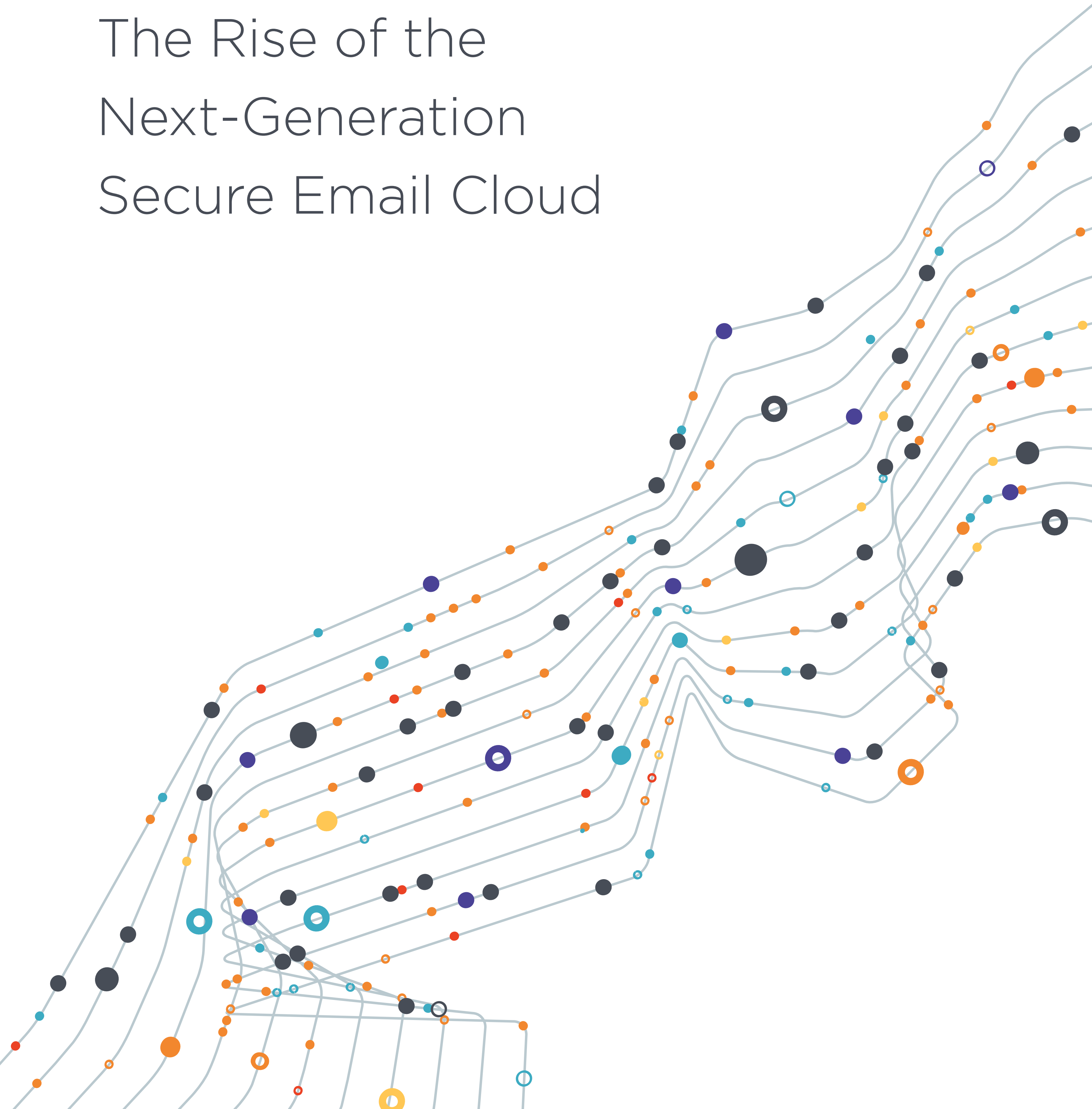
AGARI

WHITE PAPER

From SEG to SEC:

The Rise of the Next-Generation Secure Email Cloud



Executive Summary

The Time for Next-Generation Email Security is Now

The secure email gateway (SEG) worked for a number of years, but the SEG is no match for a new generation of rapidly evolving advanced email attacks that use identity deception to trick recipients. With business email compromise scams, spear-phishing attacks, and data breaches, along with other types of crime, cybercriminals are seeing massive success to the tune of $2.71 billion each year in the United States.

At the same time that cybercriminals are evolving their tactics, businesses are shedding on-premises infrastructure, moving en masse to cloud-based platforms such as Microsoft Office 365 or G Suite. These platforms provide native support for anti-spam, virus and malware blocking, email archiving, content filtering, and even sandboxing, but they lack when it comes to protecting against advanced email threats that use identity deception techniques to trick recipients.

This move to cloud-based email and the onslaught of zero-day attacks that successfully penetrate the inbox are shifting email security from signature-based inspection of email on receipt to continuous detection and response using machine learning to detect fraudulent emails and to hunt down latent threats that escaped initial detection or have activated post-delivery.

As a result, the Secure Email Cloud has emerged. This AI, graph-based approach detects advanced email attacks and cuts incident response time up to 95% in an effort to reduce the risk of business disruption and the rapidly increasing financial losses from data breaches, ransomware, and phishing. By employing a next-generation solution based on detecting identity rather than content, the Secure Email Cloud reduces the risk of serious financial, reputational, and organizational damage that occurs when rapidly-evolving threats hit inboxes.

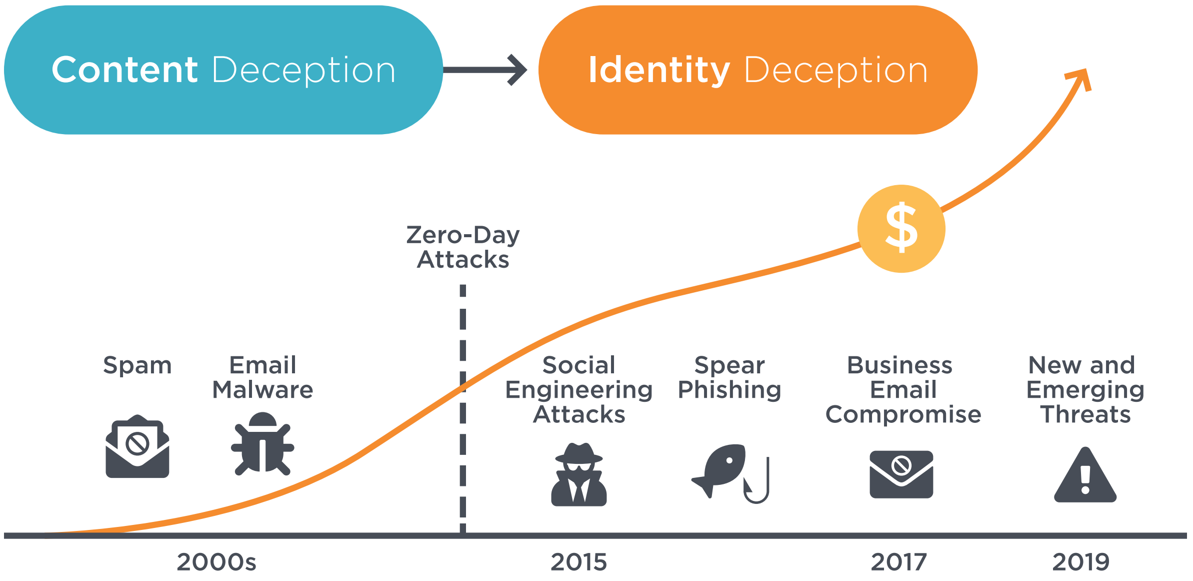
There is little doubt that email and the threats against it are changing fast. Email security must do the same.

The FBI estimates **20,000** victims lost **$1.3B** in 2018 from business email compromise in the United States alone.

Table of Contents

An Enemy in the Inbox

Identity Impersonation Has Changed the Game



The ubiquity of email, as well as the known limitations in its technology, has made the channel vulnerable to cybercriminals for decades. In the early 2000s, the secure email gateway (SEG) and various anti-malware/anti-virus vendors stopped the majority of these attacks as they focused on signature-based inspection of incoming message content. SEGs assessed the reputation of the sending infrastructure in order to identify and disrupt spam, virus and worm attacks, and scattershot credential phishing attacks. Leading SEGs still rely on detecting the “bad” or malicious content like malware, keywords, or high volumes of attacks from a single IP address.

While this approach stumped cybercriminals for quite some time, they eventually evolved to send new types of threats. Second-generation SEGs and advanced threat protection solutions leveraged malware sandboxes and new forms of dynamic analysis to counter them. Unfortunately, cybercriminals evolved email-based threats faster than most of the email security industry, changing their approach once again to using sophisticated identity deception techniques and attacks with no detectable payload, both which can easily bypass most legacy defenses.

A New Kind of Attack

Instead of relying on malicious links or software, a new generation of well-funded, increasingly networked cybercriminal operations has evolved the techniques used for email-based attacks from content deception to identity deception.

Exploiting security gaps in the underlying email protocols or the user interface constraints of email clients, attackers are able to send email messages that leverage the identity markers of trusted people and use deception techniques informed by social engineering to manipulate recipients into taking a desired action such as wiring money or divulging sensitive information. These messages hide in plain sight, easily bypassing legacy security systems undetected, and use personal and professional context to defraud businesses and individuals.

Making matters even worse, attackers are increasingly leveraging popular cloud platforms and services, and even compromised user accounts, to launch these attacks. By using Google and Microsoft infrastructure, cybercriminals prevent organizations and current email security solutions from blacklisting the services, given the tremendous volume of legitimate email that they send.

The Problem with Awareness Training

Perhaps the most obvious solution to defending against human vulnerability is simply to train end-users how to spot fake emails—showing them which rules to apply to inspect emails in their inbox. This can stop some attacks from being successful, but it is not foolproof. Even with the best security awareness training, a well-crafted targeted email attack using personal context is likely to fool users into opening the email and clicking on malicious links.

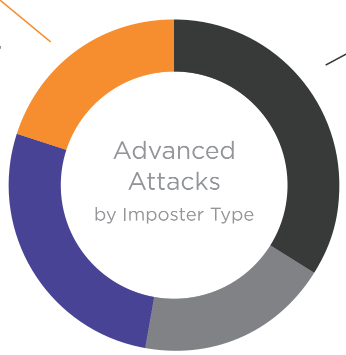
Furthermore, security awareness training will result in an uptick in reported phishes, many of which will turn out to be false positives. Clearly, a better solution is needed not only for email security, but for incident response and remediation as well.

Angles of Attack

Key Identity Deception Techniques

With identity-based email attacks posing a serious threat to individuals and organizations in every sector, it is critically important to understand how cybercriminals use identity deception techniques to evade existing security controls.

The key to any identity-based attack is impersonation—manipulating components of an email message to exactly match or bear an extremely close similarity to identity markers in a legitimate message. The most common message components that have these identity markers are the “From” header, the Subject header, and the body of the message.



20%
Look-alike Domain

From: LinkedIn <noreply@liinkediin.com>
To: Jan Bird <jan.bird@gs.com>
Subject: Diana has endorsed you!

34%
Display Name Deception (Brand)

From: Chase Support <chase@gmail.com>
To: Tom Frost <ffrost@amazon.com>
Subject: Account Disabled

27%
Compromised Account

From: Raymond Lim <rlim@contoso.com>
To: Cong Ho <cho@contoso.com>
Subject: PO 382313

19%
Display Name Deception (Individual)

From: Patrick Peterson <Patrick Peterson [hackyjoe@gmail.com]>
To: Cong Ho <cong@agari.com>
Subject: Follow up on Invoice Payment

Display Name Deception

Of these components, the display name in the “From” header is the most commonly recognized identity marker, as it is displayed prominently in most email clients. It is also the marker that is most commonly abused, since the sender of a message can specify any value for the display name. Indeed, this kind of technology continues to be the tactic of choice for cybercriminals, accounting for 53% of all email attacks.

Cybercriminals simply need to insert the name of a trusted individual or brand into the display name field within Office 365, G Suite, Yahoo, or any other cloud-based email platform. Since its point of origin is an established and widely used hosted email service, these attacks easily evade most SEG defenses, and then trick their recipients since the name matches one they are familiar with—either a brand they trust or a specific person within their organization

Compromised Accounts

The second most common form of identity deception is also the most harmful. Known as a compromised account attack, this approach is used in one out of every four new email scams, and it is by far the most difficult to detect and stop. A key driver of this attack modality is the rapidly expanding online marketplace for stolen email account login credentials belonging to high-value targets.

Here again, traditional email security controls are defenseless because these attacks are launched from a legitimate email account within a legitimate domain—perhaps even from the same domain as the target. These attacks are especially damaging because each new compromised account can lead to more. A successful compromised account not only gives fraudsters the ability to impersonate the email account's owner, but it also gives them access to the individual's contacts, ongoing email conversations, and historical email archives. This makes it possible to craft new scams that appear entirely legitimate—coming from the actual account with all the background information needed to make perfect sense.

Look-Alike Domains

The remaining identity deception technique includes look-alike domains. Here, threat actors can use common misspellings, homoglyphs, or Cyrillic characters that appear similar to the original characters in an impersonated domain to a company or a trusted service such as DocuSign, Dropbox, or Microsoft itself. While large services and corporations often register look-alike domains as "defensive domains" themselves to prevent this attack, they can never register every permutation. In addition, if the organization has not implemented the email authentication level needed to block the use of the lookalike domain, attacks can still spoof the look-alike domain, no matter who legally owns it.

By only slightly changing the domain, criminals can easily trick recipients who may not notice an extra letter or have the foresight to focus on the sending domain. Indeed, something a simple as changing a lowercase l in an email to an uppercase I can appear to be the same visually, but have an entirely different digital destination.

Despite their differences, each of these forms of identity deception is designed to bypass legacy security controls and ultimately convince recipients that the message was sent by an identity they know and trust. Once the email security system has been bypassed, cybercriminals have struck gold by taking advantage of a much weaker defense—humans themselves.

$27 Billion and Counting

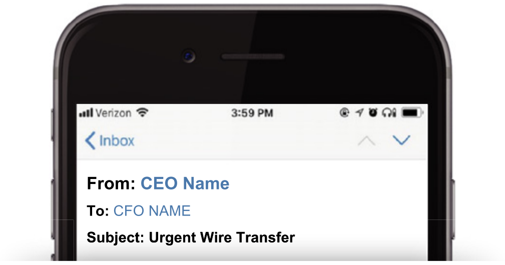
The Economics of Impersonation-Based Email Attacks

The result of these new identity deception-based email attacks is that business email compromise, data breaches, and consumer phishing are costing businesses and consumers billions.

Big Business in Business Email Compromise

These attacks are seen on a daily basis through CEO wire fraud schemes, partner invoice scams, or payroll diversion scams, with most organizations receiving hundreds or thousands of per year. Unfortunately, it only takes one to lose millions of dollars, as Google and Facebook recently discovered in a business email compromise scam that cost the tech giants $100 million each.

And it's not just huge enterprises that are discovering how easy it is to be scammed. Today, more than 90% of organizations report that they've been hit by targeted phishing attacks, with one in five suffering direct financial damage. Depending on the size of the company, industry reports estimate average losses from a successful email attack at $1.6 million—money that goes straight into the pockets of criminals.



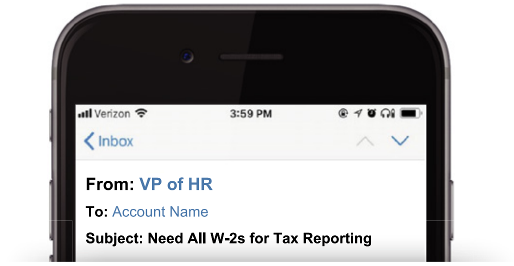
From: CEO Name
To: CFO NAME
Subject: Urgent Wire Transfer

$13.8B
2013-2018 Exposed Losses

Source: FBI/IC3

Data Breaches Continue to Concern

Business email compromise isn't the only major player, with the Verizon Data Breach Investigations Report stating that 96% of successful data breaches begin with an email. These breach-focused attacks use spear phishing or social engineering techniques to gain access to sensitive data such as employee W-2 or direct deposit information. According to the Ponemon Institute, data breaches now cost US-based businesses an average $7.9 million per incident. With 1,579 breaches reported in just the last year by the Identity Theft Resource Center, that comes out to $5.7 billion in annual costs to organizations.



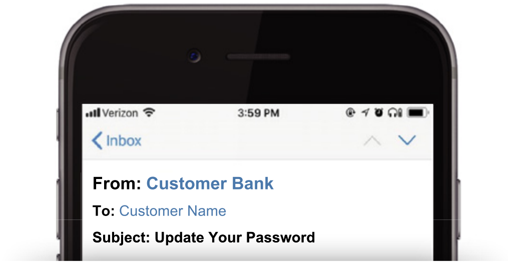
From: VP of HR
To: Account Name
Subject: Need All W-2s for Tax Reporting

$5.7
2017 Estimated Losses

Source: Ponemon/Identity
Theft Resource Center

Consumer Phishing Hits Hard

These attacks are not just targeted at employees, as consumers have been hit just as hard. In fact, RSA estimates that the total global losses from consumer phishing may be as high as $9.1 billion, in one year alone. In these attacks, cybercriminals impersonate trusted brands in order to defraud their customers, as well as other consumers and businesses. The negative headlines and reputational damage from these incidents can make the organization’s legitimate emails toxic to consumers who want to avoid falling victim to a scam, and the resulting impact on email-based revenue streams can be catastrophic.



From: Customer Bank

To: Customer Name

Subject: Update Your Password

$9.1

2017 Global Losses

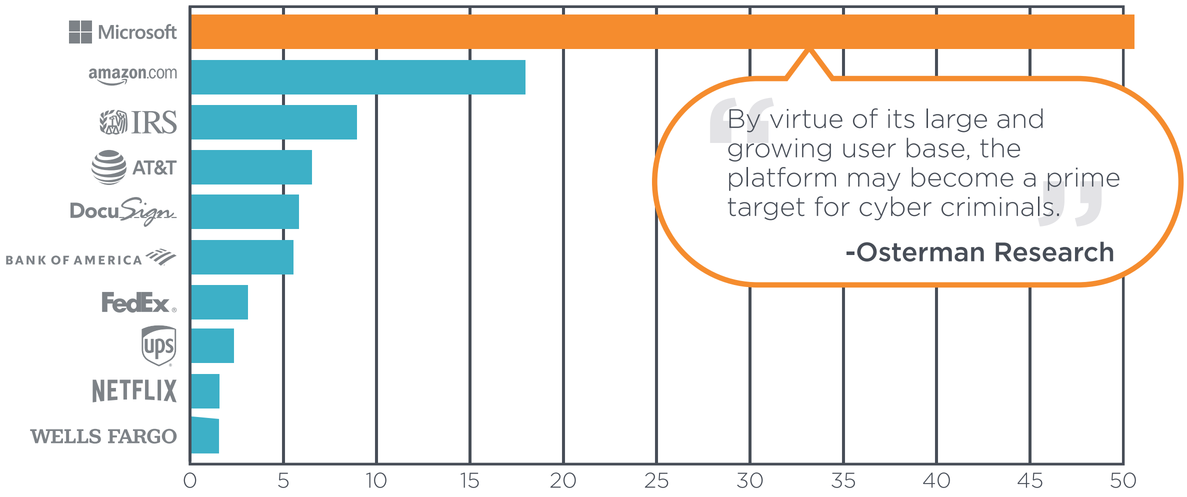
Source: RSA

Getting One Step Ahead

To counter these types of threats and those that come after them, the next generation of email security must take a fundamentally different approach to the secure email gateways and advanced threat protection solutions that are currently on the market. As cyber criminals move to outsmart current email security technology, organizations must move with them to a solution that uses identity markers to distinguish identity-based email attacks from legitimate email traffic and stop them before they reach the inbox.

Entering the Cloud

Microsoft is Most Impersonated Brand—And Biggest Target



By virtue of its large and growing user base, the platform may become a prime target for cyber criminals.

-Osterman Research

Based on the millions of attacks stopped and analyzed by Agari, Microsoft itself rises to the top when it comes to impersonation in identity deception-based email attacks. Today, 44% of brand deception attacks display the name of a Microsoft service as a way to deceive victims.

Whether it's a malicious email disguised as a Microsoft Office 365 password update, or an invitation to edit a OneDrive document linking to a spear-phishing page, the Microsoft ecosystem can be a key enabler for attacks on any organization. And as more businesses transition to the cloud, it also makes for a target-rich environment.

Inherent Threats in Cloud-Based Email

Display name deception is exceptionally easy within cloud-based environments, and building target lists is simplified since organizations are all within a searchable directory. When criminals succeed at infiltrating an O365-based email account, they gain a powerful launching pad for new attacks.

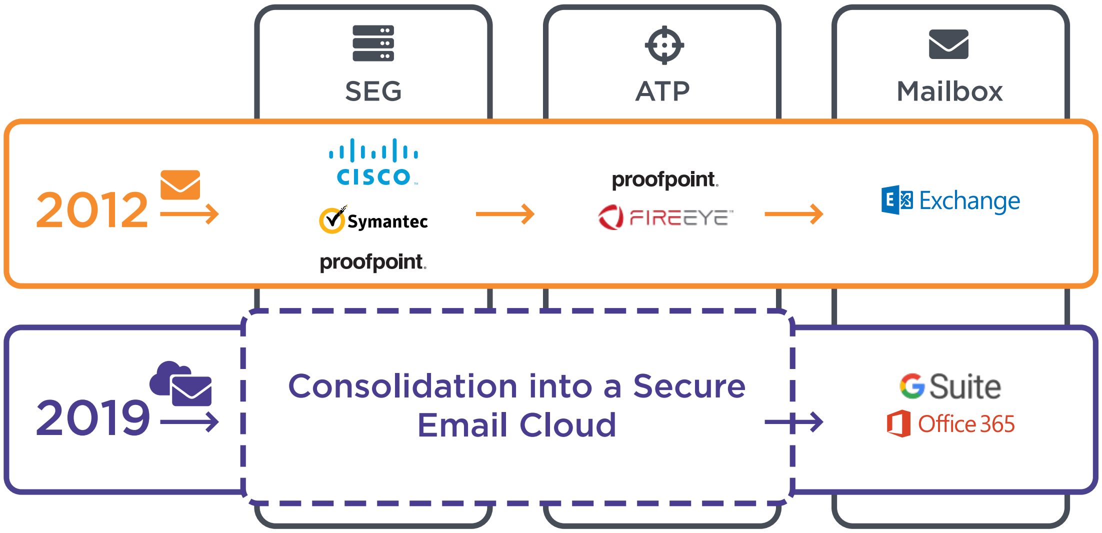
By leveraging a ubiquitous and trusted infrastructure, cyber thieves can continuously test attack methodologies until they're able to successfully circumvent security controls. And since users are frequently prompted to log in to connected services such as SharePoint, OneDrive, and Azure, phishing attacks aimed at harvesting credentials to these services can go unnoticed.

Once access is gained to a compromised account owner's contacts and archived messages, hackers are free to launch executive impersonation scams, request fraudulent wire transfers, steal valuable IP, and redirect employee paychecks, amongst other crimes. By taking it one step further, fraudsters are also able to wage fresh identity deception-based email attacks on outside organizations, using legitimate accounts to target both internal and external victims.

For organizations that have made the transition to hosted email services, these factors should serve as ample warning about the rapidly evolving threats targeting their cloud-based email operations—as well as the need for a new paradigm for email security.

Built-In Security is Not Enough

Consolidating Legacy Controls is Just the Beginning



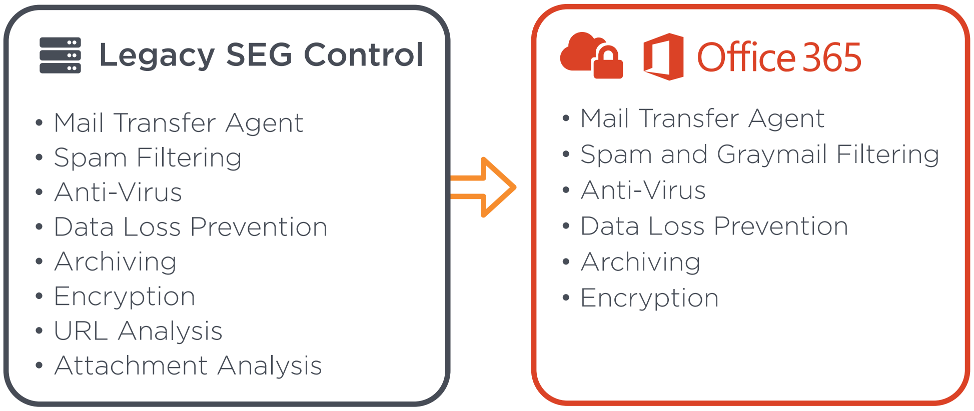
As organizations modernize their email infrastructures by transitioning to cloud email platforms, they shed layers of costly infrastructure from on-premises equipment, software, and maintenance resources.

Currently, more than half of all organizations have moved their email in the cloud with services like Microsoft Office 365 and G Suite, where much of the core functionality of legacy SEGs and APDs has been built directly into the platform.

Many capabilities of the traditional secure email gateway such as anti-spam, anti-virus, and malware protection are now being delivered in new cloud email platforms. This is a natural and expected evolution that is commonplace across all IT applications. It simply makes sense to develop new technologies in a better way than the preceding technologies, and in the case of email, this means integrating services into the base platform that in the past were bolted on.

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.

The Capabilities Built into Cloud Email



Legacy SEG Control

- Mail Transfer Agent
- Spam Filtering
- Anti-Virus
- Data Loss Prevention
- Archiving
- Encryption
- URL Analysis
- Attachment Analysis

Office 365

- Mail Transfer Agent
- Spam and Graymail Filtering
- Anti-Virus
- Data Loss Prevention
- Archiving
- Encryption

Today, nearly all the functionality of the legacy secure email gateway has been integrated as native capabilities of platforms such as Microsoft Office 365, G Suite, and others. In a recent Gartner report, Microsoft actually scored higher than all the major SEGs for anti-malware and anti-spam features.

Mail Transfer Agent: Message routing is core to email and as organizations leverage Office 365 to manage all their mailboxes globally, they need the flexibility to define email delivery paths. Microsoft's integrated MTA allows each organization to set up complex mail flows to ensure email delivery complies with specific regulatory or business needs.

Anti-Virus, Spam, and Graymail Filtering: For years, Microsoft trailed in anti-virus, spam, and graymail filtering efficacy. However, through on-going research and integration of several anti-virus and antispam engines focused on zero-day spam variants, URL analysis, bulk email categorization, and accelerated signature database updates, Microsoft has achieved parity to industry leaders.

Data Loss Prevention, Encryption, and Archiving: Microsoft recognized that in order to achieve full adoption of the Office 365 product suites, organizations needed help meeting compliance requirements associated with their business. The DLP, encryption, and archiving integrations native to Office 365 enable organizations to limit the exchange of sensitive data, ensure that authorized data is sent securely, and preserve a record of all email sent and received for legal purposes.

Enter: The Secure Email Cloud

While Office 365 covers each of these elements of security, it is not prepared to stop the next generation of email threats. This is why a new security infrastructure should be included—one purpose-built to layer on top of Microsoft Office 365 and other cloud-based email to prevent identity-based threats and other zero-day attacks.

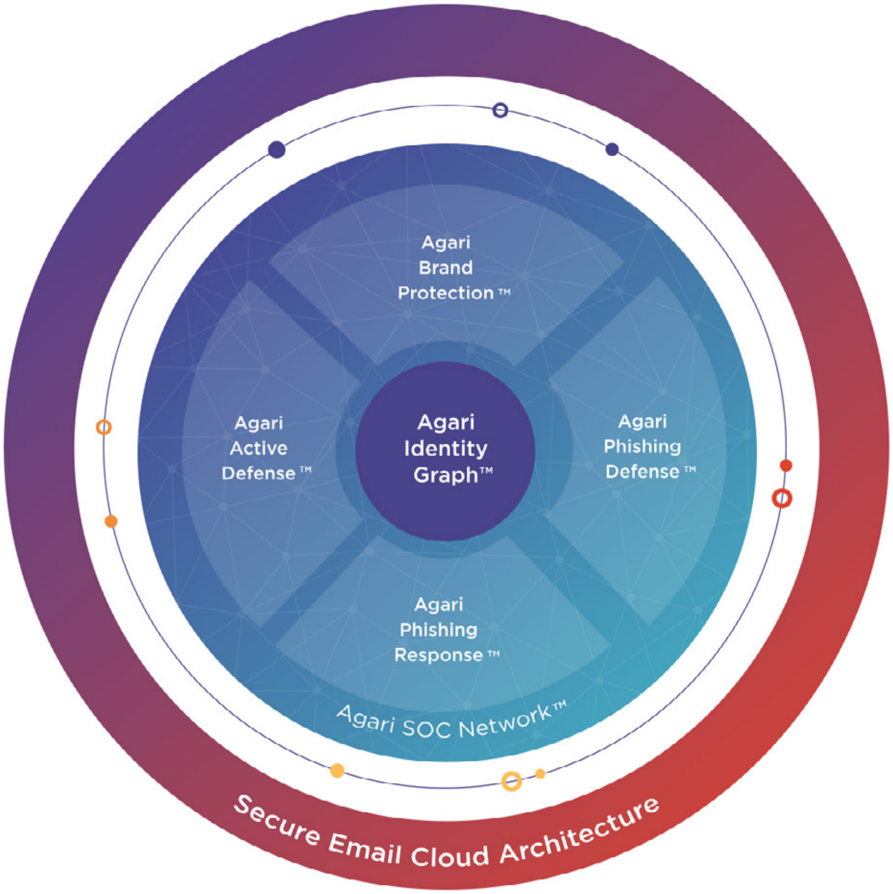
Today, the increasing sophistication of these attacks is calling into question not only the efficacy of the on-premises SEG, but the return on investment thesis as well. Considering that the cloud email platforms already provide the basic email security features of the SEG, more organizations are finding that pairing Office 365 with new Secure Email Cloud capabilities provides higher efficacy at lower cost.

The Secure Email Cloud is a next-generation approach to advanced email security, using realtime intelligence informed by trillions of emails flowing across the globe to continually detect incoming threats, as well as those that activate post-delivery. The Secure Email Cloud differs in several remarkable ways from legacy security controls and adds to the built-in controls in cloud-based platforms to include a higher layer of protection.

Built on Data Science

Introducing the Secure Email Cloud

Through the power of predictive AI and advanced machine learning, the Secure Email Cloud fundamentally transforms email security from event-based inspection of incoming messages on receipt to continuous detection and response for new and latent threats in all inboxes. In actual deployments, this unique technology approach, combined with real-time cloud delivery, detects rapidly evolving advanced attacks—including those that are highly-personalized and from time-to-time use custom variants of malware, viruses, Trojans, and worms.



A New Kind of Security System

In a similar fashion to commercial-grade AI solutions in other industries, the high-performance Agari Identity Graph™ at the center of Secure Email Cloud maps trust and authenticity of relationships and behavioral patterns between individuals, brands, businesses, services, and domains using hundreds of characteristics that define trusted communications.

The novelty in this approach is that the Agari solution functions in near the exact opposite fashion as legacy systems designed to detect known signatures of malicious email or that operate using static lists of trusted senders or domains. Unlike these static legacy approaches, the Agari Identity Graph dynamically models and scores good email and sending behavior to the level of around 300 million model updates each day.

Then, based on mathematical divergence in the scoring from known good patterns buried deep in the communication, the Secure Email Cloud applies human-like intelligence and decision making based on tailorable policies to detect and respond to malicious messages. At the same time, it analyzes each email at a depth and scale way beyond the capability of any human or other machine-based approaches.

This is possible not just because of AI tools or expertise alone, but also because of the scale and quality of the underlying labeled data set. The Secure Email Cloud analyzes around 2 trillion emails annually across a highly diverse set of industries and geographies.

The vast majority of these messages turn out to be legitimate. These good messages reach their intended recipients without delay, and continuously enable automated learning. Messages that reach a threshold of divergence are first blocked from reaching the inbox, then labeled along with indicators of compromise via automated workflows from a global network of analysts. This always-on semiautomated machine learning takes place around the clock—24/7/365.This is possible not just because of AI tools or expertise alone, but also because of the scale and quality of the underlying labeled data set. The Secure Email Cloud analyzes around 2 trillion emails annually across a highly diverse set of industries and geographies.

The vast majority of these messages turn out to be legitimate. These good messages reach their intended recipients without delay, and continuously enable automated learning. Messages that reach a threshold of divergence are first blocked from reaching the inbox, then labeled along with indicators of compromise via automated workflows from a global network of analysts. This always-on semi-automated machine learning takes place around the clock—24/7/365.

Prevent Zero-Day Attacks Every Day

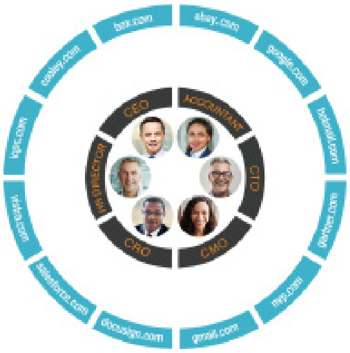
It is this combination of a human-labeled big data, semi-automated learning algorithms, and real-time cloud-based delivery that makes the Secure Email Cloud smarter and more reliable with each email analyzed. This dynamic approach to email security outsmarts fraudsters even as they change behavior—moving from domain to domain, jettisoning blocked accounts, reformulating email messages, switching out display name strategies, recompiling malware, and more.

It is also an approach that can't readily be faked or spoofed because a fraudster typically doesn't have a trusted pattern of communications with those they are intent on attacking. Even in scenarios where accounts have been compromised, behavioral anomalies can be detected. And once organizations adopt the Agari solution, there are simply easier targets in organizations that use less-effective alternatives. By using the Secure Email Cloud to block malicious messages and become a hardened target, attackers tend to turn their attention toward easier prey.

The Knowledge of Two Trillion Emails

A Deep Dive into the Agari Identity Graph™

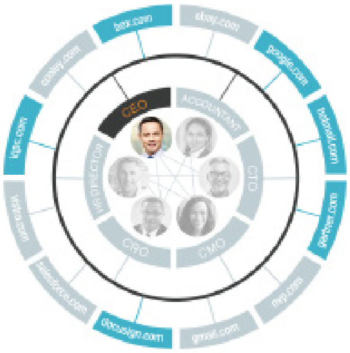
Map and Authenticate Identities



2T+

Messages Seen Annually

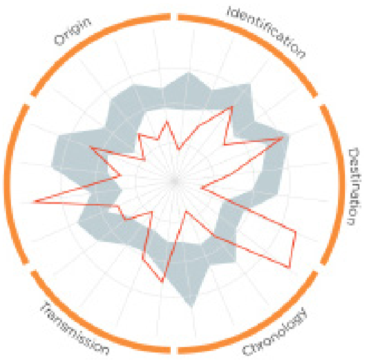
Learn and Model Behavioral Relationships



50,000+

New Domains Daily

Score Message vs. Expected Behavior



300M+

Model Updates Daily

The engine of a system designed to defend against sophisticated identity deception attacks requires advanced machine learning techniques, Internet-scale email telemetry, and real-time data pipelines that make it possible to individualize email protection using the kind of deeper, more relevant intelligence an organization needs in order to detect imposters.

As it becomes increasingly pointless to monitor an ever-expanding attack surface for phishing links or malware in search of “the bad,” it only makes sense that the next-generation solution seeks to characterize normative, legitimate behaviors that define the “good” in each email communication.

Based on those data-driven models, the Agari Identity Graph derives insights and intelligence to model good behavior and block everything else. As the ecosystem of customers grows, there is a network effect that improves the models and delivers higher levels of efficacy to stop more complex and zero-day attacks.

The Three Factors of Identity

With the behavioral baseline established, anomalies that signal fraud immediately reveal themselves, enabling businesses to focus interdiction based on identity instead of the obvious, overt attack methods. The three factors assessed by the Agari Identity Graph include a continuous cycle of three phases:

Identity Mapping: In this phase, deep data and predictive AI algorithms are used to model relationships and behaviors between individuals, organizations, and infrastructures in order to answer the question, "Does this message match the expected behavior for that identity?" Individual email messages are analyzed to determine the perceived identity and map it to a corresponding behavioral model.

Behavioral Analytics: This phase answers the question, "Does this message match the expected behavior for that identity?" The features of a message are analyzed within the context of a behavioral signature for that detected sender identity in order to determine whether it reflects anomalous behavior.

Trust Modeling: This phase answers the question, "How is the perceived sender identity related to the recipient?" The closer the relationship, the less tolerance for anomalous behavior, since there is greater potential damage stemming from an attack.

Each of these phases is predicated on leveraging a variety of algorithms and machine learning models to come up with accurate answers to their corresponding questions. The resulting identity intelligence is then combined to assign an overall risk score for an email message. The final score represents the probability that the message can be used to make fast and accurate policy-based action.

The Agari Identity Graph is unlike any technology behind a secure email gateway because of its AIdriven defense system, which recognizes and blocks identity deception tactics including business email compromise and spear phishing. This approach means that targeted email attacks never reach the inbox, providing a level of protection unparalleled by any other email security system on the market.

A Full Suite of Products

Using the Secure Email Cloud

In real-world deployments, the Secure Email Cloud framework has been shown to have high efficacy in protecting against advanced email attacks. In fact, around two-thirds of organizations that have deployed the Secure Email Cloud find that combining it with native email security embedded in platforms such as Office 365 not only provides better security, but also reduces capital equipment costs and operational overhead—often to a fraction of the price.

To understand more about how the Secure Email Cloud protects against threats that target employees, partners, and customers and helps remediate threats that bypass all defenses or activate post-delivery, let's explore the entire suite of products.

- **Agari Phishing Defense™:** Using predictive AI, Agari Phishing Defense detects advanced email threats including business email compromise, executive spoofing, and account takeovers launched from outside, or even within, an organization's email infrastructure.

- **Agari Brand Protection™:** By automating the process involved with deploying and managing the implementation of Domain-based Messaging, Authentication, Reporting, and Compliance (DMARC) protocols, Agari Brand Protection makes it easy to prevent cybercriminals from impersonating an organization in phishing attacks targeting its customers, as well as other consumers and businesses.

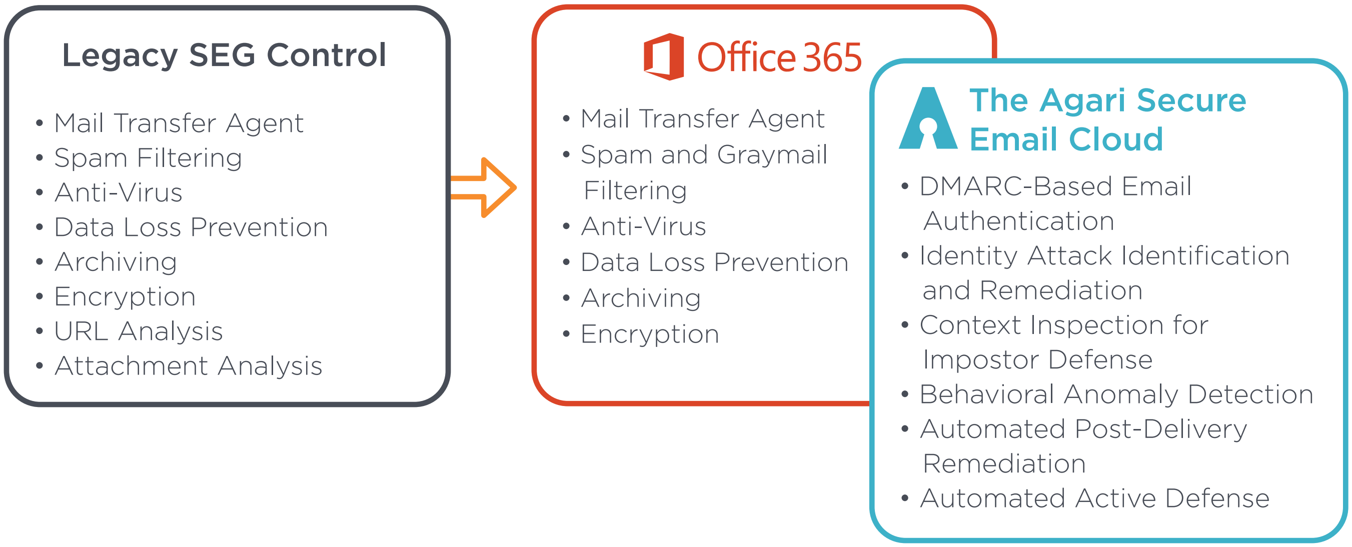
- **Agari Phishing Response™:** For that small percentage of threats that bypass security controls, Agari Phishing Response provides much-needed help to triage and resolve employee-reported phishing incidents and reduce the costs associated with incident response. Through automation of workflows, prioritization of threats, forensic analysis, impact analysis, and tools for remediation and reporting, Agari Phishing Response can reduce breach containment time by up to 95%, helping organizations reduce risk while realizing new operational efficiencies.

- **Agari Active Defense™:** Using active engagement capabilities, Agari threat researchers uncover criminals' tactics and techniques and empower security and fraud prevention teams with actionable intelligence about business email compromise (BEC) threats targeting an organization. The Agari Active Defense BEC Threat Intelligence service provides tailored reporting, data, and insights these teams need to understand threats, optimize defenses, and reduce risk from BEC attacks.

Reporting of newly discovered threats along with the indicators of compromise from the Agari SOC Network, analysts can pinpoint latent threats in the inbox that evaded prior detection and automatically remove those malicious email messages from the inbox.

The Secure Email Cloud is easy to deploy and manage, with most organizations seeing rapid time to benefit, often in as little thirty days. To help, the Agari team provides guidance and support through every step of the process from onboarding to deployment to ensure quick and efficient return on investment.

Better Together: Office 365 + Agari



Legacy SEG Control

- Mail Transfer Agent
- Spam Filtering
- Anti-Virus
- Data Loss Prevention
- Archiving
- Encryption
- URL Analysis
- Attachment Analysis

Office 365

- Mail Transfer Agent
- Spam and Graymail Filtering
- Anti-Virus
- Data Loss Prevention
- Archiving
- Encryption

The Agari Secure Email Cloud

- DMARC-Based Email Authentication
- Identity Attack Identification and Remediation
- Context Inspection for Impostor Defense
- Behavioral Anomaly Detection
- Automated Post-Delivery Remediation
- Automated Active Defense

With the legacy secure email gateway capabilities now present in Microsoft Office 365 and other cloud-based platforms, as well as the new security features available with the Secure Email Cloud, this combination is all organizations need to ensure that employees and consumers alike can open, click, and trust everything in their inbox.

The Secure Email Cloud includes all the capabilities needed for any modern organization to fight cybercrime, including email authentication to prevent spoofing, context inspection to stop zero-day attacks, URL and attachment analysis to stop known attacks, and automated post-delivery remediation to quickly remove malicious emails that get through initial controls. That is the reason why leading organizations across the globe use Agari to protect their inboxes.

After all, email and the threats against it are changing fast. Agari is here to ensure that email security does the same.

About Agari

Agari is transforming the legacy Secure Email Gateway with its next-generation Secure Email Cloud powered by predictive AI. Leveraging data science and real-time intelligence from trillions of emails, the Agari Identity Graph detects, defends, and deters costly advanced email attacks including business email compromise, spear phishing, and account takeover. Winner of the 2018 Best Email Security Solution by SC Magazine, Agari restores trust to the inbox for government agencies, businesses, and consumers worldwide.

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. Get a free trial today to discover how much money you can save by adding Agari to your email security environment.

www.agari.com/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