Net++ TECHNOLOGY

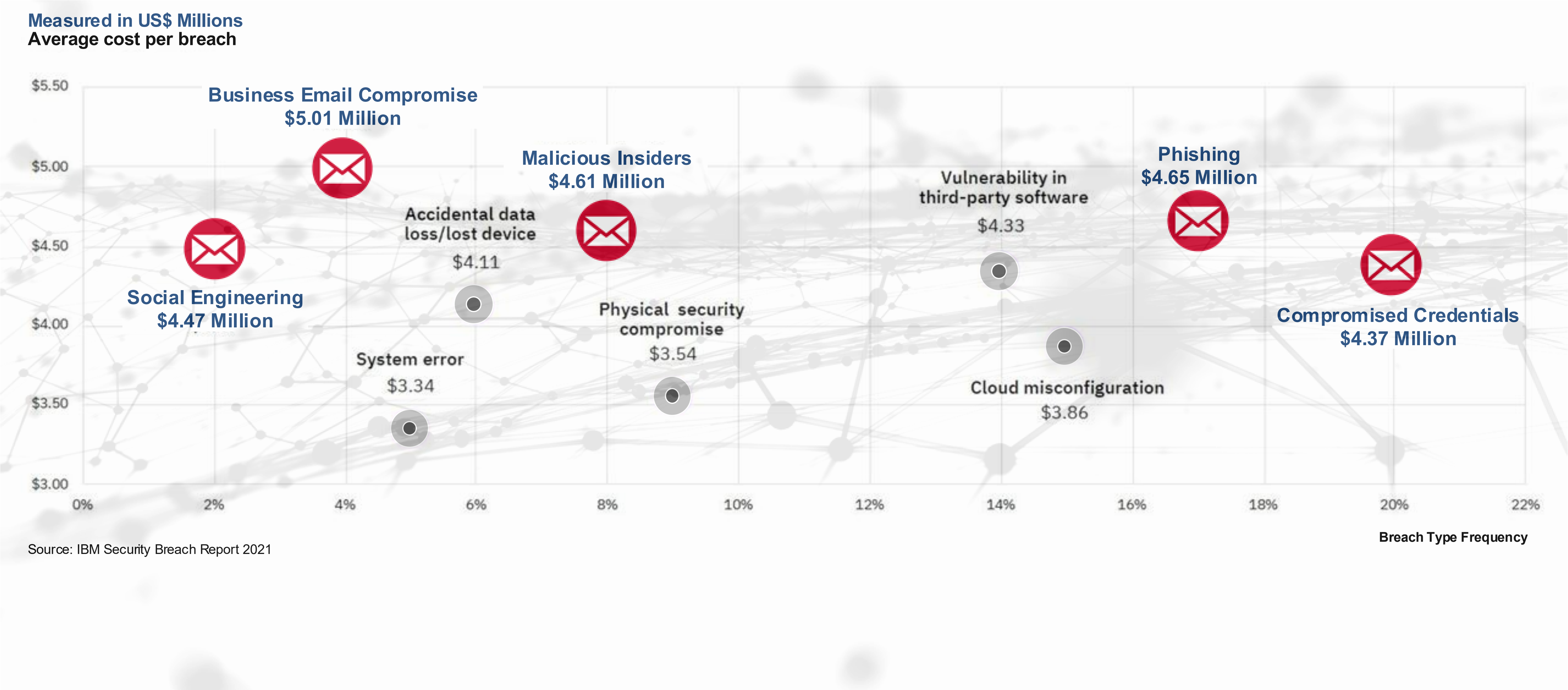
IT KLINIKA RELOADED

LOADING THREAT

Simulacija phishing napada, email zaštita, pravi alati pomažu – nije Slavica uvek kriva!

Dimitrije Veličanin

EMAIL – BR. 1 VEKTOR



Measured in US$ Millions
Average cost per breach

Source: IBM Security Breach Report 2021

Net++ TECHNOLOGY

WEB BASED NAPADI

Threat of Ever-Expanding Web

- Millions of new sites created every day
- 71% of all host names exist for 24 hours or less
- Many are legitimate, but some offer ideal cover for hackers launching attacks

Web Browsers Being Targeted

- Infection by simply visiting a site
- Web browser vulnerabilities open the door to malware Strains “detection only” based approaches

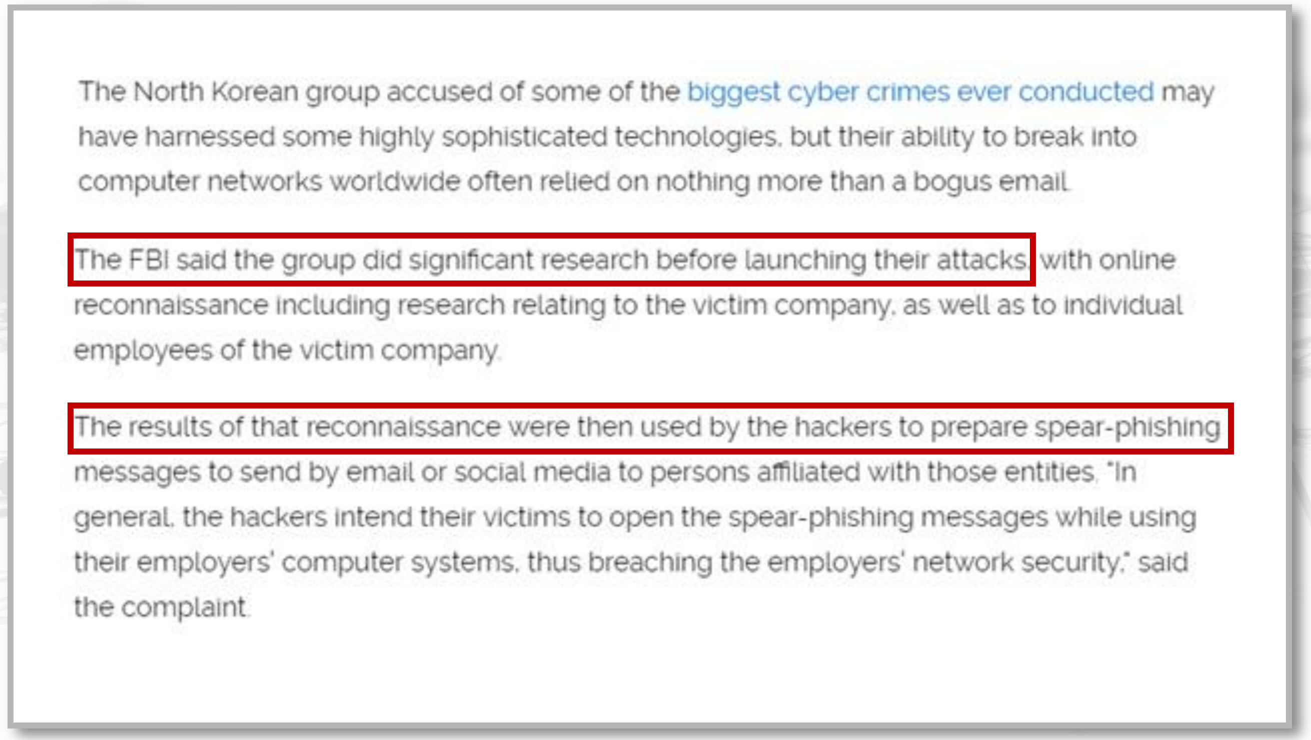
Downloading Files

- Advanced zero-day malware
- Designed to overcome less sophisticated malware
- Battle between detection false-positive rates

PHISHING NAPADI

36% of breaches used phishing[1]

85% of breaches involved the human element



The North Korean group accused of some of the biggest cyber crimes ever conducted may have harnessed some highly sophisticated technologies, but their ability to break into computer networks worldwide often relied on nothing more than a bogus email.

The FBI said the group did significant research before launching their attacks with online reconnaissance including research relating to the victim company, as well as to individual employees of the victim company.

The results of that reconnaissance were then used by the hackers to prepare spear-phishing messages to send by email or social media to persons affiliated with those entities. "In general, the hackers intend their victims to open the spear-phishing messages while using their employers' computer systems, thus breaching the employers' network security," said the complaint.

Users are seen as the weak link in the security chain

POSLEDICE

- Prekid rada
- Gubitak reputacije
- Gubitak prava intelektuale svojine
- Gubitak podataka kupaca
- Finansijski gubici
- Pravke i regulativne posledice

Net++ TECHNOLOGY

SLAVICA

- tipičan zaposleni
- prošla cybersecurity obuku (ali...)
- posla preko glave
- veruje da IT ne radi ništa po ceo dan
- veruje da IT samo smeta i izmišlja nešto
- vredna, radna, ali nije baš da voli računare

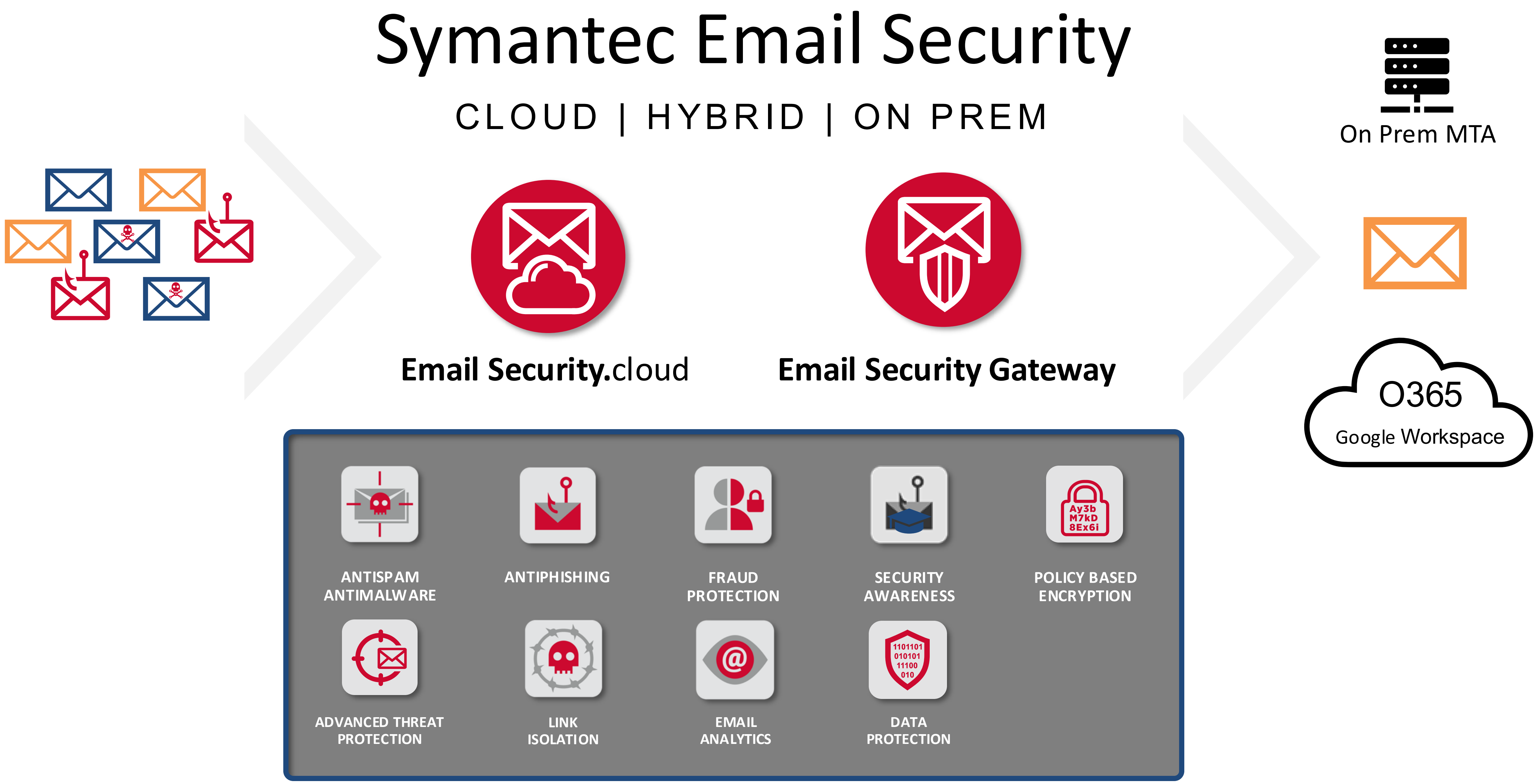
jedan radni dan

Net++ TECHNOLOGY

KAKO TO STVARNO IZGLEDA (DEMO)?

- pisanje email-a za Slavicu sa “phishing” stranom www.cyber-security.rs/login
- kako nezaštićeni korisnik ostavlja podatke na toj strani
- Slavica otvara oba email klijenta - jedan email ide preko Symantec sistema, drugi ne
- otvaranje emaila sa zasticenog netpplab domena i prikaz izolovane adrese linka, kao i izolovane web strane
- prikaz loga u Email Sec. konzoli gde se vidi da je link izolovan
- prikaz podesavanja u konzoli za Email izolaciju
- otvaranje emaila sa nezaštićenog cyber-security.rs domena i pokušaj unosa kredencijala
- prikaz blokade od strane PAN NGFW, email notifikacije i loga u PAN konzoli
- prikaz PAN podesavanja za Credential Theft

SYMANTEC EMAIL SECURITY



Symantec Email Security

CLOUD | HYBRID | ON PREM

Email Security.cloud

Email Security Gateway

On Prem MTA

O365

Google Workspace

ANTISPAM ANTIMALWARE

ANTIPHISHING

FRAUD PROTECTION

SECURITY AWARENESS

POLICY BASED ENCRYPTION

ADVANCED THREAT PROTECTION

LINK ISOLATION

EMAIL ANALYTICS

DATA PROTECTION

Symantec™ by Broadcom

Net++ TECHNOLOGY

SYMANTEC EMAIL SECURITY

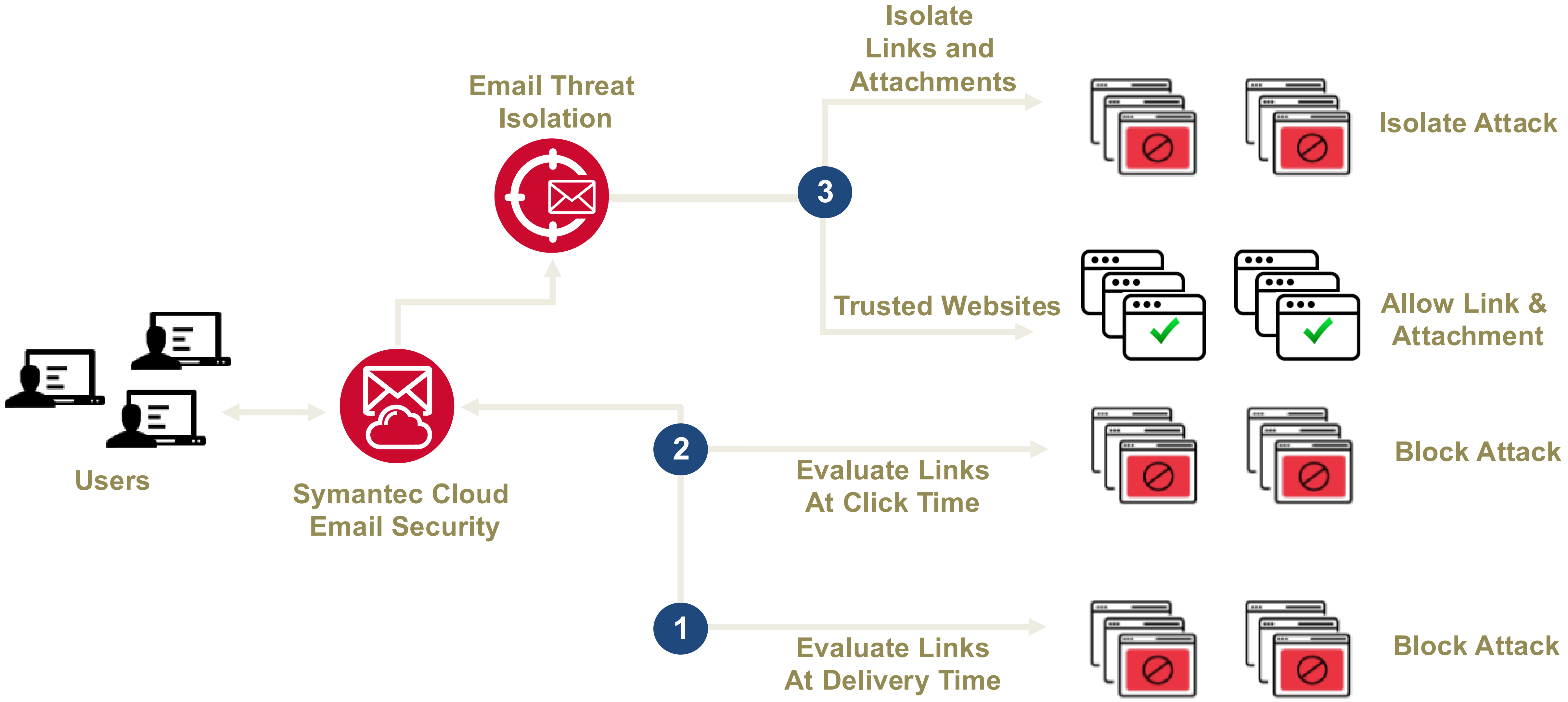
Global Intelligence Network

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		

Symantec by Broadcom

SYMANTEC EMAIL SECURITY

URL isolation eliminates the window of vulnerability

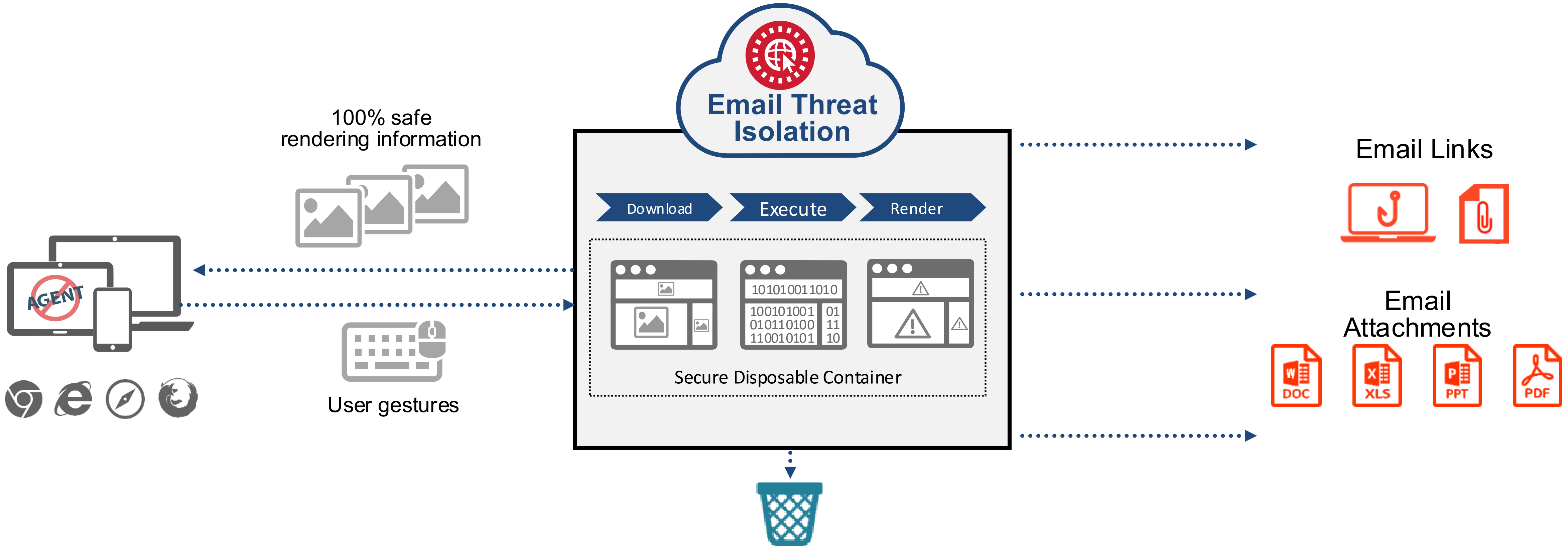


Symantec by Broadcom

Net++ TECHNOLOGY

SYMANTEC EMAIL SECURITY

Prevent Even the Most Advanced Attacks



- Defends users from spear phishing attacks by isolating suspicious links
- Prevents ransomware attacks from infecting users by isolating malicious attachments

Symantec by Broadcom

Net++ TECHNOLOGY

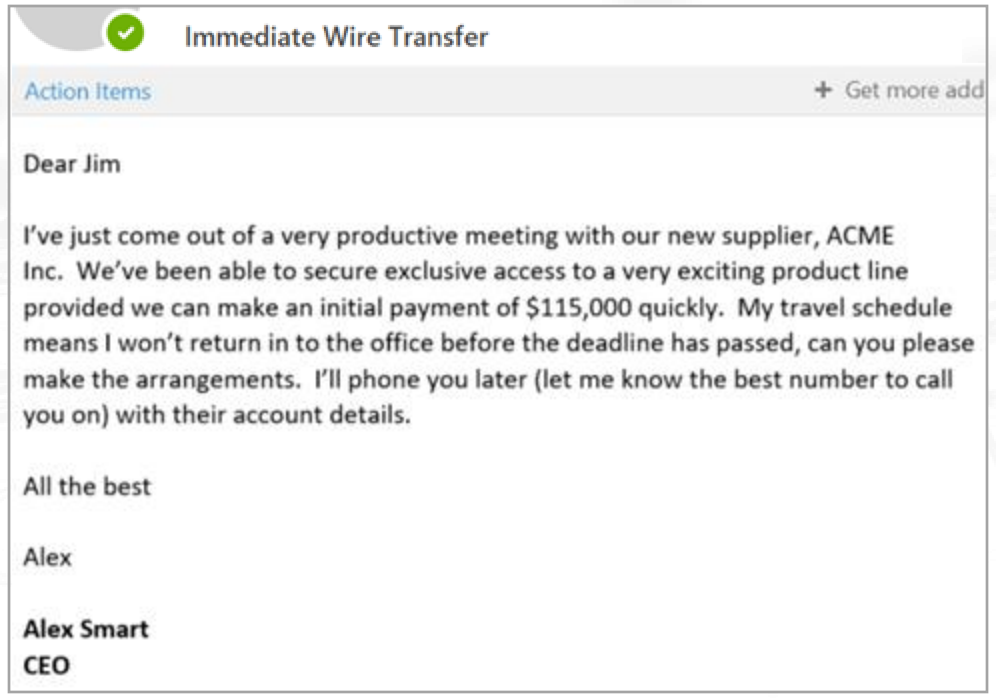
SYMANTEC EMAIL SECURITY

Issue: Business Email Compromise (Impersonation)

The Email Itself Isn't Malicious, What You're Being Asked to Do Is!

Types of Attacks:

- You receive an email from your CEO asking you to **make a wire transfer**
- You're asked to **provide tax data**, which may be used to orchestrate future attacks or perform fraud
- You're involved in a real estate transaction and asked to **change payment type** to a fake account



Immediate Wire Transfer

Dear Jim

I've just come out of a very productive meeting with our new supplier, ACME Inc. We've been able to secure exclusive access to a very exciting product line provided we can make an initial payment of $115,000 quickly. My travel schedule means I won't return in to the office before the deadline has passed, can you please make the arrangements. I'll phone you later (let me know the best number to call you on) with their account details.

All the best

Alex

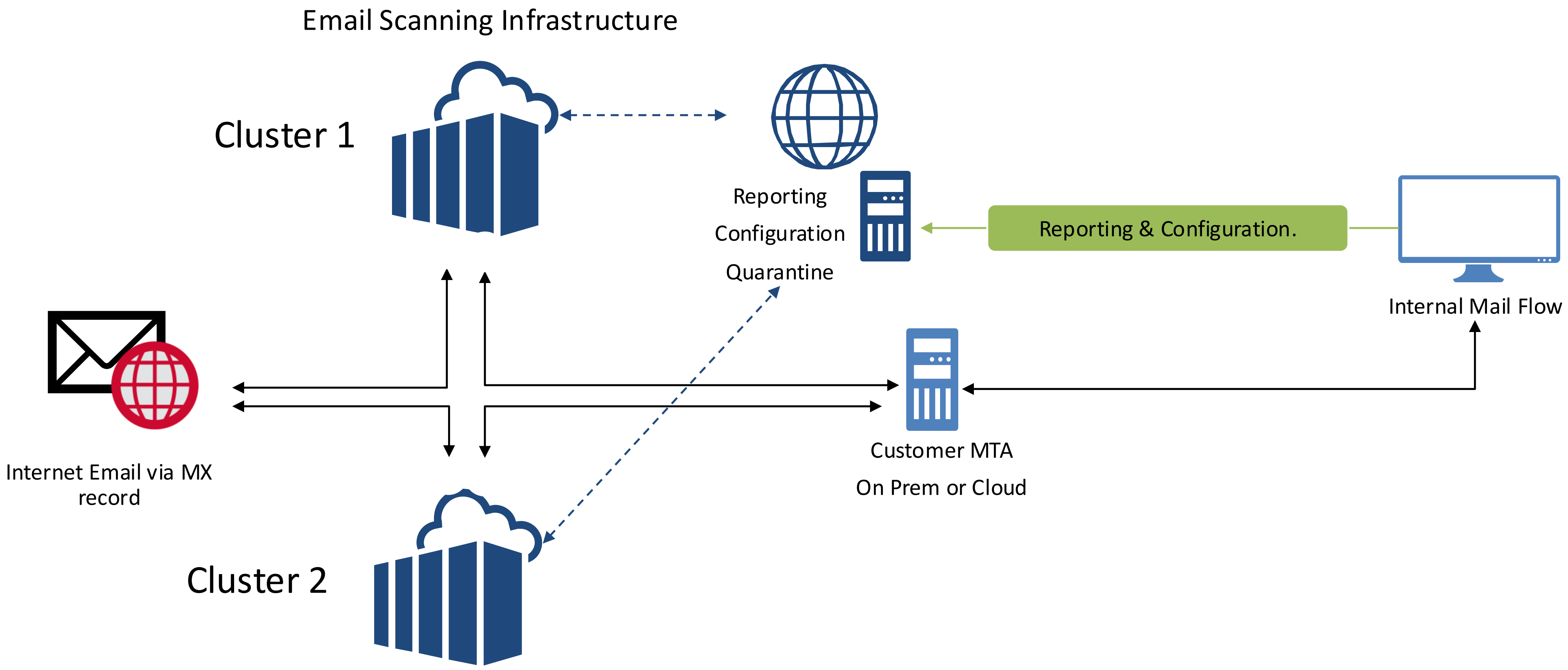
Alex Smart
CEO

Business Email Compromise scams cost = $43 Billion (2016-2021)

Source: Business Email Compromise and Real Estate Wire Fraud, Congressional Report, FBI 2022

SYMANTEC EMAIL SECURITY

Basic Cloud Architecture

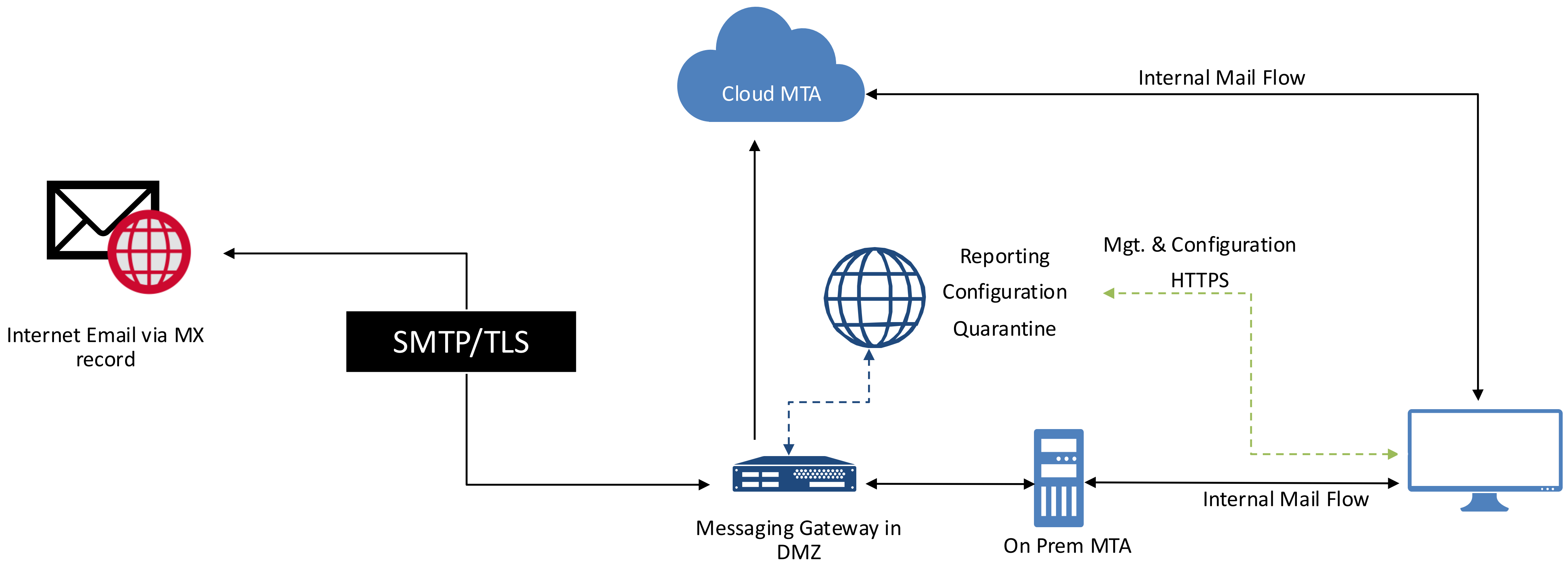


Symantec by Broadcom

Net++ TECHNOLOGY

SYMANTEC EMAIL SECURITY

Basic On Prem Architecture



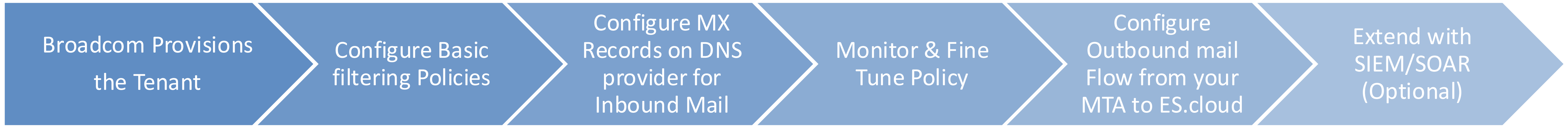
🟦 Symantec Software / Component

🟦 3rd party components

Symantec by Broadcom

SYMANTEC EMAIL SECURITY

Steps to implement Email Security.cloud



1. Broadcom Provisions the Tenant
2. Configure Basic filtering Policies
3. Configure MX Records on DNS provider for Inbound Mail
4. Monitor & Fine Tune Policy
5. Configure Outbound mail Flow from your MTA to ES.cloud
6. Extend with SIEM/SOAR (Optional)

Configure Microsoft Office 365 and Symantec.cloud for outbound mail

Configure Microsoft® Office 365™ for inbound mail

Symantec™ by Broadcom

Net++ TECHNOLOGY

PITANJA?

Net++
TECHNOLOGY

HVALA NA PAŽNJI

+381 11 36999 967
www.netpp.rs
Otokara Keršovanija 11/39, Beograd