Barracuda

DISCOVER THE

THREATS

We process and protect over **one billion emails** every day
So we know how **quickly** emails can damage a business.

91% OF HACKS START WITH A TARGETED EMAIL ATTACK[1]

To protect your organisation, you need **four layers** of email security: from your inboxes to your employees

ONE **GATEWAY DEFENCE**
TWO **RESILIENCY**
THREE **FRAUD PROTECTION**
FOUR **HUMAN FIREWALL**

LAYER ONE **GATEWAY DEFENCE**

74%

74% of 2017's top threats came in as an email attachment or link[2]

90%

Over **90% of ransomware** infections are delivered through email attachments[3]

One in every 331 emails contains malware[4]

78% of people say they know unknown links in emails are risky, yet click on them anyway[5]

TO **STAY SAFE**, YOU NEED:

- **Inbound and outbound security** to ensure all malicious emails are blocked
- **Traditional signature defences** and advanced techniques like sandboxing to guard against all threats
- **Encryption and DLP** to control and protect sensitive information
- **Email archiving** for compliance and e-discovery demands

LAYER TWO **RESILIENCY**

34%

SMBs are primary targets for ransomware, but only 34% test backups regularly[2]

140,000

Backup is vital - 140,000 hard drives fail in the United States each week[7]

33%

One-third of companies say they've **lost data from SaaS applications** like Office 365[8]

YOU NEED **BACKUP** TO ENSURE RESILIENCY AND RECOVERY FROM DATA LOSS

Microsoft makes it clear that your ***data is your responsibility*** when it comes to Office 365

Employees are ***31% less productive*** during an email downtime incident[10]

AND A **CONTINUITY** SERVICE TO ENSURE CRITICAL EMAILS GET SENT DURING AN OUTAGE

LAYER THREE **FRAUD PROTECTION**

ADVANCED ATTACKS WILL **BYPASS THE GATEWAY**

97.25%

Since 2016, the number of phishing emails containing **ransomware** has grown to 97.25%[11]

95%

95% of all attacks on enterprise networks are the result of **successful spear phishing**[12]

WHAT TYPES OF SECURITY THREATS **CONCERN DECISION-MAKERS** THE MOST?[13]

27%	A phishing attack was successful in infecting systems on the network with malware
25%	A targeted email attack launched from a compromised account successfully infecting an endpoint with malware
25%	Sensitive or confidential information accidentally leaked through email

BUT **AI PREVENTS DAMAGE** BY USING YOUR COMMUNICATIONS HISTORY TO PREDICT AND PREVENT FUTURE ATTACKS

Ai

DMARC

AND **DMARC PROTECTS YOUR BRAND AND DOMAIN** BY ENSURING HACKERS AREN'T IMPERSONATING YOU TO SEND SPAM OR PHISHING ATTACKS

LAYER FOUR **HUMAN FIREWALL**

3%

Only 3% of users **report phishing emails** to management[14]

97%

97% of users **can't identify** a sophisticated phishing email[15]

TURN YOUR USERS FROM A **LIABILITY INTO A DEFENCE**

48%

48% of IT providers say **phishing emails were behind ransomware attacks**.[16]

36%

But 36% say the **lack of employee cybersecurity training** was to blame[16]

80%

80% of security-related breaches are caused by **employee behavior**[17]

YOUR USERS ARE THE LAST LINE OF DEFENCE AGAINST HARMFUL EMAIL

SO, YOU NEED TO TRAIN THEM TO BE EFFECTIVE

Barracuda

1,000,000,000
Protects and processes one billion emails a day

60,000
Over 60,000 email protection customers

2.5m
AI email threat defence engine trained on 2.5 million emails

17bn
Archived 17 billion messages

#1
Leader in spam and virus prevention since 2003

THERE ARE THOUSANDS OF THREATS THAT EASILY BYPASS STANDARD EMAIL FILTERS. WE CAN HELP YOU FIND THEM. OUR EMAIL THREAT SCANNER IDENTIFIES THE SECURITY AND COMPLIANCE THREATS THAT ARE CURRENTLY IN YOUR ACCOUNT.

GET YOUR FREE EMAIL THREAT SCAN

1 https://www.barracuda.com/products/essentials/
2 https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
3 IDC ANALYST CONNECTION: Why SaaS-Based Productivity Tools Require Additional Threat Protection - 2017
4 https://www.symantec.com/security-center/threat-report
5 https://h30657.www3.hp.com/t5/BusinessNow-en/35-cyber-security-statistics-every-CIO-should-know-in-2017/ba-p/8278
6 Ransomware Attacks: How prepared are SMB's? IndustryView 2015
7 https://smallbiztrends.com/2017/04/not-prepared-for-data-loss.html
8 https://www.backupify.com/blog/dont-be-a-victim-to-office-365-data-loss
9 https://products.office.com/en-us/business/office-365-trust-center-welcome
10 http://www.tbline.nl/index_htm_files/The-Importance-of-Continuity-in-Office-365-Environments.pdf
11 https://blog.barkly.com/cyber-security-statistics-2017
12 https://securityintelligence.com/improving-your-security-awareness-campaigns-examples-from-behavioral-science
13 Best Practices for Protecting Against Phishing, Ransomware and Email Fraud, Osterman Research White Paper, 2018
14 https://www.cwps.com/blog/7-startling-phishing-attack-statistics
15 https://www.cwps.com/blog/7-startling-phishing-attack-statistics
16 https://solutionsreview.com/backup-disaster-recovery/backup-recovery-statistics-know-2018/
17 https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron