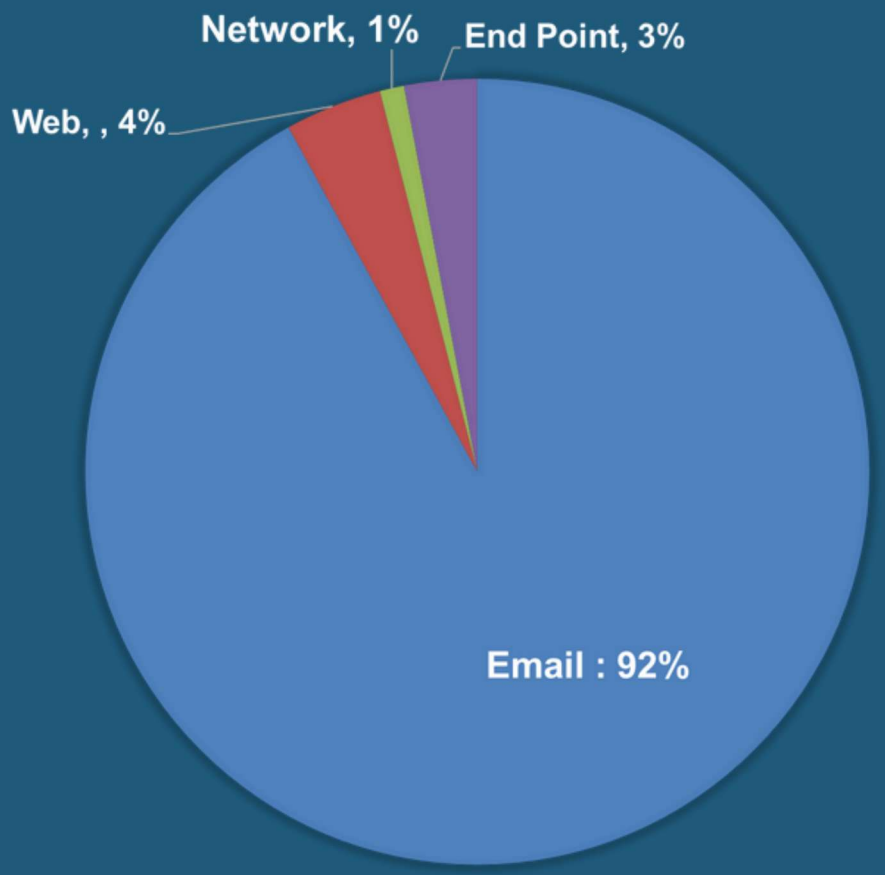
MAIL ARMOR

EMAIL SECURITY

SECURING YOUR DIGITAL WORLD

EMAIL IS STILL THE #1 THREAT VECTOR



INDUSTRY SPENDING IS NOT ALIGNED WITH THE THREATS

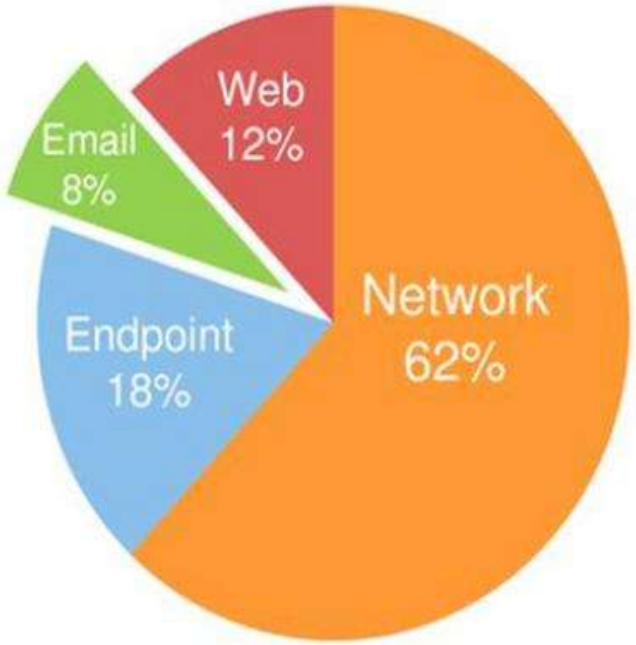
Attack Vectors

90%

of sophisticated attacks target people, largely via email

Source: Verizon DBIR, Trend Micro, FEYE, etc.

Budget spending



Source: Gartner

MAIL ARMOR THREAT DETECTION CAPABILITIES

URL Filtering

Attachment Scanning

Domain Spoofing

IP Reuptation Filtering

SPAM/ Malware (Viruses, Worms, Trojans)

Gray Mail

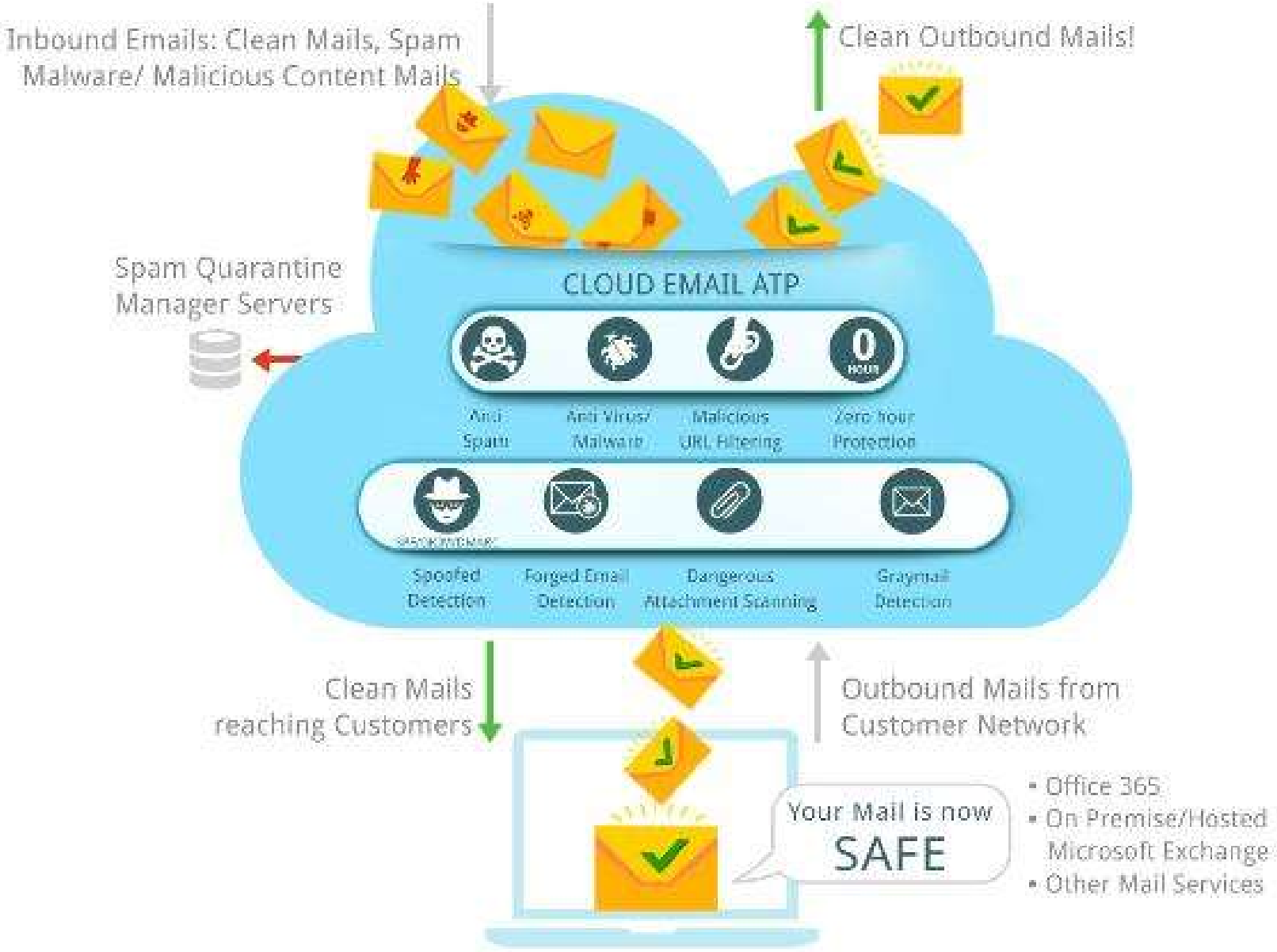
Phishing

Quishing

Ransomware

Forged Email Business Email Compromise

HOW IT WORKS


Inbound Emails: Clean Mails, Spam
Malware/ Malicious Content Mails
Clean Outbound Mails!
Spam Quarantine
Manager Servers
CLOUD EMAIL ATP
Anti Spam
Anti Virus/ Malware
Malicious URL Filtering
Zero hour Protection
Spoofed Detection
Forged Email Detection
Dangerous Attachment Scanning
Graymail Detection
Clean Mails
reaching Customers
Outbound Mails from
Customer Network
Your Mail is now
SAFE
• Office 365
• On Premise/Hosted Microsoft Exchange
• Other Mail Services

THREAT MATRIX

Threats	Detections	Present Actions
IP Reputation Filtering	Poor Reputed Ips	Email Rejects at SMTP Handshake
	Neutral Reputed Ips	Email is Accepted with Throttling and will follow further detections
	Good Reputed Ips	Email is Accepted and will follow further detections actions
Spam	Positively-Identified Spam	Quarantine the Email
	Suspected Spam	
Malware	Virus Infected Messages	Strip the infected attachment, Tag the Subject line & Quarantine the Email
	Advance Malware (Positive)	
	Advance Malware (Unknown / Suspicious)	
	Outbreak / ZeroHour (Threat Level "1" & Above)	
Graymail	Marketing	Quarantine the Email
	Social	
	Bulk	
Sender Authentication	SPF Failed Emails (i.e., fail / hardfail)	Insert Header Value & Deliver the Email
	DKIM Failed Emails (i.e., fail / hardfail)	
	DMARC Failed Emails (i.e., Quarantine / Reject)	Quarantine the Email

THREAT MATRIX

Forged Email / Business Email Compromise	Display Name Spoofing Protection (Exact Match)	Quarantine the Email
	Display Name Spoofing Protection (Near Match / Contains)	
Cousin / Lookalike Domain	Domain Name Spoofing Protection (Exact Match)	Quarantine the Email
	Domain Name Spoofing Protection (lookalike)	
	Sender Domain Age (< 30 Days)	Quarantine the Email with Subject Tag (New Sender) and Message Tag
	Sender Domain Reputation (POOR)	Quarantine the Email with Message Tag
	Sender Domain Reputation (AWFUL)	
URL Filtering	Malicious URL	Rewrite malicious URL to web security proxy & Quarantine the Email
	Bad Category URL	
	Click-at-time URL Protection	To Be Enabled
Attachment Defense	Dangerous Attachments	Quarantine the Email
	Executable Category Attachments	
	Macro File Detection	Header Value and Deliver the Email
	Password Protected File Detection	

KEY FEATURES

99.99%
Uptime Guarantee

100%
Protection from known malware

Inbound & Outbound scan
Inbound & Outbound Email Traffic

30 Secs
Average scan & delivery time less than 30 secs

Sandboxing

Zero Hour Protection
Critical first layer of defense

3 Days
Default mail spooling time in case recipent server is unavailable

99.40%
Spam catch rate

TLS
Encryption Support

25 MB
Maximum mail size allowed

Data Center
Multiple MX pointing to our centres

Anti Spam & Virus
Multi-layered Anti-Spam & Anti-Virus filtering

Reports
Mail tracking & Reports

Quarantine Management

KEY FEATURES COMPARISON

Feature / Capability	Mail Armor ATP	Office 365 Basic	GSuite Basic
Spam & Malware Filtering	✅ Advanced (Cisco ESA + AMP)	✅ Basic Filtering	✅ Google Filters
Zero-Hour Threat Protection	✅ Yes (Real-time)	❌ No	❌ Limited
Attachment Sandboxing	✅ Cisco AMP Sandboxing	❌ No	❌ Not Available
URL Protection & Rewriting	✅ Yes	❌ No	❌ No
Impersonation / Spoof Protection	✅ Advanced BEC Filtering	⚠️ SPF/DKIM/DMARC	⚠️ SPF/DKIM/DMARC
Ransomware Protection	✅ Multi-layered	⚠️ Limited	⚠️ Heuristic
Phishing Detection (AI/ML-Based)	✅ Cisco Talos AI	⚠️ Basic Rule-Based	⚠️ General ML
Email Continuity	✅ Yes	❌ No	❌ No
Quarantine Report for End Users	✅ Customizable	❌ Admin Only	⚠️ Admin Only
End-User Awareness (Banners)	✅ Yes	❌ No	❌ No
Admin Dashboard & Reporting	✅ Advanced	⚠️ Basic	⚠️ Basic
Deployment & Management	✅ Fully Managed	⚠️ Self-Managed	⚠️ Self-Managed
Support	✅ Local Support	❌ Standard Microsoft	❌ Standard Google

WHY MAIL ARMOR ?

- Powered by Cisco ESA + AMP: Real-time defense against evolving threats.
- Includes URL rewriting, sandboxing, and BEC filters not in basic O365/GSuite.
- Fully managed so no burden on internal IT teams.
- Daily quarantine reports and awareness banners for users.
- Advanced dashboards and granular security policy controls.
- Regional support from Mail Armor Support team—faster response than OEM.

THANK YOU

www.mhyracs.com

FOR DEMO / POC
sales@mhyracs.com