

# Agari + Microsoft 365

Next-Generation  
Security for Cloud Email





## Executive Summary

### The Next-Generation Approach to Email Security


Email is undergoing a fundamental transformation as organizations worldwide shift more office productivity and business applications to the cloud. With around 95%<sup>1</sup> of the Fortune 500 using Microsoft 365, Microsoft leads this movement.

But for all of its convenience and utility, email has always been highly vulnerable to cyberattacks on multiple fronts, providing fertile grounds for the email security market to grow at an estimated 22% annually, putting it on track to reach around \$18B by 2023.<sup>2</sup> Organizations are spending billions to secure their email, but is all that money being invested wisely?

The secure email gateway (SEG) represents a sizable chunk of that spend. Unfortunately the SEG is no match for modern identity-based attacks that easily evade signature-based detection. As a point of proof—today around 94% of data breaches originate from email,<sup>3</sup> not to mention countless fraud losses from schemes including spear phishing, executive and vendor impersonation, ransomware, and account takeovers.

Recognizing that email security is an organizational priority, about 60% of large organizations will have comprehensive security awareness training in place by 2022.<sup>4</sup> But, as security training becomes the norm, SOC teams already dealing with an overall cybersecurity skills shortage are becoming inundated with employee-reported phishing incidents—of which around 58% globally are ultimately determined to be false positives.<sup>5</sup>

The email security market will grow an estimated **22%** annually, putting it on track to reach around **\$18B** by 2023



As they migrate to Microsoft 365, more organizations are recognizing that current investments in email security and phishing response deserve a closer look. While legacy email security vendors continue to shore up the secure email gateway and the financial annuity it represents to them, more organizations are embracing the reality that current email security architectures are fundamentally inadequate.

Cloud-first organizations are ditching the SEG and taking advantage of the enriched security features in Microsoft 365 and the [Secure Email Cloud](#) architecture, a combined solution designed to stop malicious email attacks that often come without malware or other recognizable payloads. They have found that the SEG impedes the native security controls of Microsoft 365 by obscuring the email header and feedback loop. By removing the SEG, they have reduced costs and enabled business agility.

This new approach blocks not only traditional spam, virus, and malware, but also the next generation of identity deception attacks. It secures the corporate sending domain from unauthorized use. And, in a significant departure from legacy security controls, it detects threats moving laterally across the organization and remediates newly identified threats that have made it to the inbox by evading initial detection or that weaponized post-delivery.

More organizations are embracing the reality that current email security architectures are fundamentally inadequate



# Table of Contents

## **Introduction to a Cloud-First World**

The Migration of Workloads and Security to the Cloud 5

## **Examining Efficacy and Risk of Traditional Email Security Controls**

Persistent Security Gaps in Legacy Systems 6

## **Moving Email Security Forward**

The Business Imperative for a Modern Security Architecture 7

## **The New Paradigm for Email Security**

Cloud-Based Security for a Cloud-First World 8

## **Using Applied Data Science to Protect Email**

The Confidence to Trust Your Inbox 9

## **Advanced Email Security Coverage Charts**

Agari, Microsoft, and Combined Solutions 10

## **Conclusion**

Moving into the Next Generation of Email Security 12

## **Appendix**

Comparison of Microsoft 365 + Agari  
and the Traditional Secure Email Gateway 13

## **About Agari**

15



# Introduction to a Cloud-First World

## The Migration of Workloads and Security to the Cloud

When Marc Benioff launched the “no software” movement on the eve of the dot-com bust in 1999, there was little indication of the tectonic shift to come across the business IT landscape.

While “Googled” became a word, “elastic cloud” compute and storage became the norm and organizations turned to Infrastructure-as-a-Service (IaaS) as prices for cloud hosting dropped precipitously. Organizations worldwide could now place workers and facilities just about anywhere around the globe and adjust IT strategy and workloads on the fly.

Platform-as-a-Service (PaaS) has since emerged as a compelling way to free organizations from decades of layered on-premises systems, improve security, and deliver integrated services.

As the dust began to settle, what started off as an ingenious way to eliminate IT capital expenditures, alleviate overhead, and accelerate software deployment morphed into a new way of business.

IaaS, PaaS and Software-as-a-Service (SaaS) turned out to be ideal enablers for an increasingly virtual and mobile workforce. Equipped with the ability to avoid up-front time and cost and to quickly phase out inefficient services, business agility improved.

Today, one-third of corporate IT budgets goes to cloud services, and the industry is on track to reach about \$513B by 2022.<sup>6</sup>

With 200M users,<sup>7</sup> perhaps no SaaS solution illustrates this better than Microsoft 365, which didn't just move to the cloud, but also reinvented the office productivity suite and became more resilient to cyber attacks. Now, there are compelling business reasons to move email security to the cloud as well.



# Examining Efficacy and Risk of Traditional Email Security Controls

## Persistent Security Gaps in Legacy Systems

Given the substantial investments in email security infrastructure over the past few decades, the current state of email security is surprisingly dismal.

An estimated 22.9 phishing attacks are launched every minute of the day, many of which result in a data breach.<sup>5</sup> That data breach costs an average \$8.64 million per incident in the United States, not to mention the long-term damage to brand reputation and regulatory fines.

Executive spoofing has become commonplace because the core email architecture allows end users (instead of the network) to specify the sending identity. Currently, only around 20% of the Fortune 500<sup>3</sup> have fully protected their corporate domains, leading not only to fake messages from the C-suite, but similar attacks including brand impersonation, partner invoice scams, and employee payroll scams.

Even with domains protected, workers can be attacked through techniques such as display name deception, look-alike domains, and brand spoofs included in credential phishing, for example. Email-based scams utilizing these techniques can lead to email account takeover (ATO), which allows cybercriminals to pose as the individual to divert money, steal information, and perform other malicious activities.

ATO-based attacks are especially dangerous because they are notoriously difficult to detect and serve as a gateway to lateral movement as threat actors glean important context to compromise additional accounts, escalate their privileges, and gain access to other systems, all of which can result in a data breach across the extended enterprise. We explore a particularly virulent attack modality called vendor email compromise (VEC) in our recent [Silent Starling threat dossier](#).

Malware, virus, and Trojan attacks are still commonplace, but with effective defenses having moved into Microsoft 365, attacks have shifted to targeting core human emotions of fear, curiosity, and anxiety. These social engineering attacks come without a recognizable payload, so they bypass the SEG with plain-text emails that do not utilize traditional techniques of malicious URLs and attachments. The United States Federal Bureau of Investigation (FBI) reports \$2.1 billion in real losses from BEC scams alone.<sup>9</sup>

For its part, the SEG checks incoming email only on receipt and generally does not re-check the inbox for latent threats that evaded detection or that weaponized post-delivery.



# Moving Email Security Forward

## The Business Imperative for a Modern Security Architecture

To supplement the protection of the SEG, organizations have turned en masse to phishing simulation training. Currently around 98% of organizations enable employee-reported phishing and about 88% use phishing simulation to train employees.<sup>5</sup> But the math is against them.

SOC teams already dealing with a widespread cyber skills shortage manage close to 33,000 reported phishing incidents on average each year. With a false positive rate of 68% globally and around 6.4 hours to investigate each one,<sup>5</sup> they simply can't keep up. Exploits can take months to detect, while exfiltration of sensitive data can happen in a matter of hours.

Phishing training helps, but organizations can still expect around a 3% failure rate where employees are unable to detect a phish email.<sup>10</sup> Unfortunately, it takes only one successful attack to do serious damage. It turns out that aside from the organizational drag that comes from mass distrust of the inbox, putting employees in the direct line of defense against email-based cyber attacks is a somewhat risky proposition, particularly given the existential threats a major breach can represent.

But as ineffective as the SEG tends to be against advanced email attacks, it also presents a significant obstacle to cloud-first strategies. By placing the SEG “inline” as email passes through, the SEG obfuscates the native security features of Exchange Online Protection, preventing Microsoft 365 from optimal function. It changes the email header information viewable by Microsoft 365 and the feedback loop from users goes directly to the SEG, leaving Microsoft 365 none the wiser from user-reported phishing attempts.

All the while, the SEG requires maintenance, training, and support that consumes valuable SOC team resources. Taken together, the cost and overhead of the SEG, the systemic risks to the business plan from attacks that evade it, and the negative impact it has on native security controls built into Microsoft 365, the SEG represents a significant hindrance to organizations looking to drive higher labor productivity and worker output.

This, of course, is a big part of the reason organizations adopt Microsoft 365 in the first place as part of their digital transformation strategies. Simplifying IT infrastructure while providing workers new and improved ways to communicate, collaborate, and perform their job functions both safely and securely is a critical objective for organizations looking to attract and retain the best talent as the new generations—the digital natives—enter the workforce.

And while Microsoft 365 provides a level of security closely resembling what organizations would find in a traditional SEG, including the ability to detonate and identify actively malicious payloads with Microsoft Defender for Office 365, additional protections against the most dangerous threats are needed to safeguard the organization from advanced threats such as business email compromise, executive spoofing, and account takeovers.



# The New Paradigm for Email Security

## Cloud-Based Security for a Cloud-First World

An evolution of the legacy secure email gateway, the next-generation Secure Email Cloud architecture is built for the cloud-first world and differs in several remarkable ways. Because it's a cloud-native SaaS application and compliments the built-in security features of Microsoft 365, it offers several key enhancements.

Many of the legacy features of the SEG are already pre-built into Microsoft 365 via Exchange Online Protection (EOP) and the optional Microsoft Defender for Office 365. In fact, Microsoft 365 provides support for all areas that have been traditionally protected by the SEG: pre-content filter based control, integrated antispam, integrated antivirus, attachment sandboxing, URL analysis, and data loss prevention.

Designed to assess incoming emails by analyzing content and infrastructure reputation, these platform-native controls are proving essential to ferreting out spam, malicious URLs and malware, certain keywords, or a high volume of attacks from a single IP.

For those areas not fully protected by native functionality, the Microsoft 365 architecture offers APIs such as the Microsoft Security Graph that enable advanced security solutions to integrate seamlessly. This is where many organizations enable the secure email gateway, but because SEGs were designed two decades ago, their architecture always requires that it be inline in the mail flow, slowing down mail delivery and introducing a point of failure. Beyond the mail deliverability and increased risk of downtime, inline SEG architecture actually hinders the effectiveness of the native Microsoft 365 security.

Unfortunately, cybercriminals rely on finding new and innovative ways to bypass the filters organizations put into place to protect against them, which is why they have recently turned to identity-based deception. Different from traditional email attacks, this next-generation of email attacks rely on impersonation and plain-text emails to bypass the filters set against the attacks of the past.

This is where the Secure Email Cloud architecture augments the controls set by Exchange Online Protection to prevent advanced attacks on Microsoft 365 environments. Designed specifically to identify when a message is malicious based on identity and models of trusted behavior rather than content, Agari prevents the most costly of attacks from ever reaching user inboxes. And for those emails that evade initial detection or weaponize after delivery, Agari provides options to automatically remove emails from user inboxes, effectively preventing users from opening the email or clicking on malicious links.





# Using Applied Data Science to Protect Email

## The Confidence to Trust Your Inbox

Malicious emails that use identity deception continue to bypass the legacy SEG and the native controls of Office 365 because they are notoriously difficult to detect. Consisting of only a few words, emails reach the targeted end user because there is no malicious content to identify. Those security systems looking for previously recognized signatures of malicious content can find nothing wrong with the email.

Once the email passes through security to the inbox, the scam becomes easy to perpetuate. Cybercriminals count on the human emotions of fear, curiosity, and anxiety to convince the recipient to reply. Once engaged in a conversation, the scammer simply needs to ask for a wire transfer, gift card purchase, or payroll diversion to complete their scam.

A way to prevent these attacks from reaching the inbox comes from understanding the perceived identity of the sender and the relationship between sender and recipient. To understand identities and relationships between senders, machine learning models [identity graph relationships](#) and behavioral patterns between individuals, businesses, services, and domains using hundreds of different characteristics at a global scale.

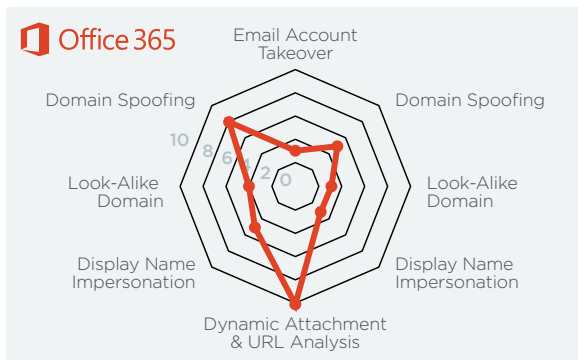
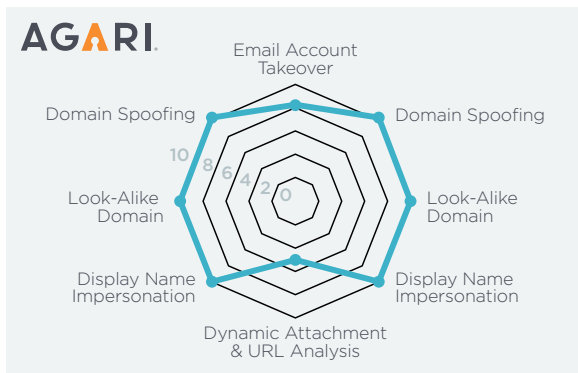
Using these machine learning models, automation, and expert human decision-making informed by massive sets of labeled data, the technology can score each message for convergence or divergence from historic patterns. In this way, the analysis identifies emails as conforming to normal “good” patterns and is thus a legitimate email. Those that diverge beyond a given threshold from established patterns are then potentially malicious or “bad”—no matter whether they contain malicious attachments or something as simple as five words. Instead of looking for the proverbial needle in a haystack, this innovative approach removes the hay to reveal the needle. It models the good to detect the bad.

This new approach gets more effective with every email analyzed. As a result, it effectively transitions the email security paradigm from one that was designed to address isolated events to one that continuously protects the organization against evolving email threats, as quickly as they emerge. And because this technology is always on, it becomes possible to continuously rescore messages and remove those that evaded initial detection from inboxes.

So while Microsoft 365 stops the vast majority of the most common types of attacks, Agari provides the defense needed to stop the most dangerous and sophisticated attacks. With this combination of the Secure Email Cloud and Microsoft 365, email attacks are stopped with 99.9% efficacy—enabling users to trust their inbox and SOC teams to quickly and efficiently identify and respond to emerging threats.

# Advanced Email Security Coverage Charts

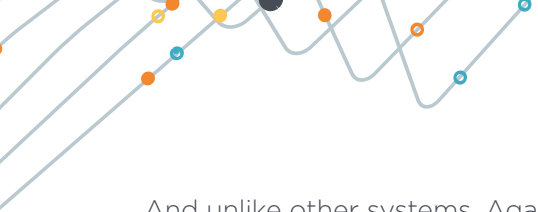
## Agari, Microsoft, and Combined Solutions



To protect corporate domains from being spoofed, Agari provides [DMARC email authentication](#) and helps organizations manage all third-party senders to reach enforcement at  $p=reject$  as quickly as possible. This prevents unauthenticated emails from reaching the inboxes of customers, partners, and employees.

This first step in securing the email environment provides the minimum level of protection to prevent brand abuse and stop cybercriminals from tricking unsuspecting customers and employees. In fact, Microsoft itself uses Agari to protect its domains such as microsoft.com, outlook.com, and office365.com.

For the business email compromise scams and account takeover-based threats that use display name deception or look-alike domains, Agari augments the Microsoft security controls to catch additional identity deception-based threats. Using a highly-innovative identity graph to model trust relationships, the Secure Email Cloud architecture detects malicious emails by understanding identities and relationships between sender and recipient. In this way, Agari can adjust to evolving threats and prevent them from reaching inboxes.



And unlike other systems, Agari not only protects against emails coming into the organization (AKA north-south traffic), but also continuously monitors and secures the emails traveling within an organization from employee to employee (AKA east-west traffic) to quickly discover if an internal account has been compromised. Part of the integrated solution for preventing advanced attacks, this key capability protects against bogus employee-to-employee emails.

Taking email security one step further, the Secure Email Cloud architecture works directly with Microsoft 365 to continuously monitor all inboxes within an organization, detecting latent threats as soon as new threat intelligence is discovered. When new threats are reported along with indicators of compromise through the global [Agari SOC Network™](#), all inboxes protected by Agari are inspected for those threats. SOC analysts are then notified via a convenient mobile app of any threats detected and can then be deleted from all affected inboxes with a few clicks.

For phishing incidents that need closer inspection, [Agari Phishing Response™](#) helps prioritize, triage, investigate and remediate threats in a matter of minutes, so cybercriminals never have the opportunity to redirect money or exfiltrate data. This has been shown to decrease phishing response time by up to 95%.

Combining Agari with Microsoft 365 provides next-generation security to protect against new and evolving email attacks and security issues while simultaneously eliminating the need for legacy infrastructure. As cybercriminals become more adept and discover new attack tactics, Microsoft and Agari continue to work together to protect your inbox from evolving threats—increasing confidence in your email ecosystem and saving you time and money.



## Conclusion

### Moving into the Next Generation of Email Security

After almost five decades in use, the architecture supporting enterprise email has been fundamentally redesigned and moved to the cloud. Microsoft 365 sits at the forefront of this movement.

In turn, the legacy Secure Email Gateway has been commoditized, with key signature-based defenses moving into Microsoft 365. The Secure Email Cloud architecture augments these native security controls to protect against modern, costly identity-based attacks.

Secure Email Cloud architecture works with Exchange Online Protection and Microsoft Defender for Office 365—not against them—to prevent business email compromise, domain spoofing, spear phishing, account takeovers, and all forms of identity-based email attacks.

Microsoft 365 and the Secure Email Cloud architecture are proven to work together to help organizations stay safe, reduce phishing incident investigative workloads, and provide premium protection of their email environment so employees, partners, and customers can trust their inboxes.

70% of Agari customers who use Microsoft 365 have eliminated their SEG entirely and now rely on the native security controls built into the two platforms for complete email security protection. This includes leading organizations such as Informatica, Honeywell, and Mars.

























Organizations that have moved to Microsoft 365 as well as those with hybrid deployments can rely on the same protections while eliminating the cost, overhead and complexity the SEG introduces to their business.















These protections differs in many ways from traditional legacy protections and include the ability to secure sending domains through DMARC email authentication, continuously protect against evolving identity-based attacks, automate remediation workflows for phishing incidents, and guard against email account takeover-based attacks.










This new paradigm of email security reduces the dependence on phishing training to defend organizations against the costly and time-consuming business disruption caused by modern attacks. It also simplifies the security infrastructure, reduces capital expenditures, and overhead while better equipping organizations to achieve the intended business benefits from their cloud deployment.

# Appendix

## Comparison of Microsoft 365 + Agari and the Traditional Secure Email Gateway

Advanced Threat & Impersonation Protection	O365 + Agari	Traditional SEG
Attachment Sandboxing		
URL Rewriting and Live Analysis		
Behavioral Relationship Analysis		
Display Name Impersonation Prevention (Own Users & Brand)		
Display Name Impersonation Prevention (External Users & Brand)		
Look-alike/Cousin Domain Spoofing (Own Brand)		
Look-alike/Cousin Domain Spoofing (External Brands)		
Domain Spoofing Prevention (Own Brands)		
Domain Spoofing Prevention (External Brands)		
Account Takeover Attack Prevention (Internal & External)		
Continuous Dormant Threat Detection/Response		
Protects both Microsoft 365 and Microsoft Exchange on-premises from a single console		

Email Authentication	O365 + Agari	Traditional SEG
SPF, DKIM, DMARC Builder		
Automated Sender Discovery & Inventory Management		
Hosted DMARC, SPF, & DKIM Records		
Workflow-Driven Authentication Configuration Management		
Native Look-alike/Cousin Domain and Non-Authorized IP Threat Intelligence		
API Access to Threat Intelligence		
Takedown Vendor Integration Support		

Phishing Response	O365 + Agari	Traditional SEG
Employee Incident Reporting		
Incident Management Workflow (ID, Classify, Prioritize Research and Respond)		
Incident Resolution Time Tracking		
Integrated Forensic Investigation and Analysis		
Automated Message Removal from O365 Inbox		
Continuous Latent Threat Detection / Response		

 Agari  Microsoft  Both

Note: Graphic represents Agari A1 Bundle with Microsoft Office 365 E5.



Reporting & Configuration	O365 + Agari	Traditional SEG
Identity Access Management with Role-Based Access	●	●
Automated User and Administration Notification	●	●
Real-time Removal of Unwanted and Malicious Email	●	●
'Claw Back' Removal of Unwanted and Malicious Email	●	●
Full Support of Azure Active Directory for Policy and Impersonation Control	●	●
Executive Dashboard Overview	●	●
Threat Disposition Reporting	●	●
Real Time Threat Reporting	●	●
Pre-Built Email Filtering Reports	●	●
Advanced Message Search	●	●
ROI-based Reporting	●	●
Impersonation-Based Threat Taxonomy Dashboard with Forensic Drill Down	●	●
API-Driven, Frictionless Deployment Model	●	●

Compliance and Email Hygiene	O365 + Agari	Traditional SEG
Antivirus Protection	●	●
Antispam Protection	●	●
Data Loss Prevention	●	●
Email Archiving	●	●
Sender/IP Reputation Analysis	●	●
TLS Encryption	●	●
Email Message Encryption	●	●
SPF, DMARC, DKIM Inbound Validation	●	●
Content Filtering Control	●	●
Sharepoint, One Drive and MSFT Teams File Scanning	●	●

Agari
  Microsoft
  Both

Note: Graphic represents Agari A1 Bundle with Microsoft Office 365 E5.

# About Agari

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, supply chain fraud, spear phishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity. Learn more at [agari.com](http://agari.com).

[www.agari.com](http://www.agari.com)

## Discover How Agari Can Improve Your Current Email Security Infrastructure

As your last line of defense against advanced email attacks, Agari stops attacks that bypass other technologies—protecting employees and customers, while also enabling phishing response teams to quickly analyze and respond to targeted attacks. Try our [simulated demo](#), or get a free trial today to discover how much money you can save by adding Agari to your email security environment.

[www.agari.com/free-trial](http://www.agari.com/free-trial)

## Calculate the ROI of Implementing Agari

Discover how much money you can save by adding Agari to your email security environment with our custom ROI analyzer.

[www.agari.com/roi-calculator](http://www.agari.com/roi-calculator)

- 
1. Microsoft CEO Satya Nadella's 6 Key Statements at Inspire 2019
  2. Email Security Market Work US \$18 Billion by 2023 at 22% CAGR ...
  3. Agari Research
  4. Gartner Magic Quadrant for Security Awareness Computer-Based Training
  5. Agari 1H 2021 Email Fraud and Identity Deception Trends report
  6. IDG 2020 Cloud Computing Survey, CBInsights Microsoft Strategy Teardown ...
  7. Office365itpros: Teams Drives SharePoint Online Growth to 200 Million Active Users
  8. IBM Security Cost of Data Breach Report 2020
  9. FBI IC3 Public Service Announcement: I-040620-PSA
  10. Verizon 2019 Data Breach Investigations Report