

# MPS WHITEPAPER

## EFFECTIVE EMAIL THREAT SECURITY FOR SERVICE PROVIDERS AND THEIR ENTERPRISES

As Email remains the primary method for business communication, cybercriminals continue to use it as their preferred method of attack. In an era of Cloud platforms, businesses need to decide if they want to treat Email Security as another module, such as calendar synchronization, or if they want to invest in dedicated, carrier-grade Email Threat Security services.

Businesses paying more attention to security represent an opportunity for Security Service Providers to position themselves as value added experts, helping organizations navigate the ever-changing world of Email cybercrime.

### Cybercriminals and Email

Email is still the most popular and pervasive tool cybercriminals use to launch and distribute threats. But in recent years, fewer mass spam attacks have been launched. Instead, cybercriminals are focusing on higher-value operations, including malicious scams and attacks, spear-phishing attacks, and targeted attacks.

This increased volume of email threats is not new, but the nature of these attacks has changed: the number of targeted and zero-day attacks are rising and are more difficult to detect and stop than traditional malware.

In addition to these dangerous targeted attacks, data loss through email is another serious issue, establishing the need for organizations to both enforce security and control policies that protect employees and the disclosure of sensitive information over email.



## YOUR EMAIL RISKS

The cybercriminals' intentions with email communication are numerous, ranging from looking to lure users into transferring money, to individual hackers seeking sensitive information, and even nations engaging in economic espionage. The tools available to those seeking to undermine email security are very easy to obtain.

The risks can be divided as follows:

### Spam messages

Unsolicited messages with a variety of intentions: sell products or services to consumers, including black market items such as prescription drugs or counterfeit goods.

### Malicious Code

Email is a common avenue for the delivery of malicious code. Hackers seeking to infect a system with virus, spyware, or other type of malware may simply attach the installer or link to a malware hosting URI. As soon as the systems are infected, they can be used as entry points for internal networks, for sending spam, or to simply exfiltrate the computer's content.

### Phishing attacks

These are a variation of spam with more dangerous intentions. These unsolicited messages attempt to fool unsuspecting users into disclosing sensitive information. Malware can also be combined in phishing attacks to trick the user to open a file - seemingly legitimate documents that, when triggered, install the malware and compromise the user's computer.

### Insider Threat

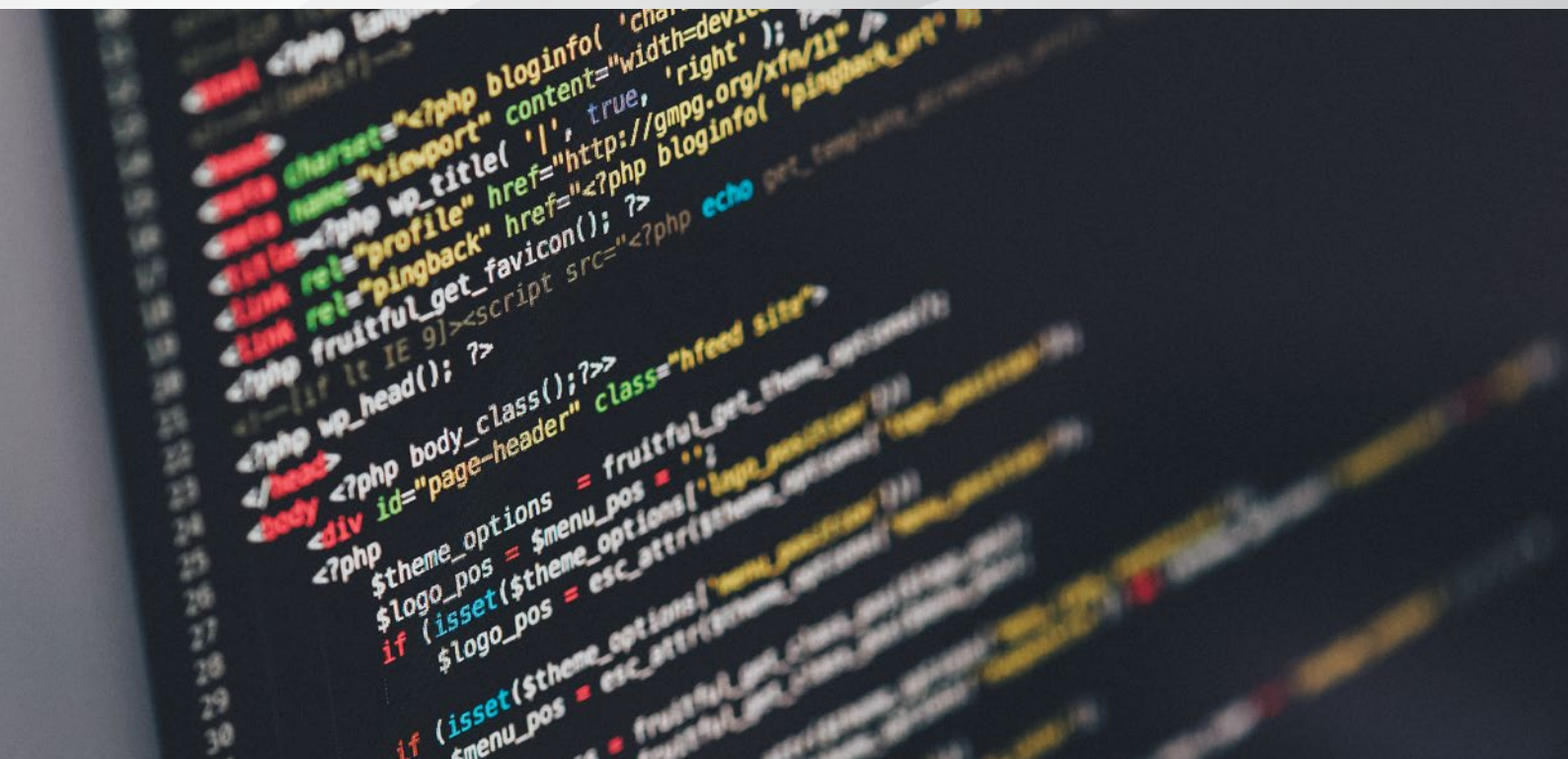
Employees with authorized access to the email system may, either intentionally or accidentally, cause damage to the organization by leakage of unauthorized, sensitive information.

### DoS Attacks

A denial-of-service attack aims at crashing systems by flooding an organization's email server with fake messages that consume all available server resources. This causes network congestion and, eventually, failure.

### Inappropriate Content

Employees may send or receive inappropriate content. Pornography, hate mail, and many other examples can constitute a violation of company policies and even national laws.



## THE SECURITY LAYER FOR ALL EMAIL PLATFORMS

How can your organization move to cloud-based email and productivity solutions without compromising security or adding risk?

The rapid and dramatic move to cloud-based productivity solutions is the future. These hosted services provide users with more efficient and flexible ways to collaborate, and they offer businesses and IT departments significant cost savings compared to traditional on-premise applications.

But how do these broadband solutions, built to fit both individuals and organizations of all sizes and all expertise's, handle the very specific nature of Email security?

Microsoft, Google, and other cloud vendors have included, free antimalware and DLP protection in their cloud-based email offerings. But how complete and effective are these built-in capabilities? And what else do organizations need to be fully protected?

It quickly becomes apparent that the "baseline" security capabilities included with Microsoft Office 365, G Suite, and other cloud-based email and productivity solutions

simply aren't fully suited for the demanding security any organization needs.

For example, Microsoft Office 365 only includes basic, signature-based anti-malware capabilities, which can't detect or block most of today's sophisticated targeted and zero-day attacks without adding their advanced threat protection solution at additional cost.

The phishing link protection in MS Office 365 is limited to a list of known bad domains, so it doesn't offer much protection against the sophisticated redirect and time delay techniques cybercriminals use to disguise malicious links. The built-in data loss prevention and encryption capabilities in Office 365 only offer limited policy management capabilities.

With MPS you will get, for instance, Data Leakage Protection, Business Reporting, Multitenant management of users, domains, and subdomains, Antivirus, Spam Waves Detection, DKIM, Quota management and rate control, IP Reputation, SPF, and many other security features that leverage your simplified email service into a carrier grade Email Ecosystem.

### AnubisNetworks MPS

AnubisNetworks **MAIL PROTECTION SERVICE** is a high performance, multi-tenant email Security service/platform, for on-premises and cloud services offered via Service Providers, Resellers or directly to SMB and Corporate customers.



#### MPS for Enterprises

An email Security solution for SMBs and enterprises, delivered as Cloud service or as on-premises VM.

- Reliable outbound and inbound filtering.
- A Carrier-grade email Backbone.
- Same user experience both as a SaaS service and as an appliance.

#### Opportunity

Benefit of Carrier-grade email security with data leakage and outbound control, on top of inbound security capabilities.



#### MPS for Service Providers

A complete multi-tenant platform to sell mail protection as an own brand (OEM) value-added service.

- Robust and Scalable Cloud platform.
- Multi-tenant platform.
- Allows new revenue streams with a private label service for Service Providers and their channel partners.
- Flexible deployment in existing email infrastructure.

#### Opportunity

Offer multi-tenant, private label, email security cloud-based solutions to Partners and enterprises.

## WHY THIS PRODUCT FOR END ORGANIZATIONS?

- ✓ AnubisNetworks' Cloud is secure and managed by Email IT security specialists.
- ✓ Multi-tenant management ensure an organization can always scale or delegate a problem.
- ✓ AnubisNetworks' privacy features ensure no one outside the organization sees the good and quarantined email.
- ✓ Cloud Computing for Security-Software-as-a-Service (SecaaS) means no Hardware costs.
- ✓ Bandwidth costs are reduced because 80% (average percentage of spam and malware in email) of email never reached the organization's infrastructure.
- ✓ Organization's network is protected from external attacks, because email is tunneled and controlled in the cloud.
- ✓ Outbound email filtering ensures reputation management for the Organization

## WHY THIS PRODUCT FOR SERVICE PROVIDERS?

- ✓ Software paradigm change, from traditional hardware employment to Software-as-a-Service. No investment in Hardware and Software.
- ✓ Software-as-a-Service permits continuous streams of revenue, with minimum maintenance and Operational costs.
- ✓ Brand identity is maintained, as MPS permits full customization per scope.
- ✓ Global players are reaching end companies directly, with bundled offers (i.e. Google) bypassing the sales channel. Resellers need to position themselves away from Global Players.
- ✓ Reseller adds email security to its portfolio, a critical, must-have service, for any company.
- ✓ Companies trust more in cloud if it is managed by specialists, and if privacy and management autonomy are guaranteed.



## THREAT INTELLIGENCE ECOSYSTEM

MPS has inside two engines. These provide MPS with the reputation and fingerprinting assessment.

These engines interconnect to AnubisNetworks Global Threat Intelligence Platform:

- ✓ Email fingerprinting close and exact matches with a global database of spam, phishing and malware email.
- ✓ Reputation on the sender IP, and sudden reputation changes.
- ✓ Reputation requests count, which may indicate spam waves.
- ✓ Known infections by Botnet families, especially with Malware knows to use email attack vectors.
- ✓ Social references in Dark social web to credentials.



## MAIN FEATURES FOR MPS

AnubisNetworks' Mail Protection Service includes multiple analysis engines that are continually updated to scan emails and accurately detect and eliminate known spam and malware threats.

Providing intelligent, real-time protection against targeted threats and zero-day attacks in addition to the industry's most proven and trusted signature-based protection, MPS intercepts millions of messages per day and analyzes these both internal and externally. MPS uses our Threat Intelligence Ecosystem, which makes it possible to catch and help stop zero-day attacks and targeted threats that traditional anti-malware solutions typically miss.



## FOLLOW US

-  [facebook.com/anubisnetworks](https://facebook.com/anubisnetworks)
-  [twitter.com/anubisnetworks](https://twitter.com/anubisnetworks)
-  [linkedin.com/company/anubisnetworks](https://linkedin.com/company/anubisnetworks)
-  [youtube.com/anubisnetworks](https://youtube.com/anubisnetworks)

### PORTO

**Address**  
UPTEC, Rua Alfredo Allen 455/461  
EC.3.12, 4200-135 Porto,  
Portugal  
**Phone:** +351 217 252 110

### LISBON

**Address**  
Av. D. João II, Lote 1.07.2.1, 4th Floor,  
Parque das Nações, 1998-014, Lisbon,  
Portugal  
**Phone:** +351 217 252 110

### BOSTON

**Address**  
125 Cambridge Park Drive  
Suite 204, Cambridge, MA 02140,  
USA  
**Phone:** +1 617 245 0469