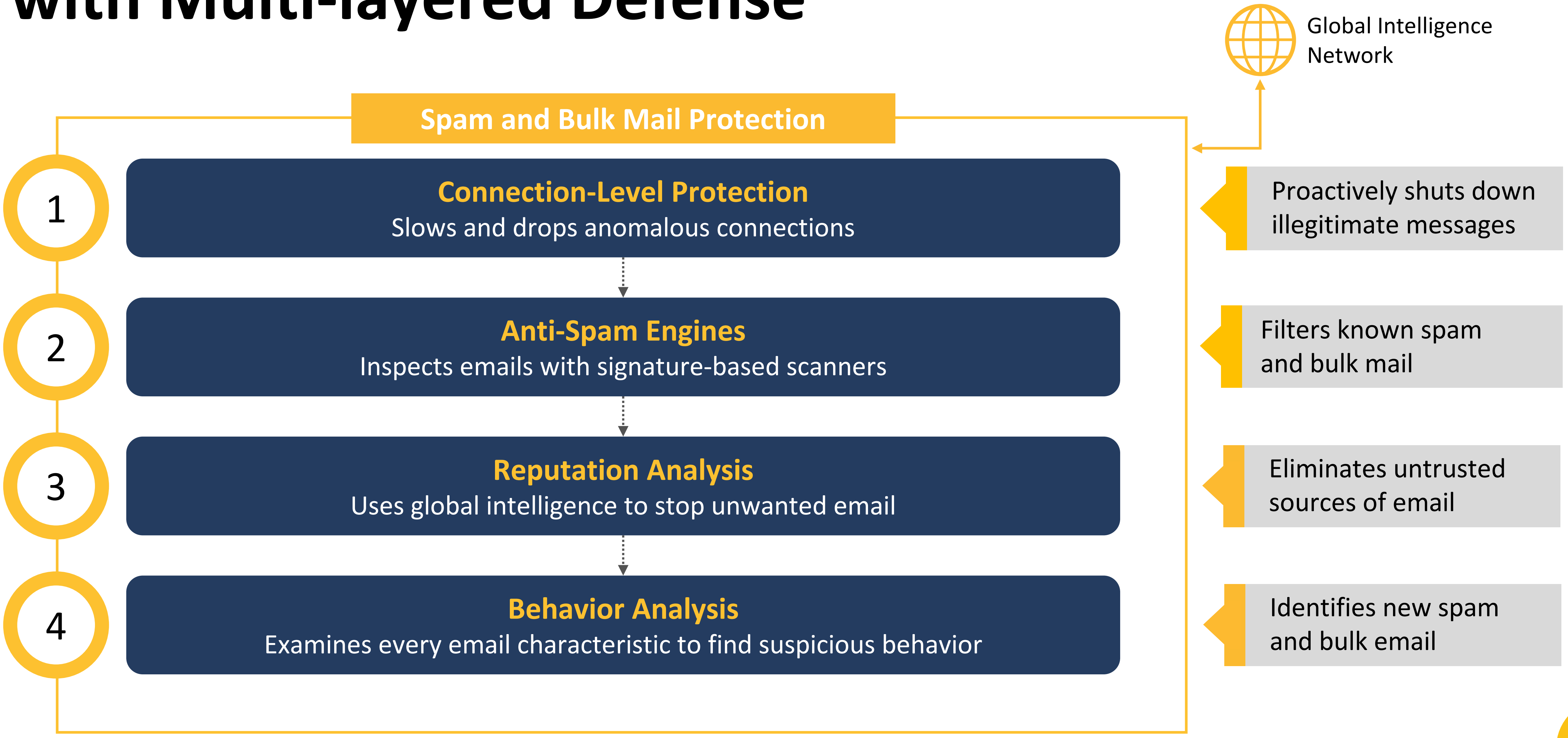
- User Impersonation
- Domain Impersonation
- Whitelist Trusted Senders

Advanced Email Security Analytics

Reports/Logs

API Datafeed

Symantec Blocks Unwanted Email with Multi-layered Defense



Global Intelligence Network

Spam and Bulk Mail Protection

1 **Connection-Level Protection**
Slows and drops anomalous connections

Proactively shuts down illegitimate messages

2 **Anti-Spam Engines**
Inspects emails with signature-based scanners

Filters known spam and bulk mail

3 **Reputation Analysis**
Uses global intelligence to stop unwanted email

Eliminates untrusted sources of email

4 **Behavior Analysis**
Examines every email characteristic to find suspicious behavior

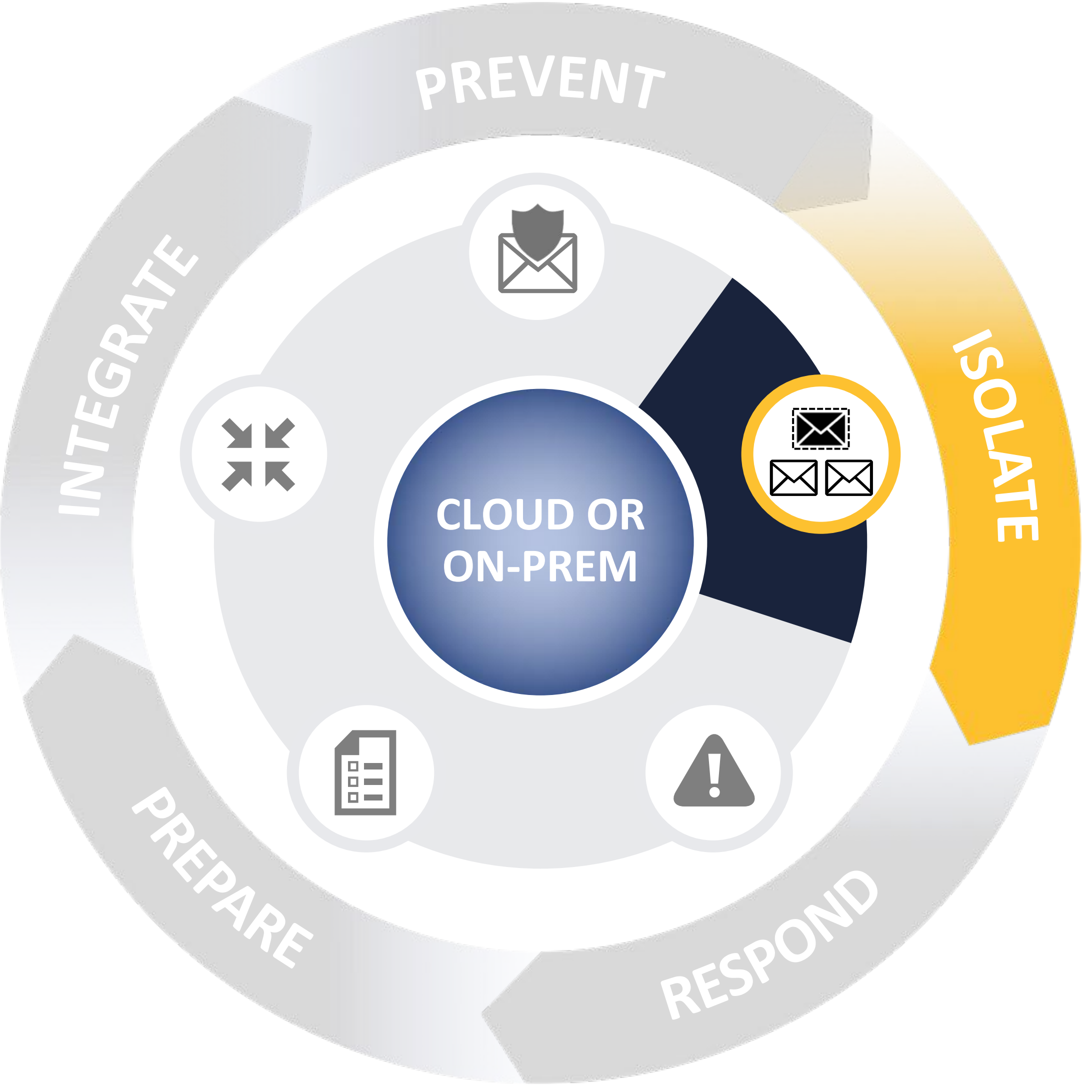
Identifies new spam and bulk email

Email Security Framework

Email Threat Isolation

ANALYZE

INSULATE



Email Threat Isolation Overview

Symantec.

USE CASE #1

Isolate Malicious URLs

“I want elevated levels of protection for my users against spear phishing and advanced attacks.”

USE CASE #2

Isolate Malicious Attachments

“I want to prevent ransomware and other malware from infecting endpoints with weaponized attachments.”

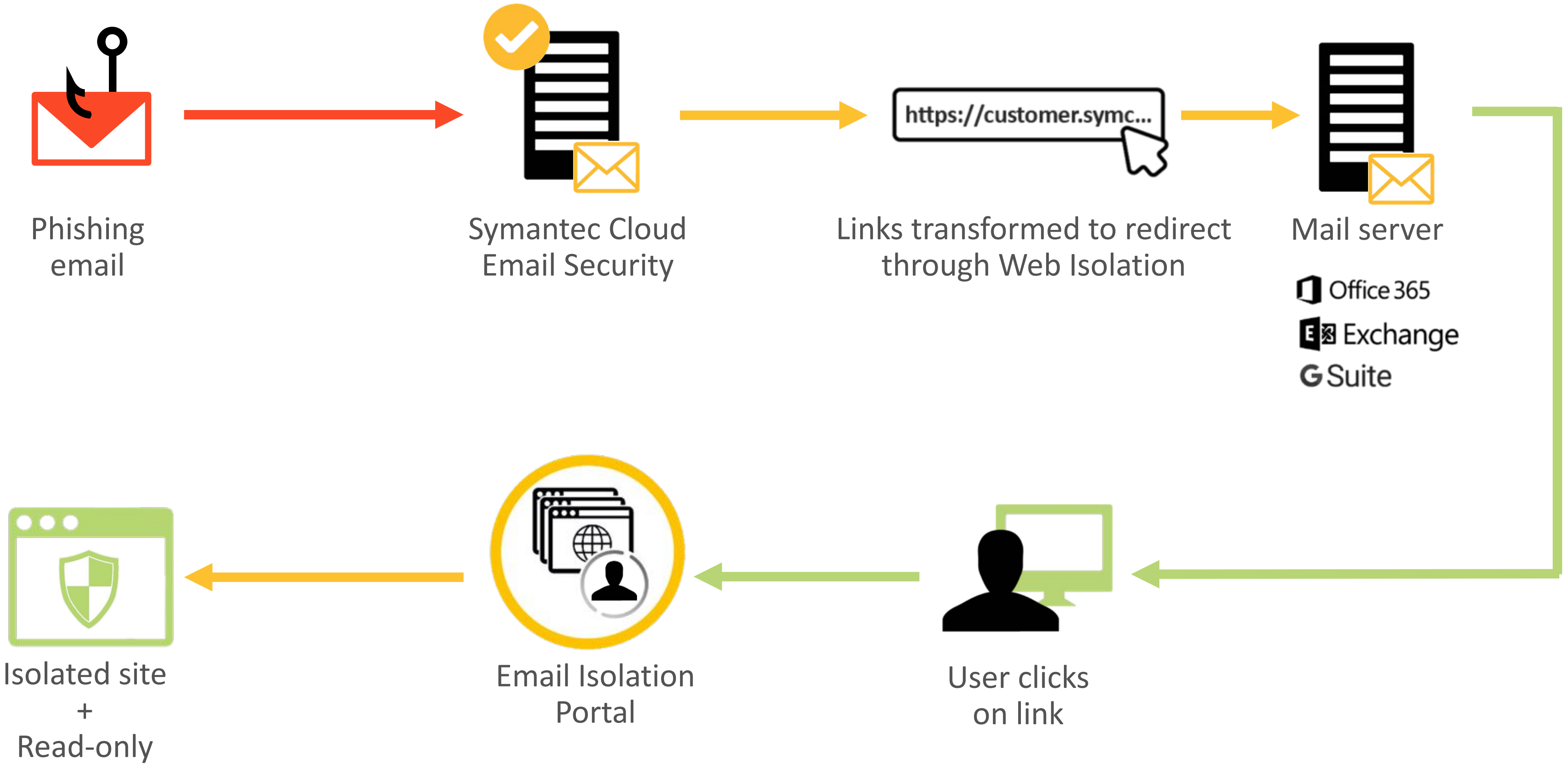
USE CASE #3

Stop Credential Theft

“I want to stop users from submitting corporate passwords and sensitive information to malicious websites.”

Take prevention to the next level with threat isolation

How Email Threat Isolation Works



Phishing email

Symantec Cloud Email Security

Links transformed to redirect through Web Isolation

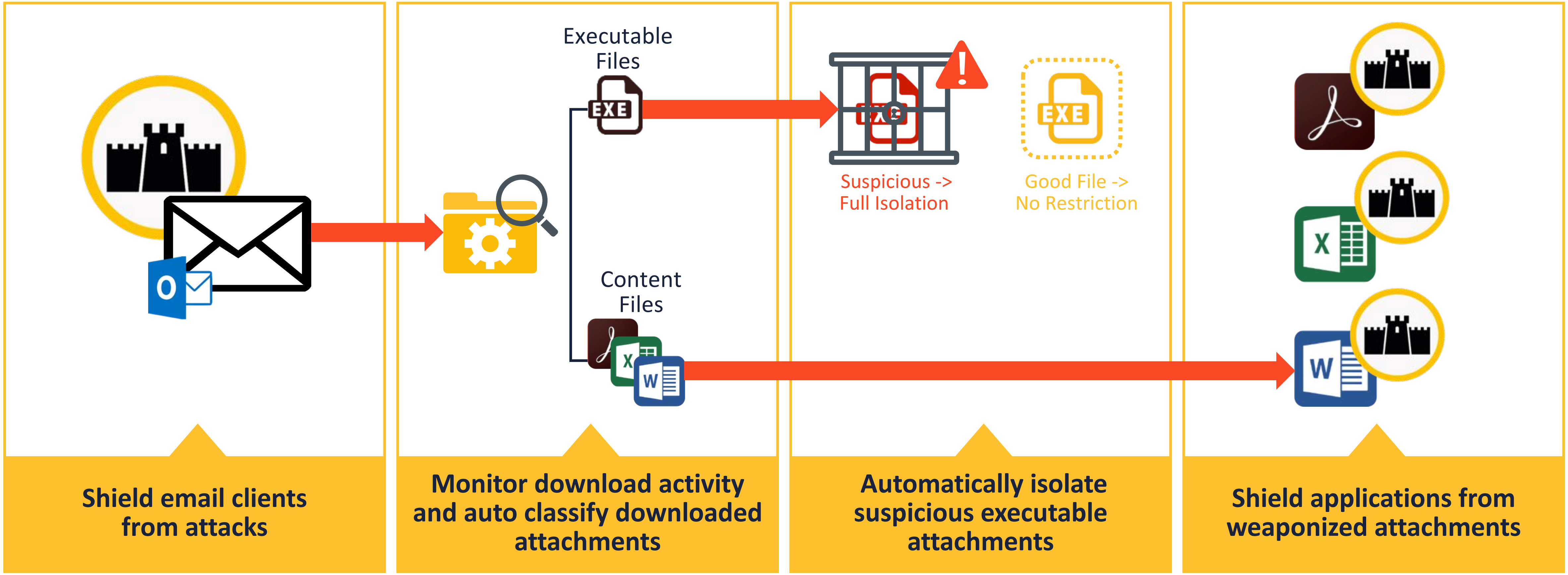
Mail server

User clicks on link

Email Isolation Portal

Isolated site
+
Read-only

Defend Against Weaponized Attachments with SEP Hardening



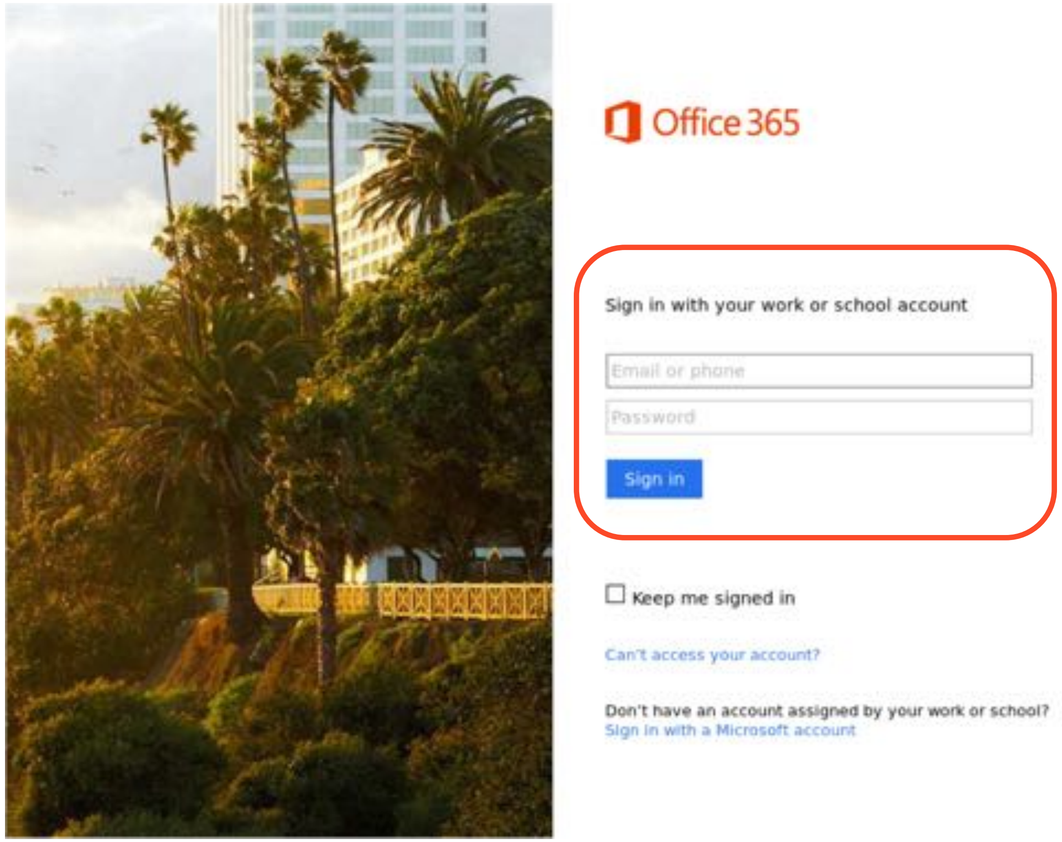
Shield email clients from attacks

Monitor download activity and auto classify downloaded attachments

Automatically isolate suspicious executable attachments

Shield applications from weaponized attachments

Prevent Credential Theft with Read-only Protection



Sign in with your work or school account

Email or phone

Password

□ Keep me signed in

Can't access your account?

Don't have an account assigned by your work or school?
Sign in with a Microsoft account

Eliminate phishing and its risks by rendering websites in read-only mode

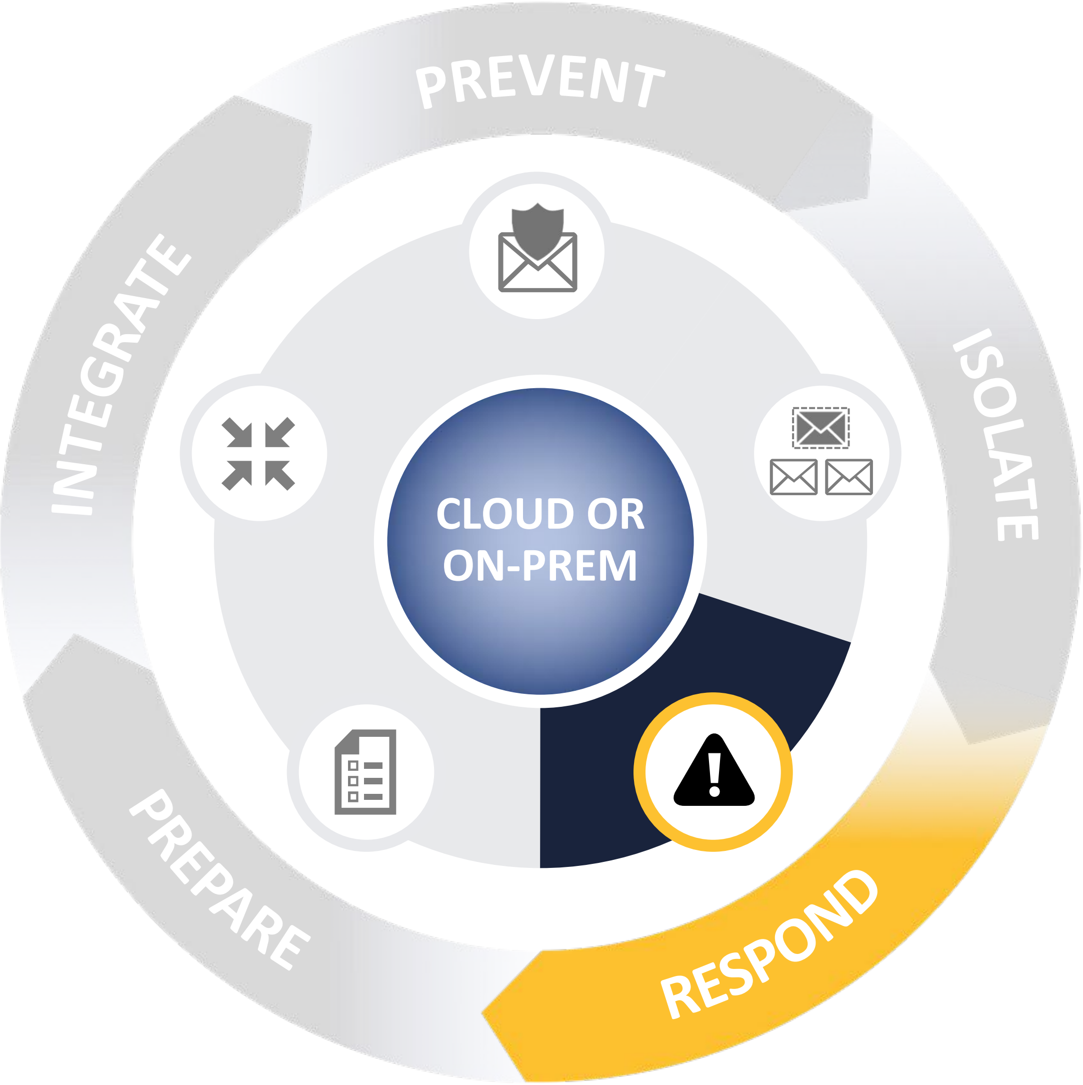
Prevent sensitive information from being enter into malicious web forms

Requires **no hardware or software**

Email Security Framework

ATP:Email

- EXPOSE
- PRIORITIZE
- INVESTIGATE
- CONTAIN
- RESOLVE



Detect and Respond Overview

USE CASE #1

Visibility

"I need deep visibility into sophisticated attacks and prioritization of incidents to accelerate threat response."

USE CASE #2

Hunting

"I want to hunt threats in my email and correlate events across my security environment."

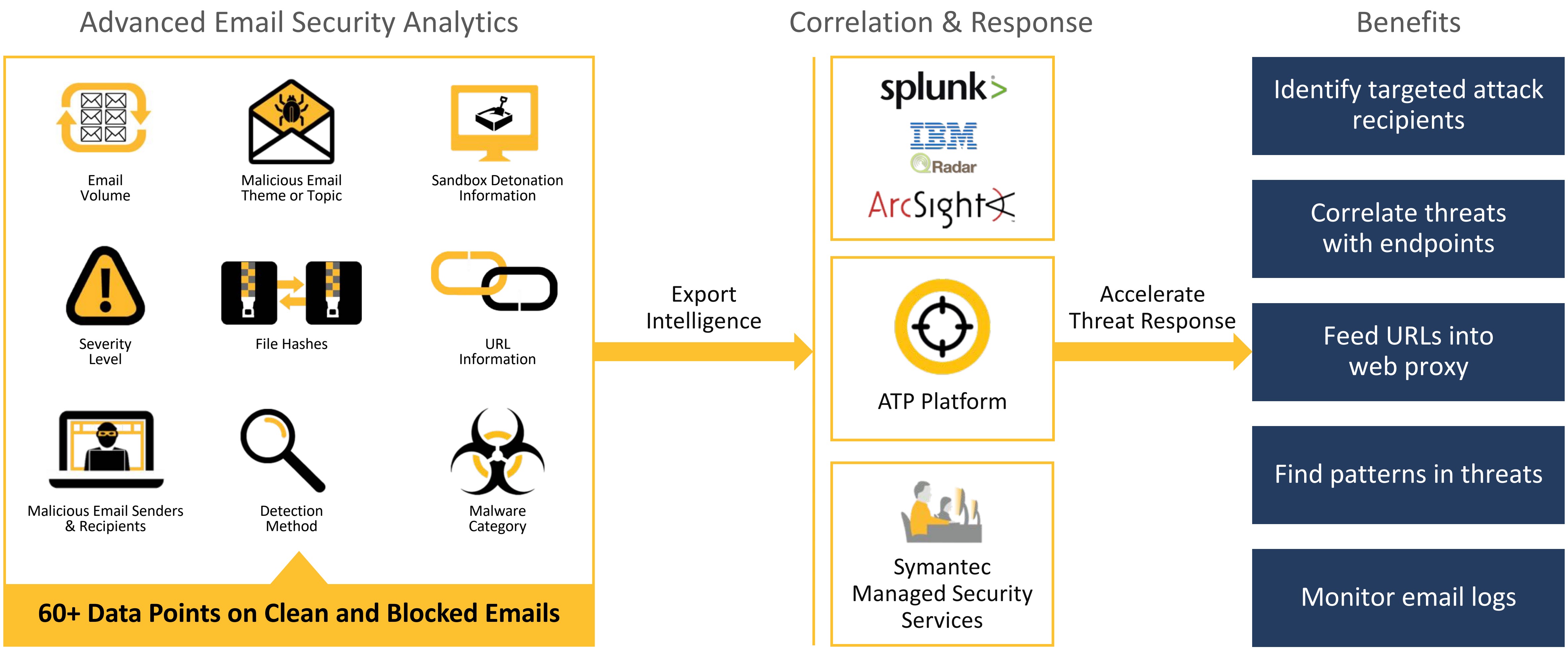
USE CASE #3

Remediation

"I want to contain threats and orchestrate response across my security controls."

Stop targeted and advanced email attacks in their tracks

Gain the Deepest Visibility Into Targeted & Advanced Attacks



Advanced Email Security Analytics

- Email Volume
- Malicious Email Theme or Topic
- Sandbox Detonation Information
- Severity Level
- File Hashes
- URL Information
- Malicious Email Senders & Recipients
- Detection Method
- Malware Category

60+ Data Points on Clean and Blocked Emails

Export Intelligence

Correlation & Response

- splunk> / IBM QRadar / ArcSight
- ATP Platform
- Symantec Managed Security Services

Accelerate Threat Response

Benefits

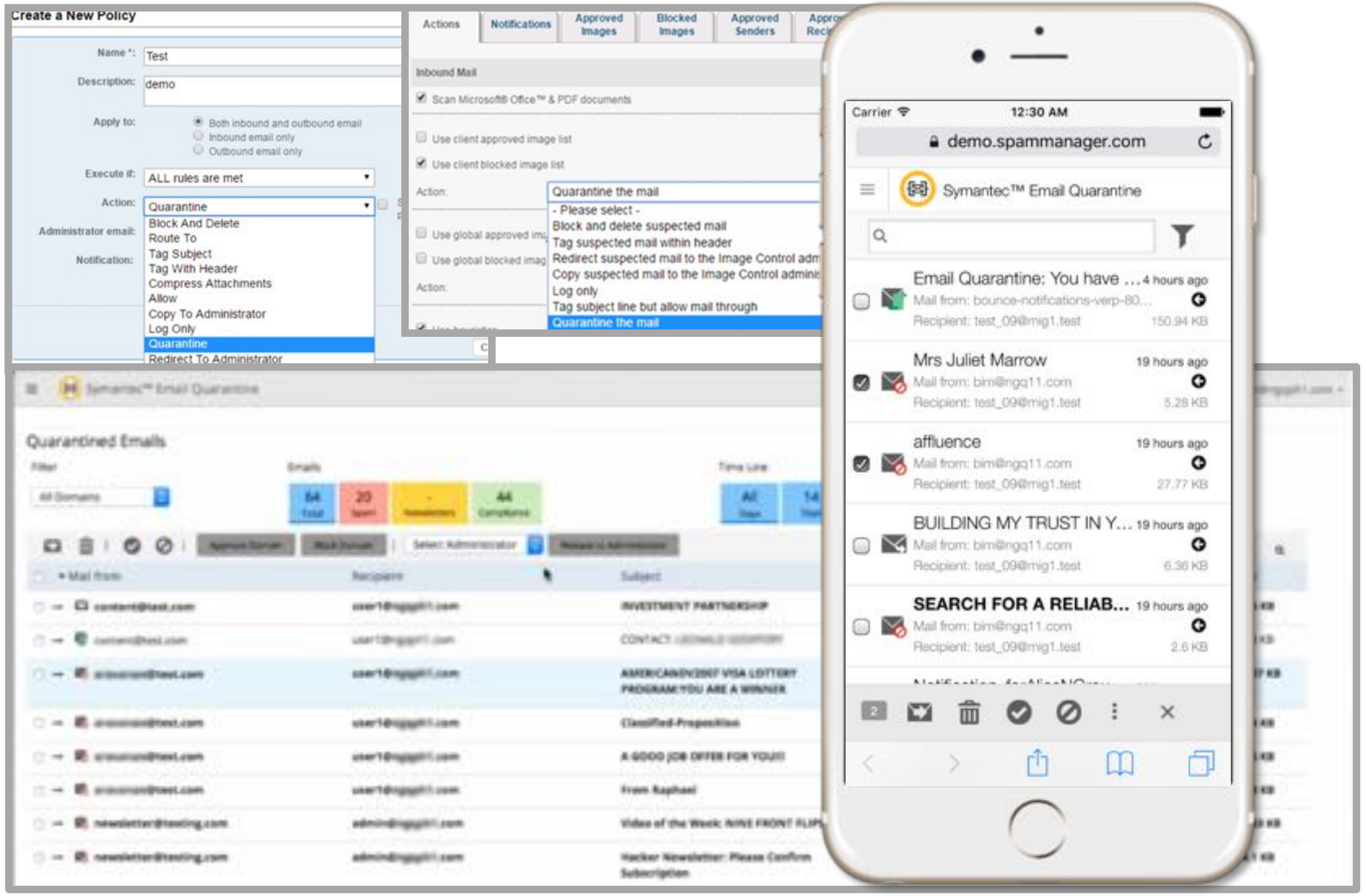
- Identify targeted attack recipients
- Correlate threats with endpoints
- Feed URLs into web proxy
- Find patterns in threats
- Monitor email logs

Remediate Threats by Quarantining Dangerous Emails

Enhanced **mobile experience**

Clearly differentiates between **spam and information protection** messages

Quarantine **data protection & image control** messages



Create a New Policy

Name *: Test

Description: demo

Apply to: ● Both inbound and outbound email ○ Inbound email only ○ Outbound email only

Execute if: ALL rules are met

Action: Quarantine

Administrator email:

Notification:

Inbound Mail

☑ Scan Microsoft® Office™ & PDF documents

☐ Use client approved image list

☑ Use client blocked image list

Action: Quarantine the mail

☐ Use global approved ima

☐ Use global blocked imag

- Please select -
Block and delete suspected mail
Tag suspected mail within header
Redirect suspected mail to the Image Control adm
Copy suspected mail to the Image Control adminis
Log only
Tag subject line but allow mail through
Quarantine the mail

Mail from	Recipient	Subject
content@test.com	user1@ngqg11.com	INVESTMENT PARTNERSHIP
content@test.com	user1@ngqg11.com	CONTACT
[illegible]	user1@ngqg11.com	AMERICAN DV2007 VISA LOTTERY PROGRAM:YOU ARE A WINNER
[illegible]	user1@ngqg11.com	Classified-Proposition
[illegible]	user1@ngqg11.com	A GOOD JOB OFFER FOR YOU!!
[illegible]	user1@ngqg11.com	From Raphael
newsletter@testing.com	admin@ngqg11.com	Video of the Week: NINE FRONT FLIPS
newsletter@testing.com	admin@ngqg11.com	Hacker Newsletter: Please Confirm Subscription

	Subject	Time	Mail from	Recipient	Size
☐	Email Quarantine: You have …	4 hours ago	bounce-notifications-verp-80…	test_09@mig1.test	150.94 KB
☑	Mrs Juliet Marrow	19 hours ago	bim@ngq11.com	test_09@mig1.test	5.28 KB
☑	affluence	19 hours ago	bim@ngq11.com	test_09@mig1.test	27.77 KB
☐	BUILDING MY TRUST IN Y…	19 hours ago	bim@ngq11.com	test_09@mig1.test	6.36 KB
☐	SEARCH FOR A RELIAB…	19 hours ago	bim@ngq11.com	test_09@mig1.test	2.6 KB

Show **additional message information** such as attachment names and direction

Can **hold DLP violating message** for quarantine admin review and release or release to an admin

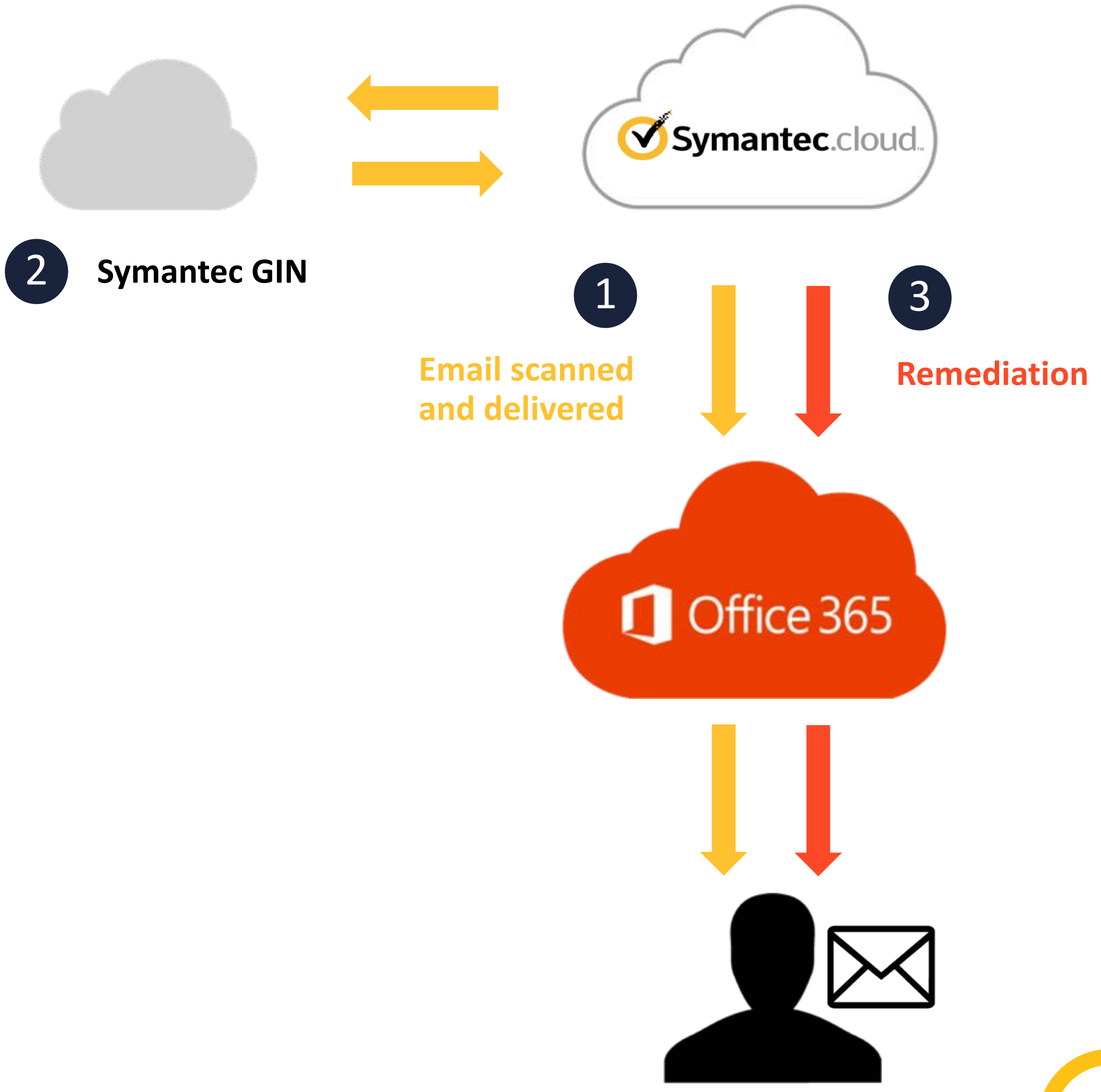
Enhanced reporting options with more details on usage

Automatically Remediate Email Threats in Office 365

Clawback emails from Office 365 **after** they've been delivered

Contain threats and stop missed email attacks from spreading

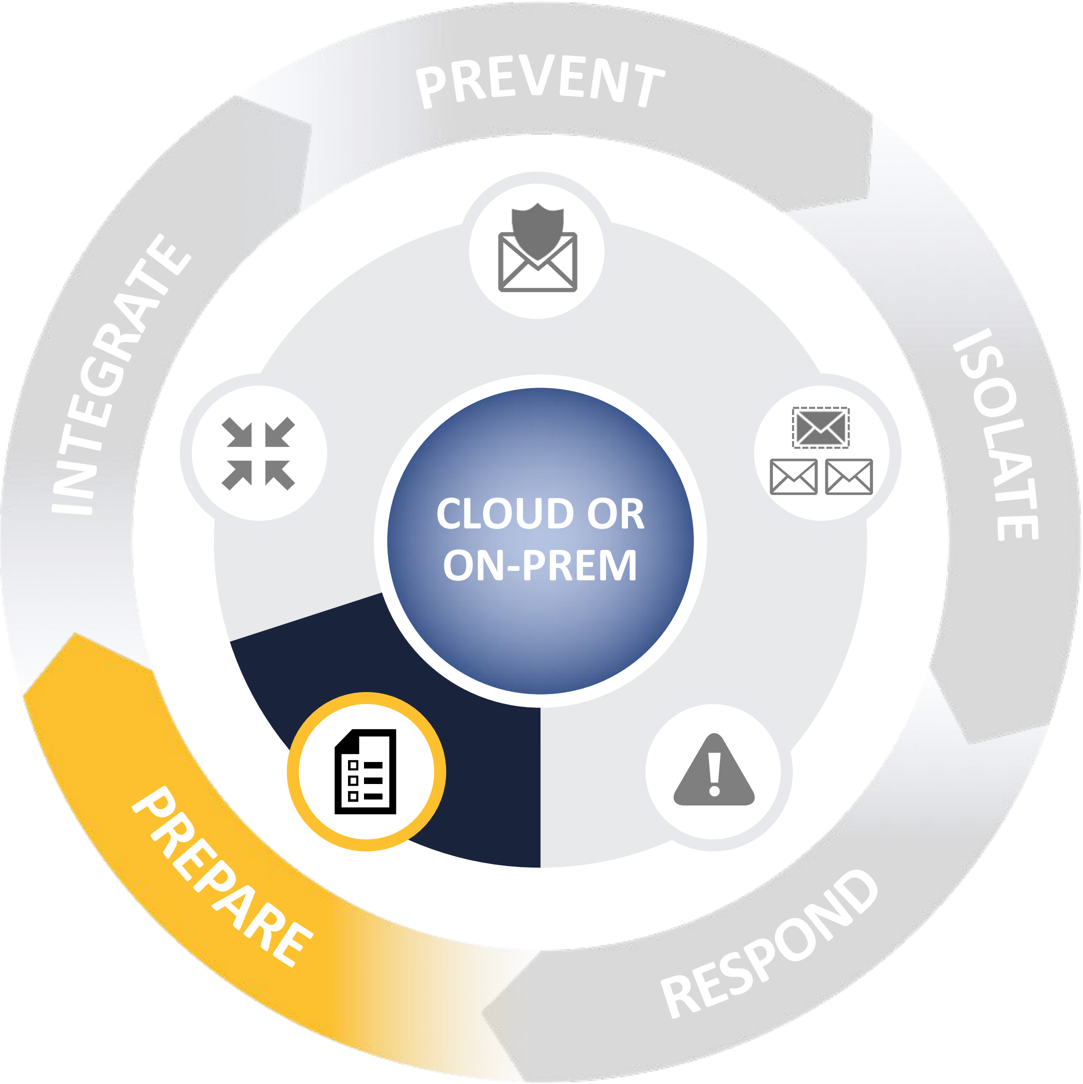
Speed remediation of potential issues



Email Security Framework

Security Awareness

- SIMULATE
- BENCHMARK
- TRAIN



Copyright © 2018 Symantec Corporation

Prepare Overview

Symantec

USE CASE #1

Assessment

“I want to assess employee readiness to email attacks by simulating real-world threats.”

USE CASE #2

Tracking

“I want to track progress of my employee security awareness over time.”

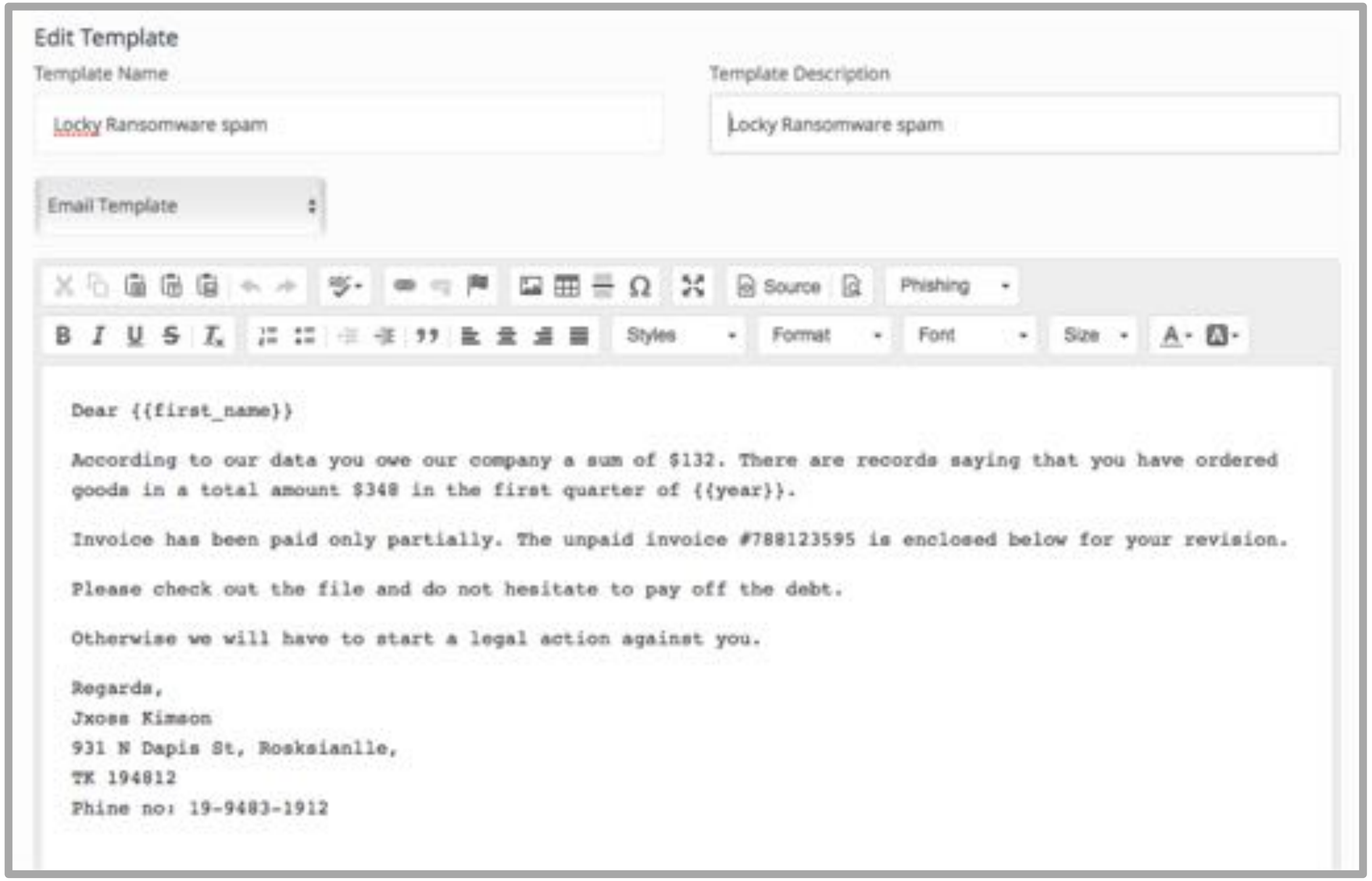
USE CASE #3

Education

“I want to reduce my security risks by educating users to recognize sophisticated email attacks.”

Reduce your business risks with effective security training

Easily Tailor Assessments to Your Needs



Edit Template

Template Name: Locky Ransomware spam

Template Description: Locky Ransomware spam

Email Template

Dear {{first_name}}

According to our data you owe our company a sum of $132. There are records saying that you have ordered goods in a total amount $348 in the first quarter of {{year}}.

Invoice has been paid only partially. The unpaid invoice #788123595 is enclosed below for your revision.

Please check out the file and do not hesitate to pay off the debt.

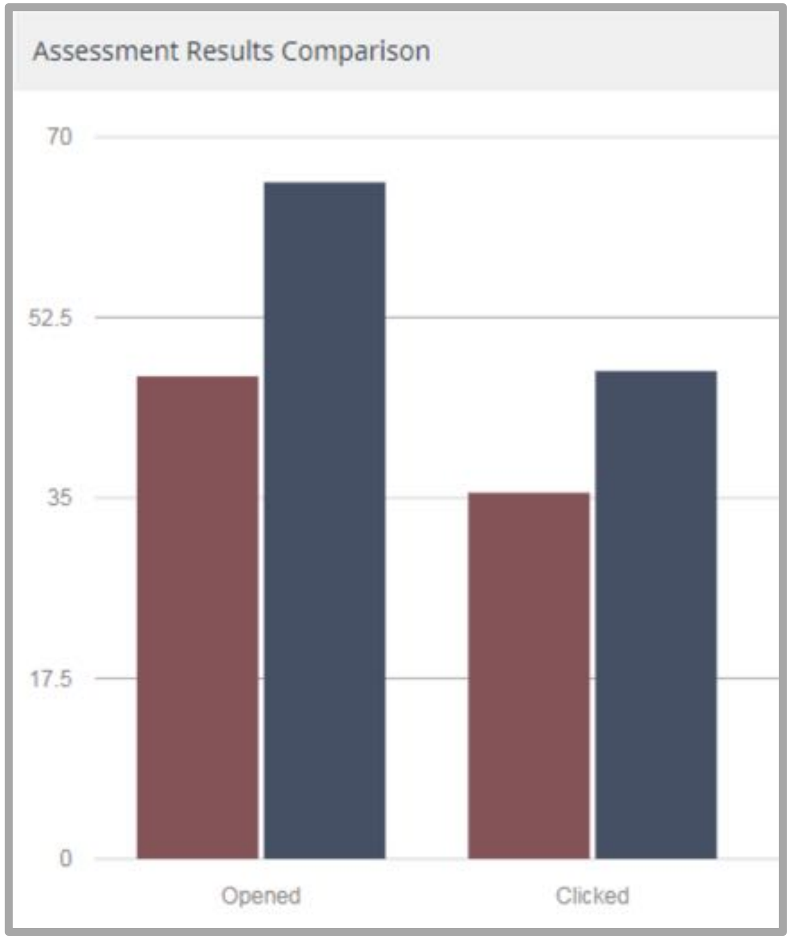
Otherwise we will have to start a legal action against you.

Regards,
Jxoss Kimson
931 N Dapis St, Rosksianlle,
TK 194812
Phine no: 19-9483-1912

- Mimic the latest, real-world email threats
- Create custom assessments with templates and landing pages
- Quickly deploy and manage security assessments

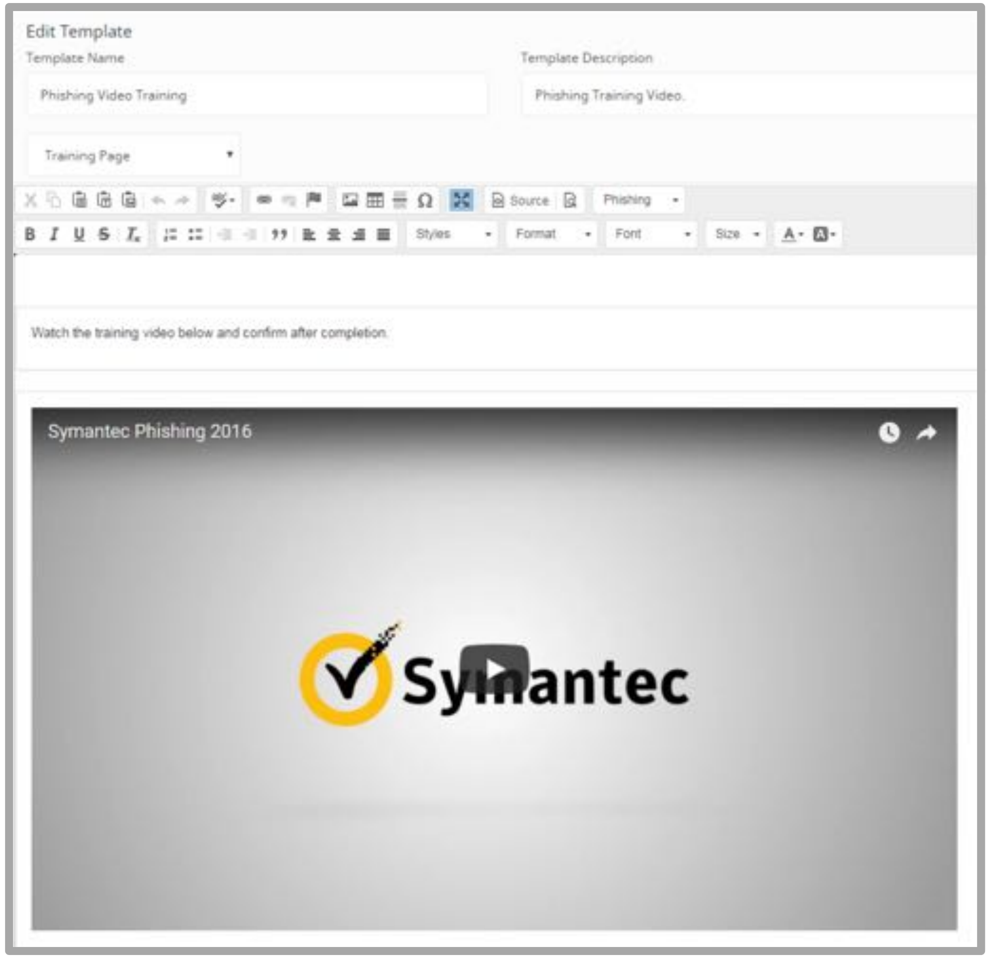
Improve Security Awareness With Integrated Insights

- Understand user behavior with executive dashboards and detailed reporting
- Identify key trends by comparing results to previous assessments
- Develop user risk profiles by combining assessment results with email threats



Condition Employees to Recognize and Report Email Attacks

- Alert vulnerable users to complete required security education
- Teach users to spot sophisticated email attacks through training
- Customize training alerts and landing pages to the needs of your business



Edit Template

Template Name: Phishing Video Training

Template Description: Phishing Training Video.

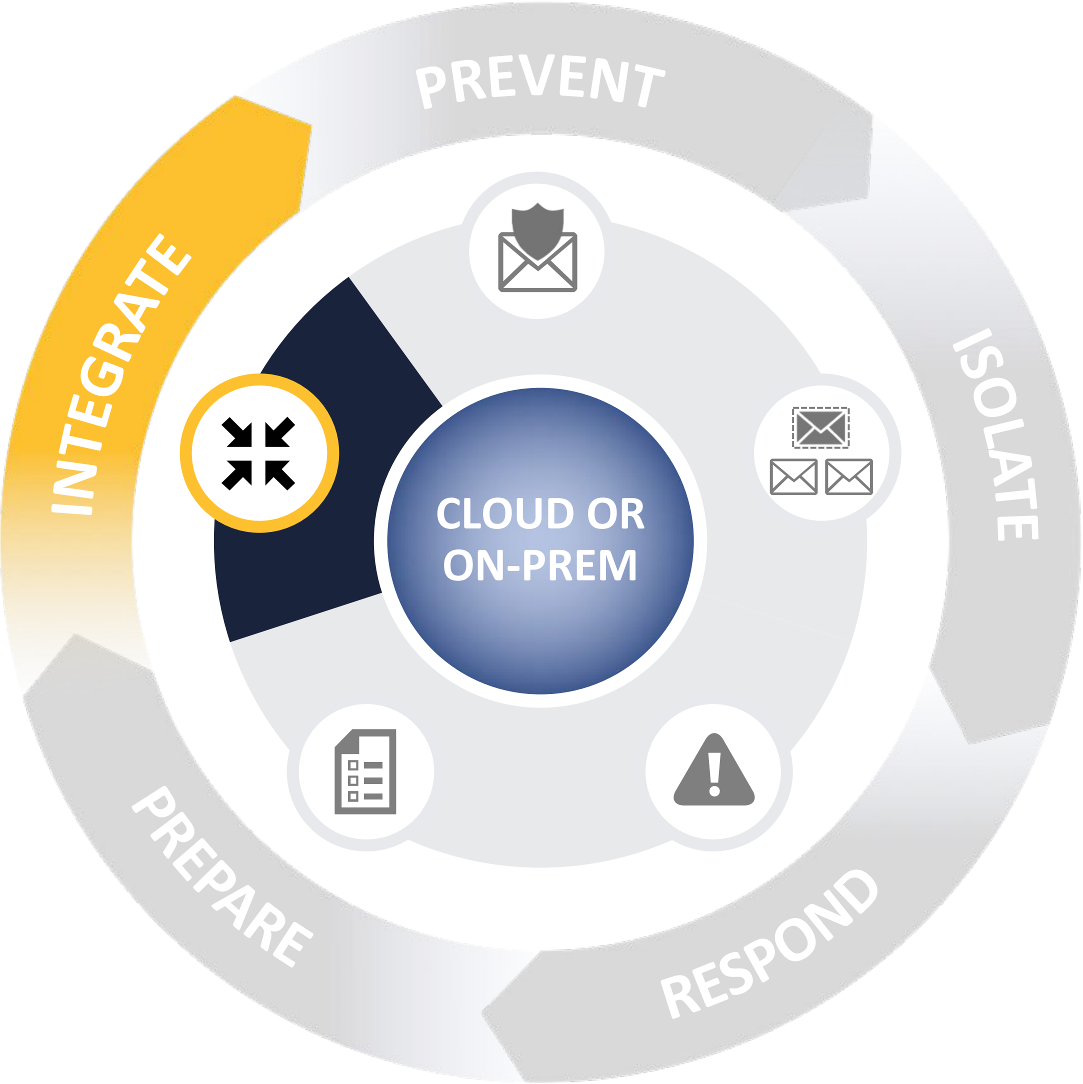
Training Page

Watch the training video below and confirm after completion.

Email Security Framework

Symantec.

- DLP
- ENCRYPTION
- CASB
- SIEM
- ENDPOINT
- WEB



Integrate Overview

Symantec.

USE CASE #1

Integrated Information Protection

“I want advanced information protection across my email channel.”

USE CASE #2

Secure Cloud Adoption

“I want to securely move my infrastructure to the cloud.”

USE CASE #3

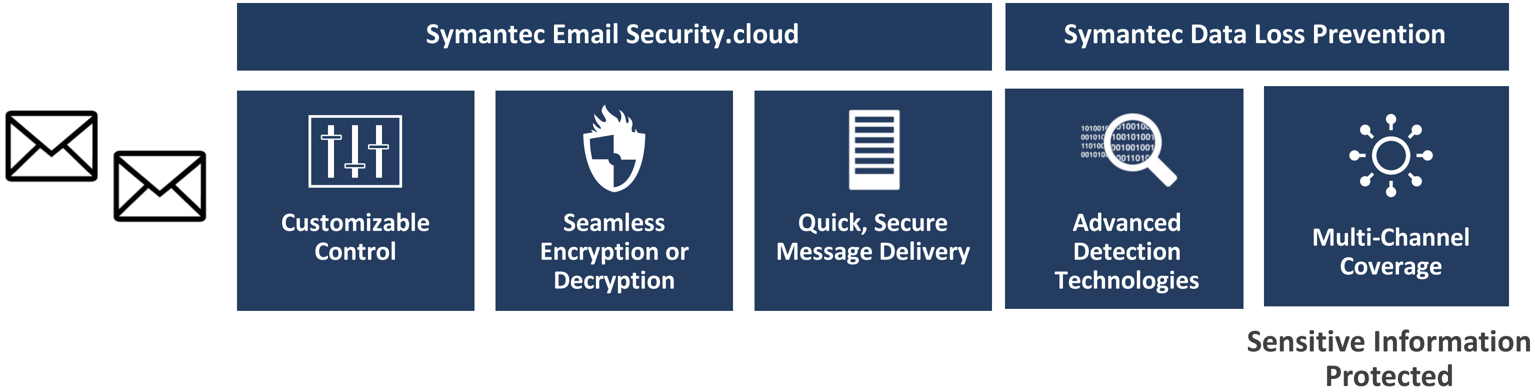
Security Infrastructure

“I want to leverage existing investments by integrating email security with the rest of my security infrastructure.”

Harness the power of an Integrated Cyber Defense platform

Information Protection

Protect Your Sensitive Data in the Cloud



Symantec Email Security.cloud

Symantec Data Loss Prevention

Customizable Control

Seamless Encryption or Decryption

Quick, Secure Message Delivery

Advanced Detection Technologies

Multi-Channel Coverage

Sensitive Information Protected

✓ PCI ✓ HIPAA ✓ ITAR ✓ GLBA

Granular DLP policies protect sensitive data and help address legal & compliance requirements

Symantec DLP integration prevents data leakage with advanced detection technologies & multi-channel coverage

Policy-based encryption policies automatically safeguard the security & privacy of confidential emails

Protect Office 365 with Comprehensive Cloud Security

Symantec Email Security

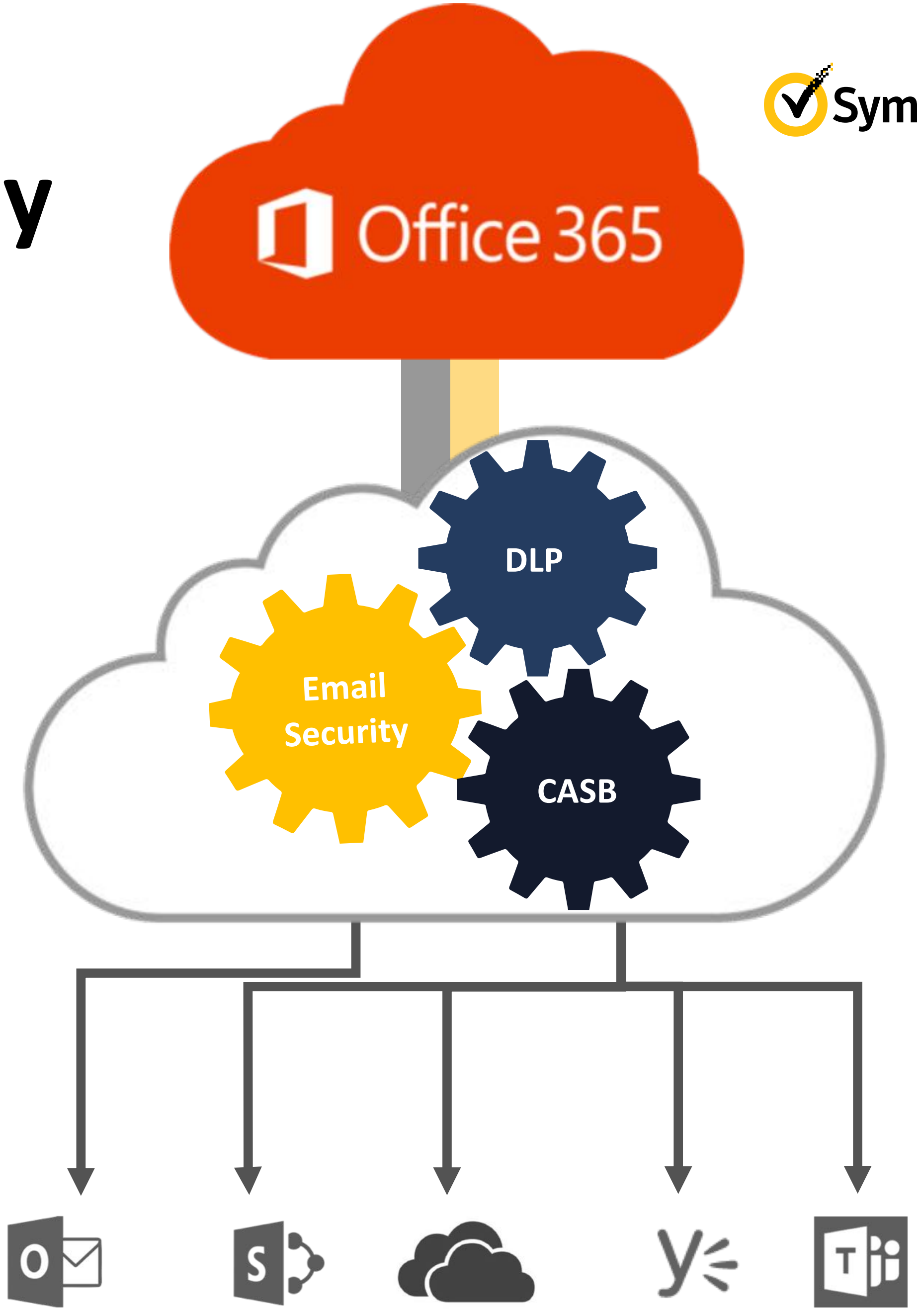
- Protect against advanced attacks in external email

Symantec CASB

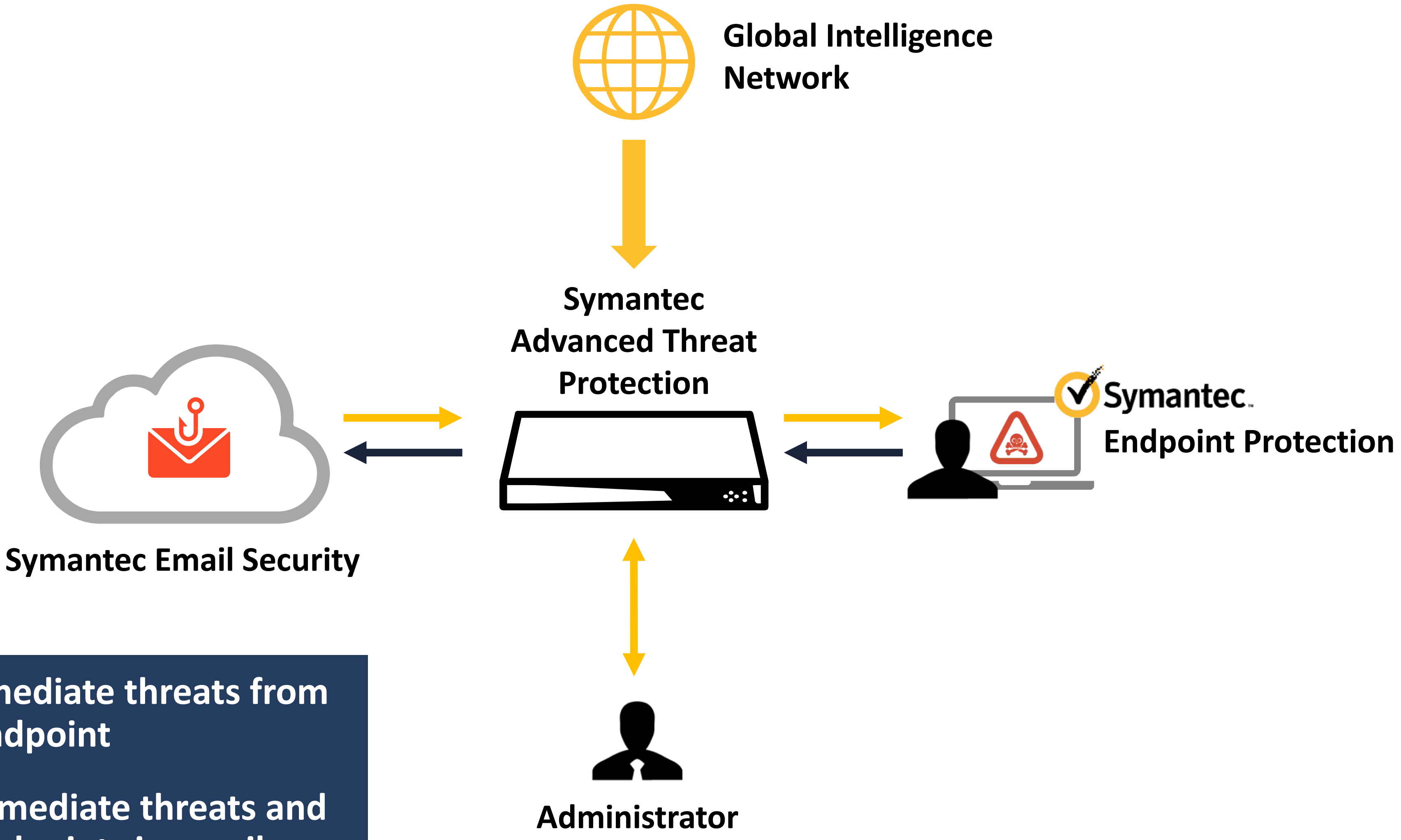
- Protect against advanced attacks in internal email and content for Office 365 apps
- Control access to apps and content

Symantec DLP

- Protect data in email and Office 365 apps



Orchestrate Response Across Emails and Endpoints

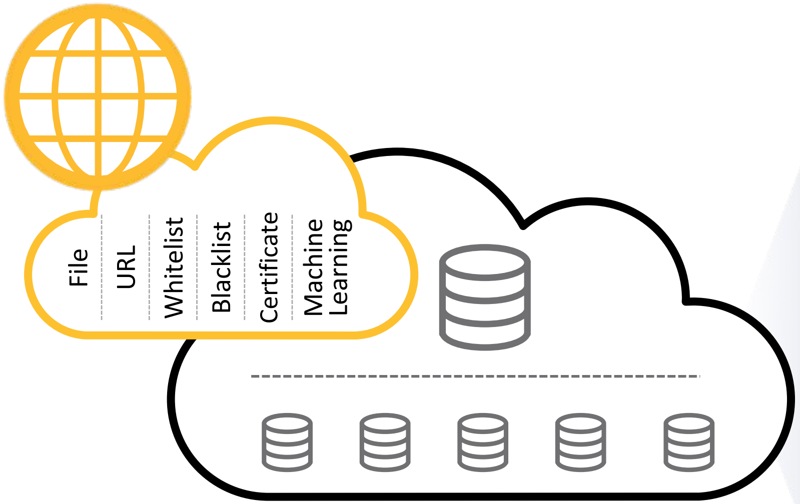

Global Intelligence Network
Symantec Advanced Threat Protection
Symantec Email Security
Symantec Endpoint Protection
Administrator

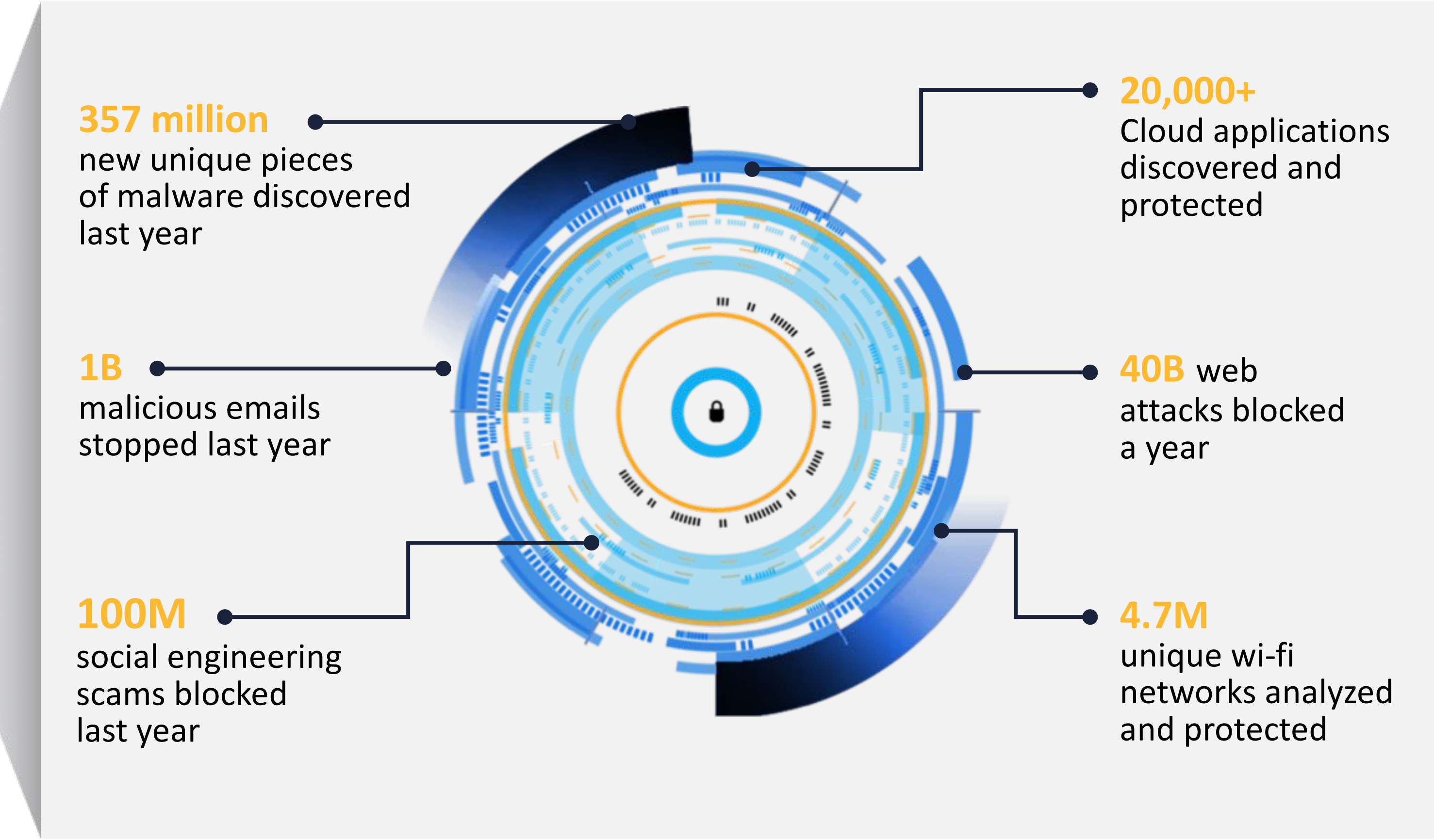
- Blacklist and remediate threats from emails on the endpoint
- Blacklist and remediate threats and attacks from endpoints in email

Why Symantec?

Symantec™

Global Threat Intelligence Network





357 million new unique pieces of malware discovered last year

1B malicious emails stopped last year

100M social engineering scams blocked last year

20,000+ Cloud applications discovered and protected

40B web attacks blocked a year

4.7M unique wi-fi networks analyzed and protected

CLOUD GLOBAL INTELLIGENCE SOURCED FROM:

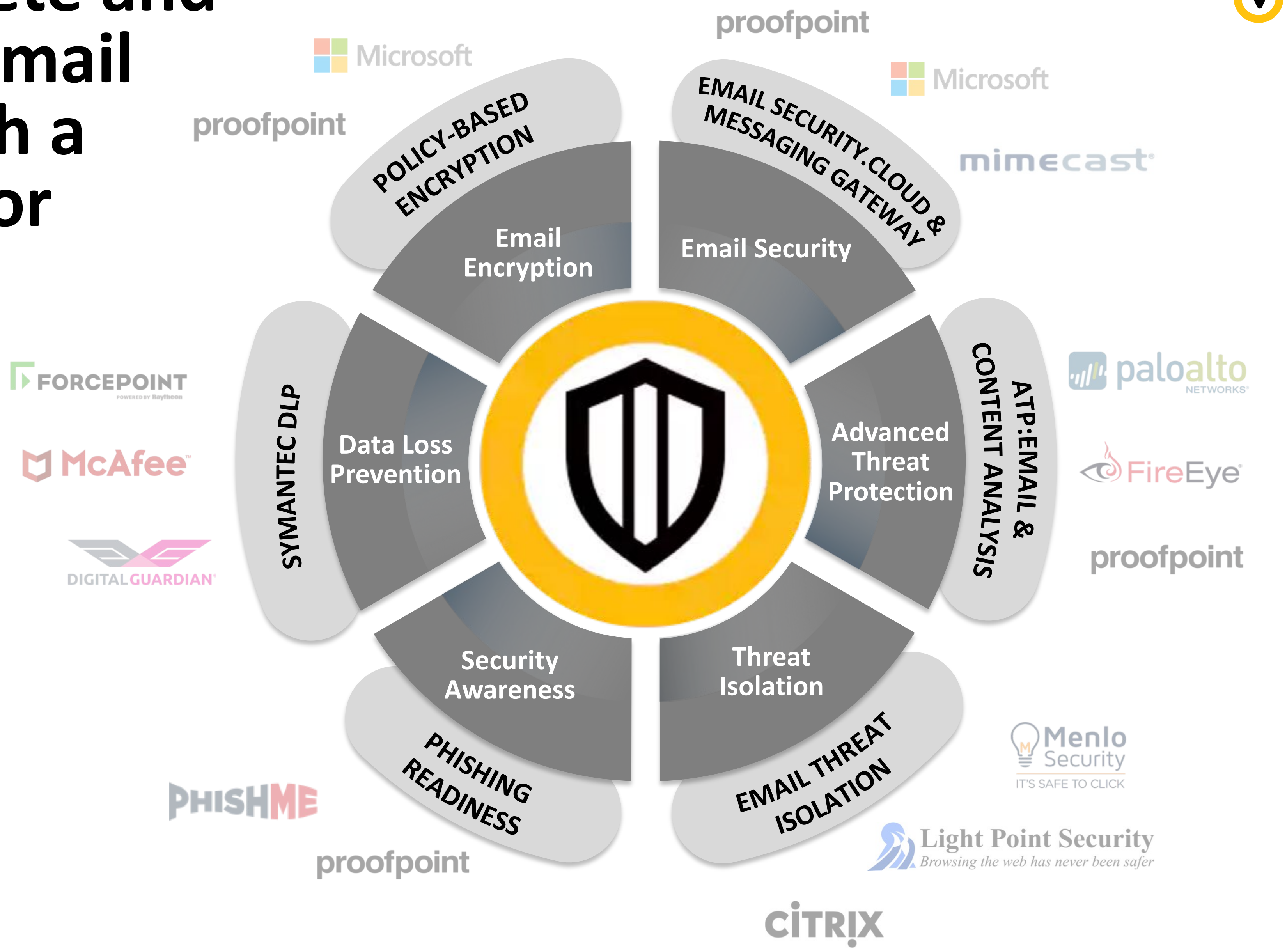
1 billion previously unseen web requests scanned daily

2 billion emails scanned per day

175 million Consumer and Enterprise endpoints protected

9 global threat response centers with **3500+** Researchers and Engineers

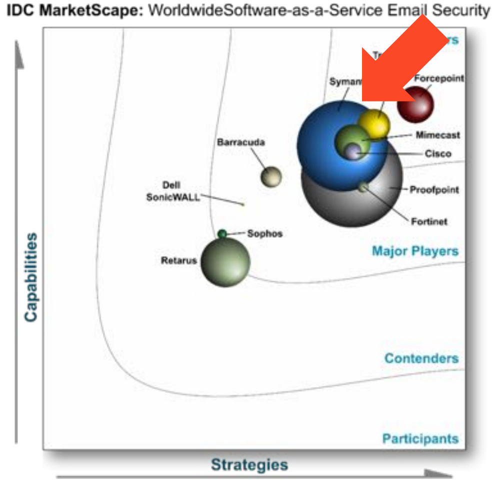
Gain Complete and Integrated Email Security with a Single Vendor



Symantec

Email Security Market Leadership

SaaS Report



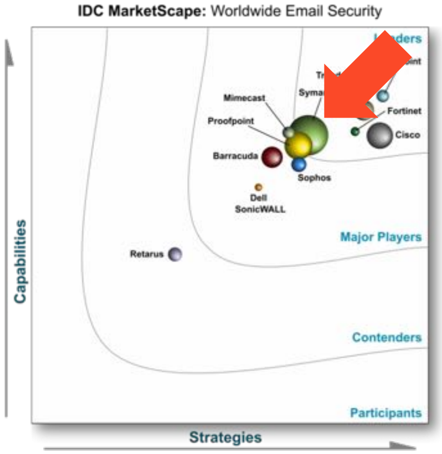
"Symantec is positioned in the Leaders category in this IDC MarketScape because of its cloud-first strategy."

- IDC MarketScape: Worldwide Software-as-a-Service Email Security 2016 Vendor Assessment

Overall Report

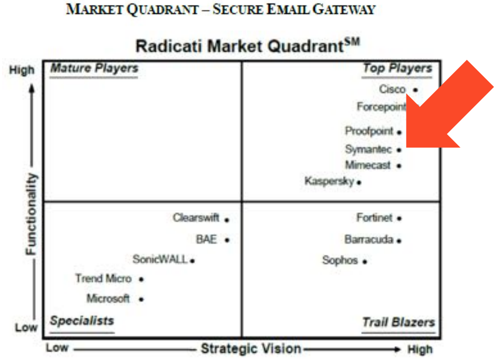
"Symantec is the overall revenue leader in messaging security and in the software-as-a-service and software on-premise categories."

- IDC MarketScape: Worldwide Email Security 2016 Vendor Assessment



Source: IDC, 2016

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM



"Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats."

- Radicati Group Secure Email Gateway Market Quadrant 2016

Complete, Multi-layered Security

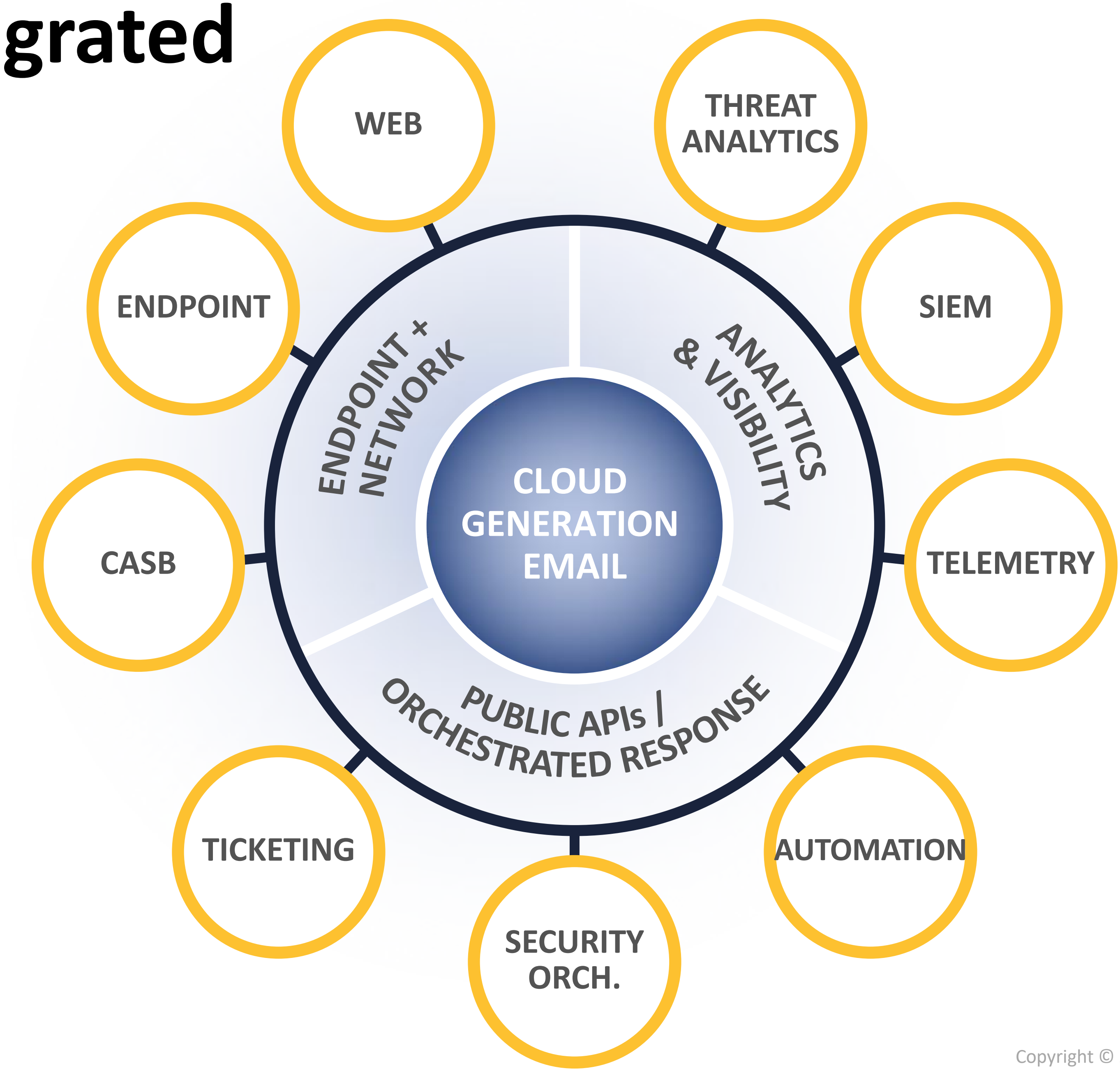
Strong Endpoint and Web Integrations

Deep Threat Visibility

Advanced DLP and Encryption

Orchestrated Threat Response

Email with Integrated Cyber Defense



The Symantec Difference

	Key Capabilities	Symantec	Proofpoint	Microsoft	Mimecast
Prevent	Link Protection	✓	⚠ (checks blacklists)	⚠ (checks blacklists)	✓
	Threat Protection Efficacy	✓	⚠ (Avg Efficacy)	✗	⚠ (Avg Efficacy)
Isolate	Comprehensive Malware Isolation (Email, Endpoint)	✓	✗	✗	✗
	Credential Phishing Protection	✓	✗	✗	✗
Respond	Advanced Threat Analytics	✓	⚠ (no clean email visibility)	✗	✓
	Multi-Vector Correlation & Response (Email, Endpoint, Web)	✓	✗	✗	✗
Prepare	Security Awareness Training	✓	✓	✗	✓
Integrate	Strongest Office 365 Security (Email, CASB, DLP)	✓	✗	⚠ (only basic DLP & CASB)	✗
	Holistic Messaging Security (Email, Slack, FB, etc.)	✓	✗	⚠ (only basic CASB)	✗

Cloud Email Security User Stories

Symantec

CLOUD EMAIL SECURITY

User Stories

Superior Protection for Office 365

Comprehensive Spear Phishing Defense

Advanced Business Email Compromise Protection

Complete Ransomware Protection

Targeted Attack Investigation and Response

Advanced Confidential Data Protection

Security Awareness & Education

Symantec™

Thank you