vade

# EVALUATING MICROSOFT 365 EMAIL SECURITY SOLUTIONS

ARCHITECTURE MATTERS

Microsoft 365 is the #1 target for cybercriminals.
While EOP is sufficient for detecting known threats, you need additional protection. As an MSP, what are the key requirements for a modern Microsoft 365 email security solution that will work for your clients and also your business?

## 4 Key Requirements

For a Modern Microsoft 365 Email Security Solution

**1. Fast Provisioning**
Provisioning licenses and onboarding clients should be quick, painless, and built to scale.

**2. Low Maintenance**
Busy MSPs want to focus less on maintaining solutions and more on growing their business.

**3. Advanced Protection**
Blocking advanced threats requires predictive technology that learns from previous threats.

**4. Remediation**
Mitigating threats post-delivery should require little to no IT resources.

## 4 Things to Consider When Choosing a Solution

ARCHITECTURE · CONFIGURATION · USER EXPERIENCE · THREAT DETECTION

**ARCHITECTURE**
The solution should complement and layer effectively with EOP, augmenting rather than disabling native protection.

**CONFIGURATION**
Easy set up and maintenance is crucial to quickly deploying a solution to your end users and clients. Set it and forget it.

**USER EXPERIENCE**
Solution should require little to no training, freeing up admin resources and preserving the Microsoft Outlook experience.

**THREAT DETECTION**
Sophisticated email threats require an advanced solution that detects unknown threats and highly targeted attacks.

### ARCHITECTURE

The solution's architecture will determine its compatibility with EOP and whether deployment will require significant planning and resources.

**SITS OUTSIDE M365**
A SEGs disables EOP's native protection. When the gateway goes down, so does your email.

**SECURE EMAIL GATEWAY**

**REQUIRES MX CHANGE**
Hackers can see the solution in the MX record, making it vulnerable to MX record bypass.

**CAN'T SCAN INTERNALLY**
Because the SEG is outside Microsoft 365, it cannot scan the internal email flow.

**SITS INSIDE M365**
Layers with EOP and provides complementary protection. If the solution goes down, EOP continues to protect your email.

**API-BASED SOLUTION**

**NO MX CHANGE**
An API-based solution doesn't require an MX change, making it invisible to hackers.

**SCANS INTERNAL EMAILS**
Because it is inside M365, an API-based solution scans internal email flow for insider threats.

### CONFIGURATION

Quick and easy deployment is crucial to scaling your business.
How does configuration compare between a SEG and an API-based solution?

**SECURE EMAIL GATEWAY**
Configuring a SEG requires creating rules in Microsoft Exchange and then manually copying those rules over to the SEG. You will need to repeat this process each time you need to create more rules.

**API-BASED SOLUTION**
Rules are created in Exchange and automatically ingested by the API solution. No external quarantine means avoiding set-up of complex rules and configurations and no quarantine monitoring.

### USER EXPERIENCE

It's not just about end users and clients. You and your admins need a solution that is easy to set up and manage and doesn't require continual monitoring and maintenance.

**SECURE EMAIL GATEWAY**
Requires training
Sends daily digests
Requires quarantine management
Constant maintenance

**API-BASED SOLUTION**
No user training required
Transparent to end users
Microsoft Outlook experience
Set it and forget it

### THREAT DETECTION

To battle sophisticated email threats, a solution must be continuous, adaptive, and equally sophisticated. SEGs and API-based solutions have different approaches to threat detection.

**SECURE EMAIL GATEWAY**
**Static, rule-based protection**

Scans for blacklisted IPs and domains and phishing URLs to block known spam, phishing, and malware attacks. New, reported threats are manually added to blacklists to prevent future attacks.

**API-BASED SOLUTION**
**Continuous, adaptive protection**

Performs behavioral analysis on the entire email, including the origin, content, and context. Blocks unknown spam and malware, dynamic phishing, and advanced spear phishing attacks.

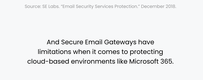
### REMEDIATION

How will you respond to threats that have already reached your end users? SEGs and API-based solutions have vastly different remediation capabilities.

**SECURE EMAIL GATEWAY**
Because it sits outside Microsoft 365, admins cannot retrieve email threats that have been delivered. Without the ability to remove emails post-delivery, admins must conduct manual threat investigation and response.

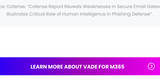
**API-BASED SOLUTION**
Microsoft 365 integration enables auto and one-click removal of threats post delivery. Reported threats that reach a threshold are auto-remediated by the AI across all users.

Sophisticated email threats require sophisticated protection. When it comes to protecting your MSP, EOP is not enough.




Source: SE Labs, "Email Security Services Protection," December 2018.

And Secure Email Gateways have limitations when it comes to protecting cloud-based environments like Microsoft 365.




Source: Cofense, "Cofense Report Reveals Weaknesses in Secure Email Gateways, Illustrates Critical Role of Human Intelligence in Phishing Defense".

LEARN MORE ABOUT VADE FOR M365

The CHANNEL CO. CRN TECH INNOVATORS 2019 · PERFECT FIT MSPs by Vade · SC ★★★★★ · CYBER SECURITY EXCELLENCE AWARDS WINNER 2019


Vade © 2020