E-MAIL SECURITY

AGENDA

- INTRODUCTION
- COMPONENTS AND FEATURES
- IMPLEMENTATION AND DEPLOYMENT
- DMARC
- ENCRYPTION
- Q&A

NTS

SECURE E-MAIL

NTS

INTRODUCTION

- SMTP is a language
- old but gold protocol
- new technology still did not replace SMTP
- It just works

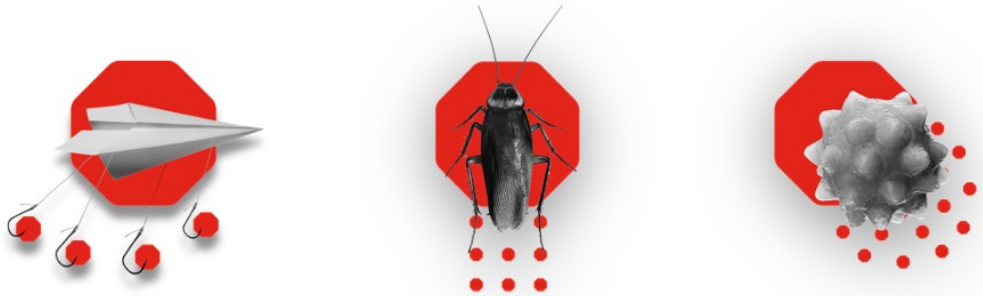
- SMTP relies on third party for security
- threats continue to evolve, so must the security layer

SECURE E-MAIL

NTS

INTRODUCTION

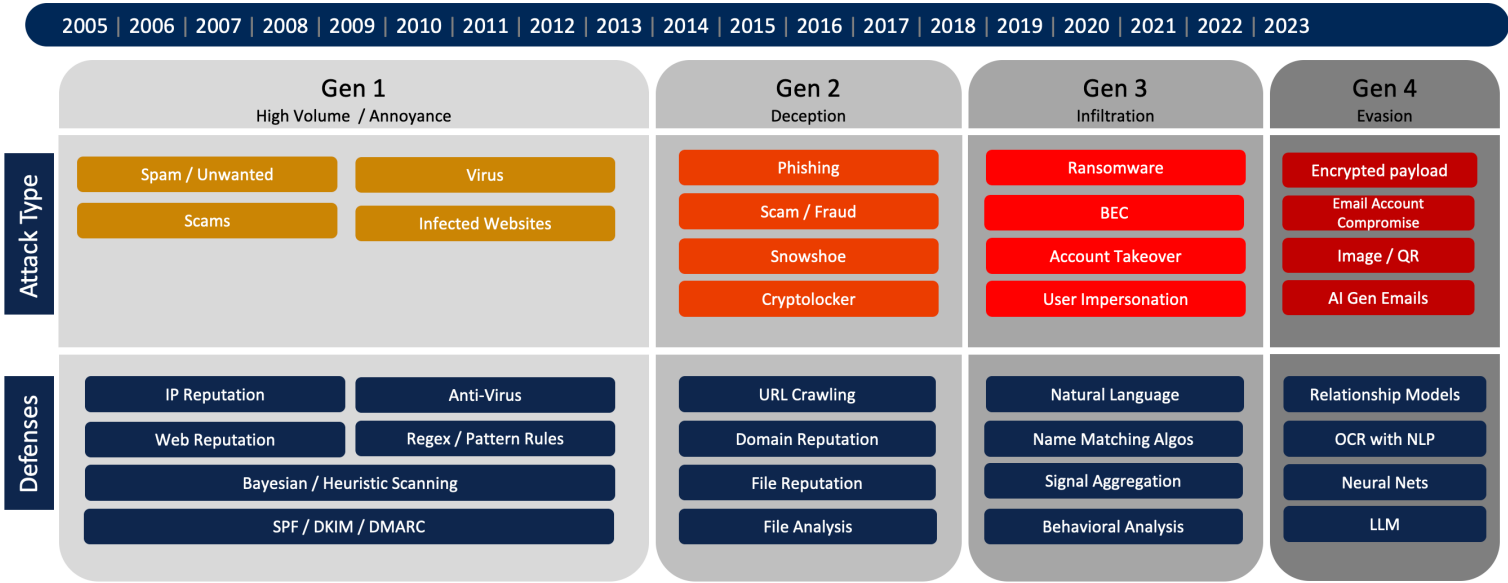
Email is still the #1 threat vector



SECURE E-MAIL

NTS

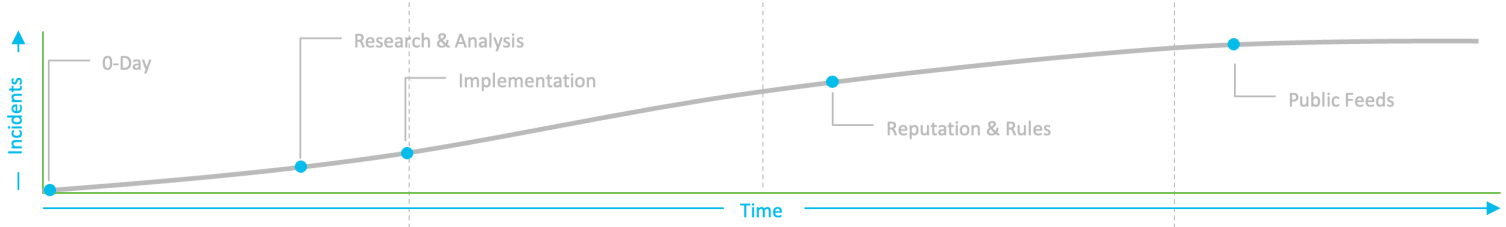
THREAT LANDSCAPE



SECURE E-MAIL

NTS

THREAT LIFE CYCLE



Unknown / Targeted	Emerging	Known	Widely Known
Relationship Models	Malware Analytics	Sender IP Reputation	Public Threat Feeds / VirusTotal
Natural Language Understanding	Cloud URL Analysis	Domain Reputation	STIX/TAXII Subscriptions
Phishing Models	Algorithm Matching	Web Reputation, Category	
BEC Models		File Reputation	
		Sender Authentication (DMARC, SPF)	
		Anti-Spam & Graymail	
		Anti-Virus	

SECURE E-MAIL

NTS

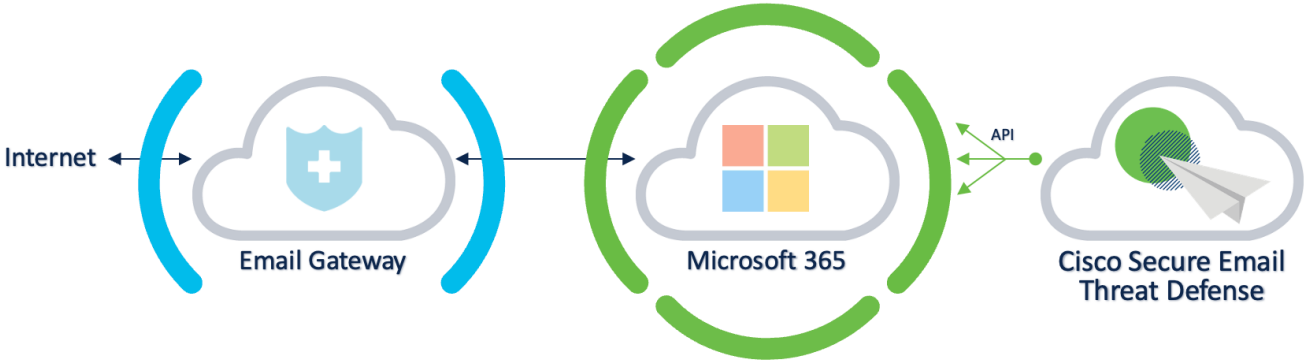
COMPONENTS

Secure Email Gateway

Modifies and filters **inbound** and **outbound** messages that cross the perimeter

Cisco Secure Email Threat Defense

Has complete visibility of **inbound**, **outbound and internal** messages



SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY

- IronPort ♡
- traditional gateway
- granular controls
- feature rich
- reliable performance
- flexible deployment

SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY

Connection and Content Filtering				Virus & Malware Filtering		
Reputation Filtering	SDR	Connection Filtering	CASE	Anti-Virus	File Reputation	File Analysis
Host and IP filtering via SBRS & ETF	Domain reputation filtering	Throttling, SPF, DKIM & DMARC	Multi-verdict scanning	Block known viruses	SHA-based file blocking	File types, behavioral indicators, sandboxing

Content Filtering		Anti-Phishing	
Graymail Detection	Content Filtering	Outbreak Filtering	**Threat Defense Connector**
Control marketing, social and bulk	Admin driven rules (ETF & FED)	9-12 hr lead time on zero-day outbreaks	Metadata & behavioral analytics

SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY

Advanced Malware Protection

- Block known malware
- Examine files with context-driven analysis
- Auto-remediate threats in O365
- Gain visibility into messages trying to enter or leave the network

File reputation

Fuzzy fingerprinting

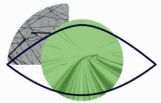
Indications of compromise

Known signatures

File sandboxing

- Advanced analytics
- Dynamic analysis
- 846+ indicators

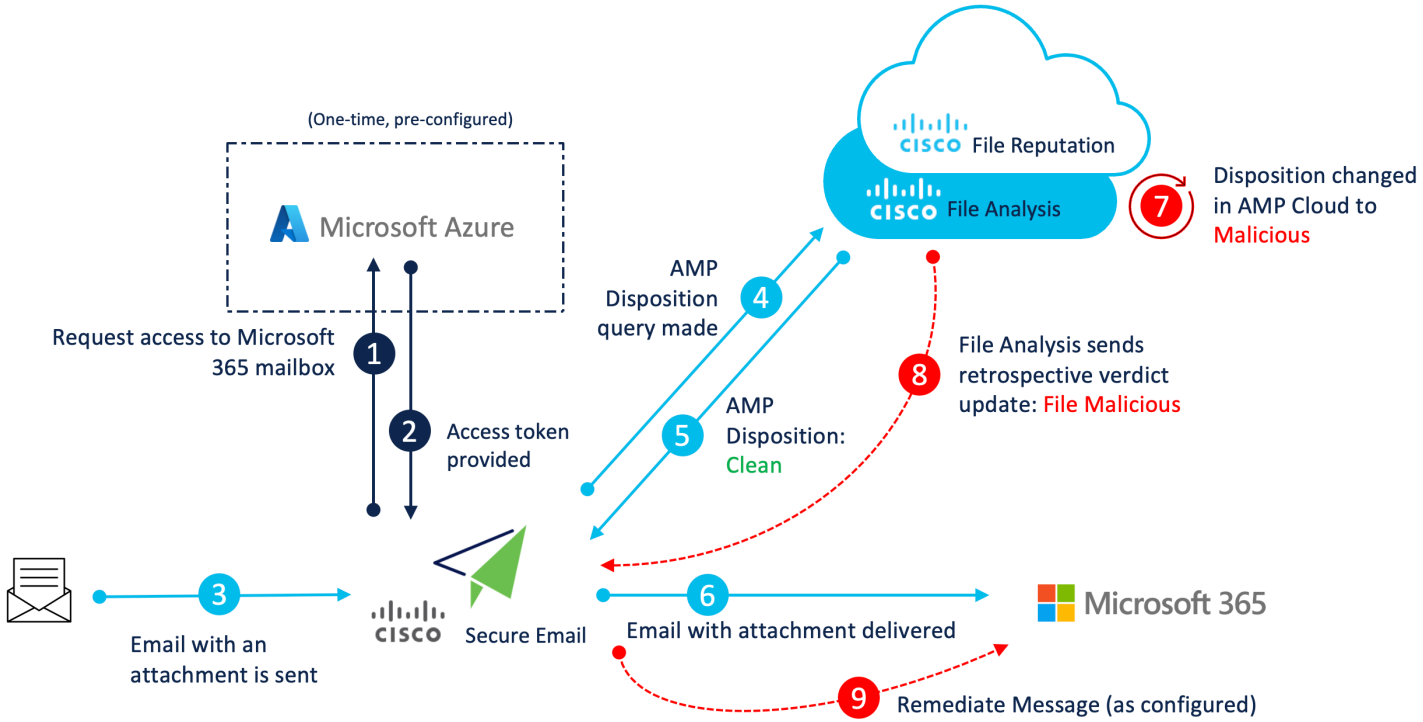
File retrospection



SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY



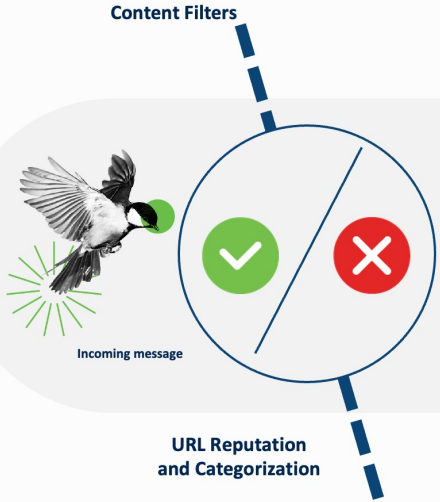
SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY

Content Filters

- Customize filters in three different ways for additional security
- Complete visibility of user interaction
- Easily enforce business and compliance policies



URL Filtering

Rewrite URL	Cisco Cloud Web Proxy
Defang / Block	BLOCKEDwww[.]proxy[.]orgBLOCKED
Replace with text	"This URL is blocked by policy"

SECURE E-MAIL

NTS

CISCO SECURE EMAIL GATEWAY

Forged Email Detection

- Inspect SMTP envelope for True sender address
- Match sender address against company directory
- Send appended mail to warn users of potential forgery
- Record a log of attempts and actions taken

Pre-processing

From: Chuck chuck.robbins@mail.com

Subject: [URGENT]

Need help transferring funds

Inspects the SMTP envelope address

$ telnet mail-smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to mail-smtp-in.l.mail.com.
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 – gsmtp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM:adam@outside.com
250 2.1.0 OK i11si22058766wmh.67 - gsmtp

Post-processing

From: adam@outside.com

Subject: {Possibly Forged} [URGENT]

Need help transferring funds

Compare against Company directory

- Allison Johnson
- Barry Smith
- Chuck Robbins
- Dave Tucker

SECURE E-MAIL

NTS

CISCO SECURE EMAIL THREAT DEFENSE

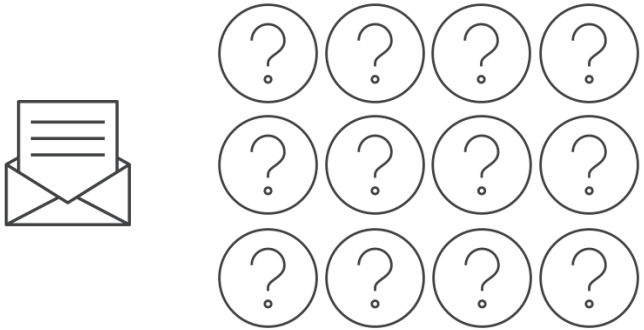
- SaaS solution
- AI, Machine and Deep Learning
- visibility to incoming, outgoing and internal messages
- focusing on Microsoft 365 and Hybrid Exchange
- context and relationship driven
- simple implementation

SECURE E-MAIL

NTS

CISCO SECURE EMAIL THREAT DEFENSE

Content vs Context



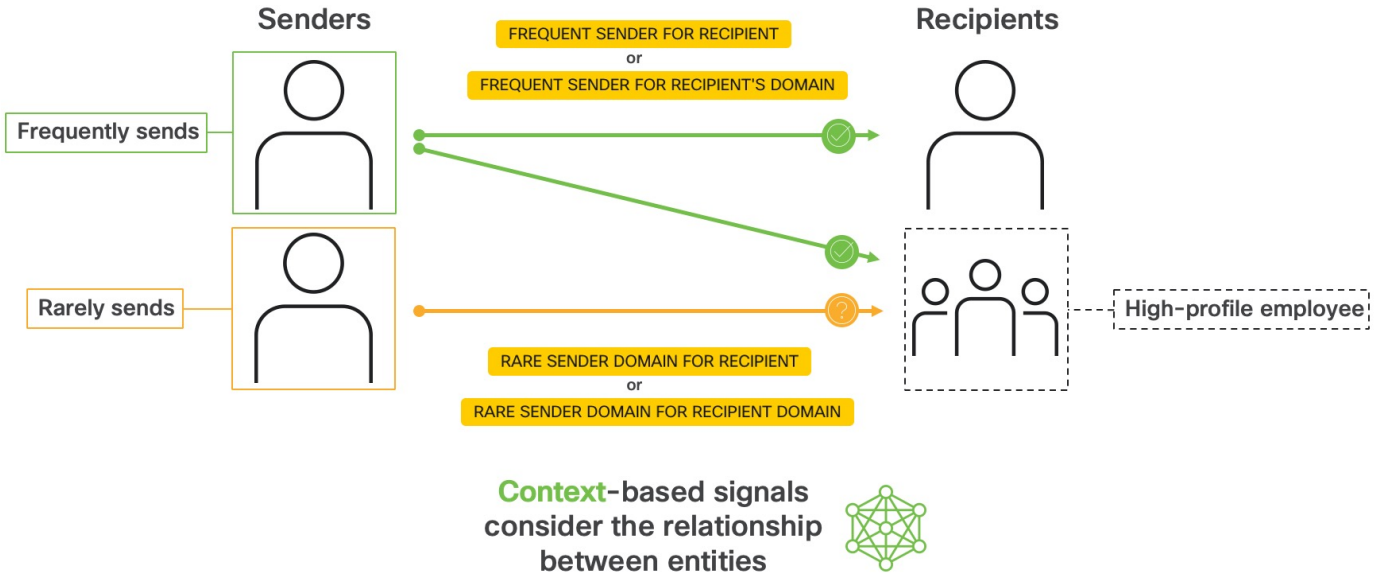
Content-based signals analyze the individual email

Context-based signals consider the relationship between entities

SECURE E-MAIL

NTS

CISCO SECURE EMAIL THREAT DEFENSE

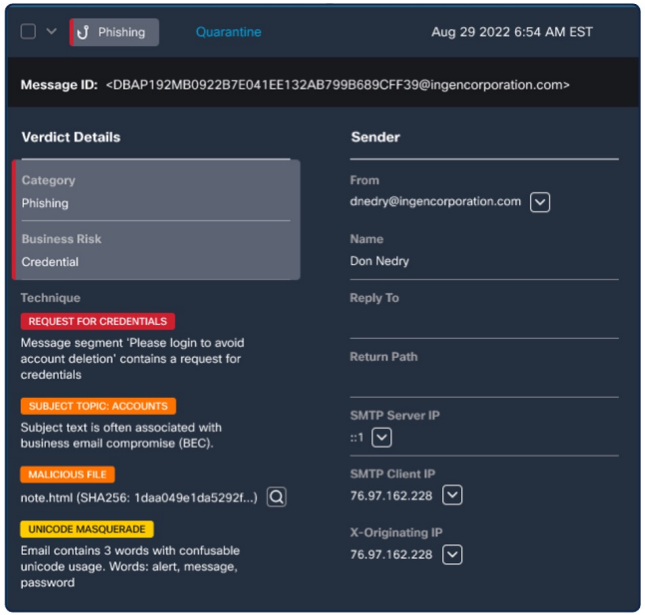


SECURE E-MAIL

NTS

CISCO SECURE EMAIL THREAT DEFENSE

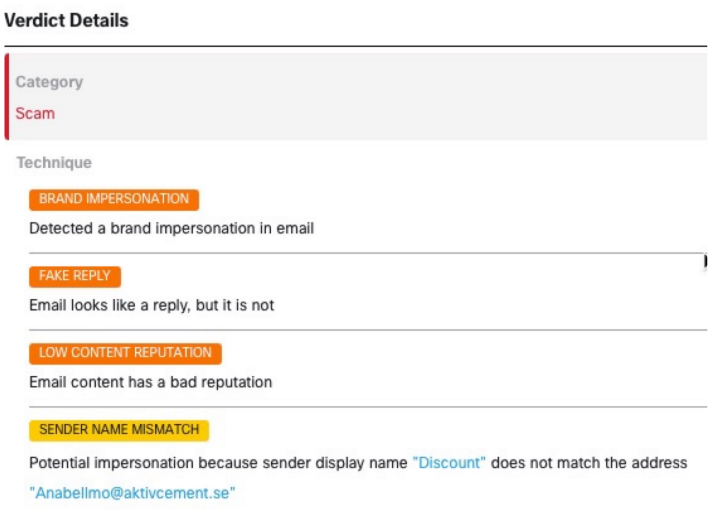
Graymail	Marketing	Social	Bulk	Spam
Spam	Junk	Win Big	Bot / DGA	Education
	Adult	Pharma	Reputation	Job / Offer
Scam	Fraud	Advance Fee	Fake Company	ATO
	Extortion	Charity	Romance	Investment
	Lottery	Employment	Inheritance	Money Mule
Phishing	Credential	Financial	Doc Share	Forgery
Business Email Compromise	Identity	Brand	Spoof/Cousin	ATO (external)
	Compromise	Payroll	Gift Card	Wire Transfer
	M & A	Invoice		
Malware	Ransomware	Cred Stealer	Crypto Miner	Ad/Spyware
	Malicious URL	Bot/Phish Kit	Viral	Trojan / CNC

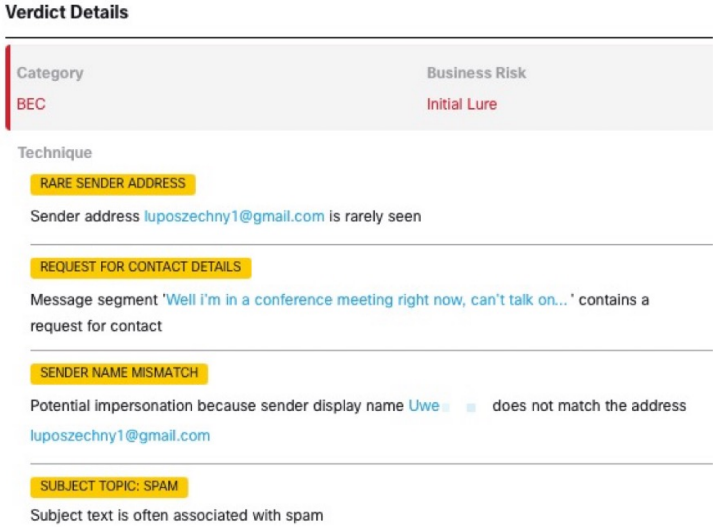


SECURE E-MAIL

NTS

CISCO SECURE EMAIL THREAT DEFENSE

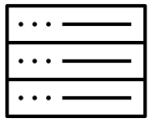




SECURE E-MAIL

NTS

DEPLOYMENT



On-Premises

Hardware or Virtual Machines

Cisco Secure Email Gateway

Hybrid

Best of both worlds

Cloud

Agile, Scalable, Secure

Cisco Secure Email Cloud Gateway

Cisco Email Threat Defense

SECURE E-MAIL

NTS

ENCRYPTION WITH KITEWORKS EPG

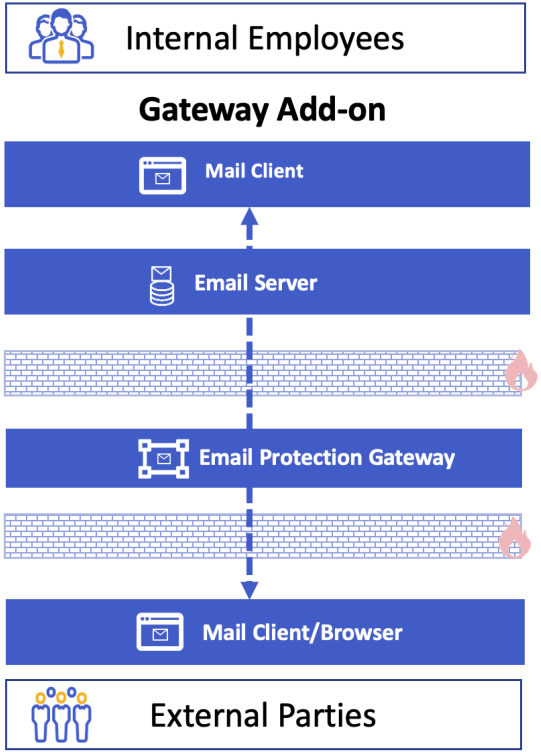
- Email Protection Gateway Addon
- SMTP hop
- securing information communication
- utilizing S/MIME and OpenPGP standards
- B2B and internal encryption
- enterprise owns the keys, not vendors and not users
- automated policy driven encryption for seamless user experience
- public CA integration
- hardened virtual appliances

Kiteworks

SECURE E-MAIL

NTS

KITEWORKS ENCRYPTION – USE CASE: EXTERNAL



Transparent as part of native email client with automatic coverage.

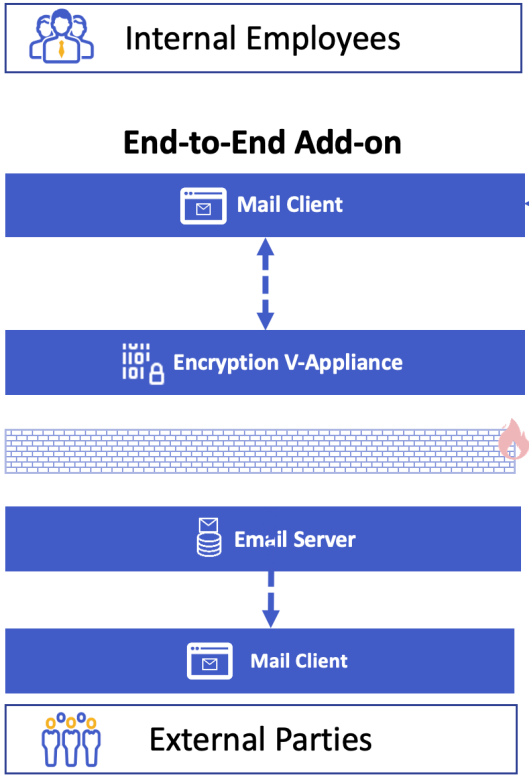
EPG checks for policy for given recipient

Mail client decrypts S/MIME, TLS, OpenPGP protocols.
encrypted HTML if other methods unavailable

SECURE E-MAIL

NTS

KITEWORKS ENCRYPTION – USE CASE: END TO END



The message is encrypted via S/MIME directly in the sender's email client – keys and certificates are automatically collected and managed.

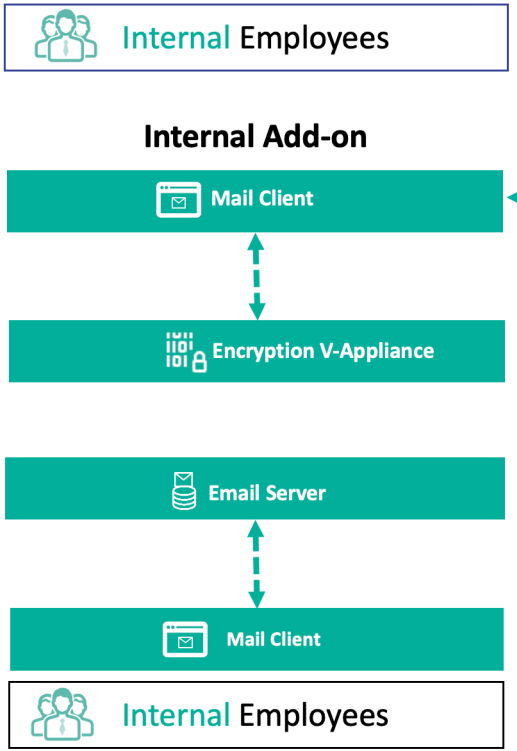
No interruption to decrypt/scan the message content. Maintains highest level of privacy protection.

Decrypted with client S/MIME protocol.

SECURE E-MAIL

NTS

KITEWORKS ENCRYPTION – USE CASE: INTERNAL



The message is encrypted via S/MIME directly in the sender's email client – keys and certificates are automatically collected and managed.

No interruption to decrypt/scan the message content. Maintains highest level of privacy protection.

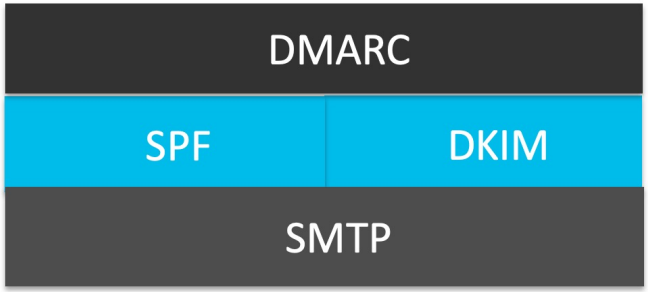
Decrypted with client S/MIME protocol.

SECURE E-MAIL

NTS

DMARC

- Domain based Message Authentication, Reporting and Conformance
- released 2012
- secure your domain
- utilization of SPF, DKIM and DMARC
- open protocol

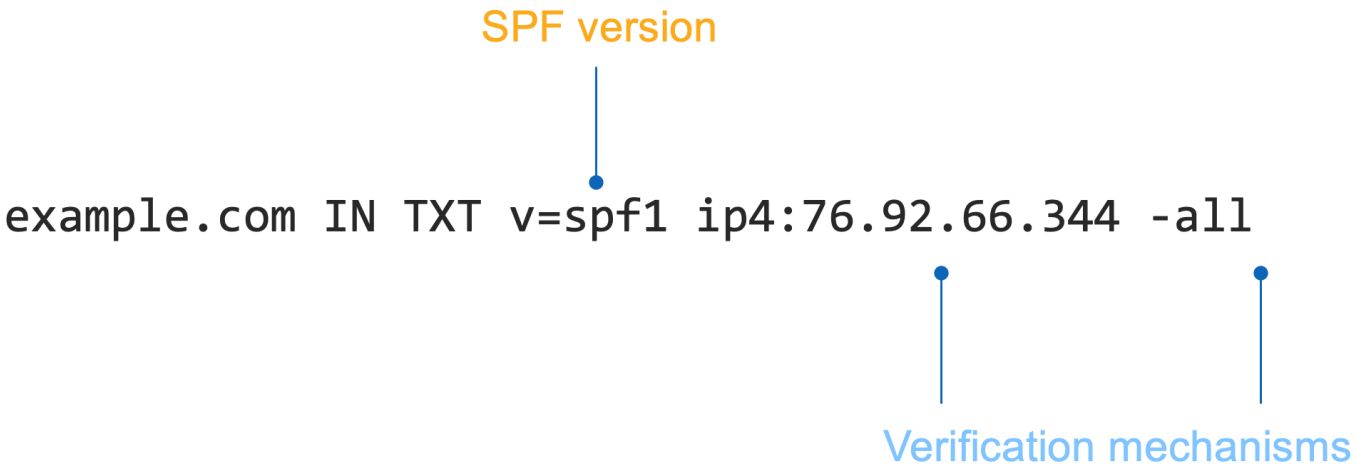


DMARC builds on the existing SPF and DKIM standards whilst introducing three important concepts:

1. **Alignment** - any domain authenticated by SPF or DKIM must match those of the From domain;
2. **Reporting** - mailbox providers can report to domain owner's sender level detail such as IP range and authentication status;
3. **Policy** - domain owners can specify the action an email receiver should take if authentication did not occur - options include None, Quarantine and Reject.

NTS

SENDER POLICY FRAMEWORK (SPF)



SECURE E-MAIL

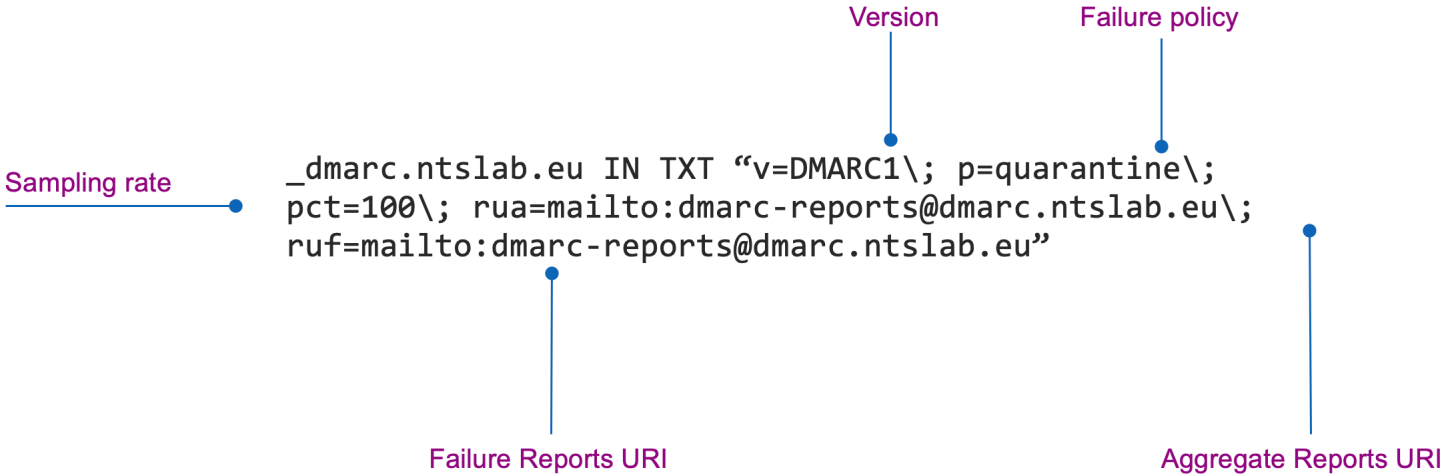
NTS

DOMAIN KEYS IDENTIFIED MAIL (DKIM)

SECURE E-MAIL

NTS

DMARC POLICY



SECURE E-MAIL

NTS

MOVING TO DMARC

- combine results of SPF and DKIM evaluation
- DMARC needs SPF or DKIM to pass
- set DMARC record in DNS to receive reports
- evaluate reports through tool to get visibility
- work through tool to only allow valid messages
- set DMARC policy to reject

SECURE E-MAIL

NTS

KEY TAKEAWAYS

- SMTP is as relevant as always
- Phishing, BEC, Malware, etc. will never stop
- E-Mail Security is a major first layer of defense
- significant cost-value ratio if done right
- new technology challenges old practices
- use AI to battle AI
- increasing requirement for encryption due to compliance
- start your DMARC journey

221 GOODBYE