Reaching Beyond The Perimeter:
A Deep Dive into Mimecast’s Email Security 3.0 Strategy
The Evolution of Email-Borne Attacks & Email Security Systems

On the day the Web went live, echoes of the ensuing internet usage explosion were heard and understood as an opportunity by a certain breed of person. While there have been criminals for as long as there has been human civilization, in no time in human history has there been a better, safer (for the criminals), or more scalable platform for separating organizations from their money, sensitive data, or for causing mayhem.

Cybercriminals and other malicious actors have leveraged the Internet and its key applications of email and the Web since the beginning. In fact, Mimecast estimates that even today approximately 60% of all email sent to organizations is spam or malicious. And the web is no better. The Anti-Phishing Working Group regularly detects more than 80K unique phishing web sites every month.

What better way is there to reach your potential victims, to communicate with, and defraud them? Is there any surprise that the billions of global email and web users are such a fertile audience to attack? Over the years cybercrime and the security industry have been on parallel, intertwined maturation paths - the evolution of one driving the other forward.

And over the years what has resulted through the continued evolution of the cybercriminals tools and techniques is a highly specialized and industrialized marketplace for cybercrime. At the same time, in response, the cybersecurity marketplace has rapidly grown to be greater than $100 billion annually and has become equally specialized and industrialized.

As is common with maturing markets, cybercrime of today is made exponentially easier and more powerful through the use of specialized, off-the-shelf tools and “as-a-service” methods including “bulletproof” hosting, Dark Web-based services, malware development, ransomware-as-a-service, phishing, fraudulent website building, and sketchy financial transaction processing – enabling any criminally minded person to take part in cybercrime in just the way that fits their interests, expertise, and personal business models.

Email at the Center

Email has been right at the center of these attack and security trends and perfectly highlights the evolution of both cybercrime and cyber-defense. Bad actors have moved from the relatively unsophisticated to the very sophisticated using email. The evolution started years ago with unwanted advertising email (spam), moved to broad-based, malware-centric attacks (phishing and ransomware), to today’s highly customized and targeted email-borne attacks (spear-phishing and impersonations). As the attackers shifted their goals, tools, and techniques, the defenders have had to react accordingly. It seems clear that no matter how cybercrime evolves, email, due to its ubiquity and flexibility, will remain at its center.
Mimecast was founded to address the challenges of securing, archiving, and generally better managing enterprise email. During this time email evolved into the mission critical business communication application that it is today. And this transition increasingly exposed emails' inherent lack of security and its corresponding utility for cybercriminals. To address this security challenge the pace of Mimecast's innovation has only accelerated, as can be seen in figure 1 below.

One of the great insights at the founding of Mimecast was its creation as a purely multi-tenant, cloud-based platform, and not as on-premises software, as was standard at the time. In retrospect the cloudification of security controls starting with email security was extremely logical given the nature of internet-based email – it comes across the internet so why not filter it there before delivery? But even more so, the ability to outsource a key security control to a service provider, with superior technology and compute resources than what can be assembled on-premises, with massive economies of scale and scope, and 24x7 IT and security operations expertise, has been key for addressing the security skills and resource gaps that most enterprises face.
Mimecast’s Email Security 3.0 Strategy

The need for world-class email security has certainly not lessened over the years since Mimecast’s founding in 2003. Just the opposite. This has led Mimecast to come forward with the next major evolution of our email security strategy that we have termed simply: Email Security 3.0. The “3.0” moniker both implying the 3rd major generation in the evolution of email security, but also the 3 areas or “zones” of security capabilities that need to be applied together to truly provide comprehensive, pervasive, and even proactive email security.

Mimecast’s Email Security 3.0 strategy is here to help IT and security professionals achieve a new and more comprehensive form of protection by providing security controls:

- **At the email perimeter** – Enforcing security controls at the point of entry or exit of the organization or of the email platform.
- **Inside the network and the organization** – Security capabilities focused on applications, systems, and people that are internal to the organization.
- **Beyond the perimeter** – The realm of the internet that is beyond the direct view and control of an organization’s IT and security teams, but where cybercriminals develop and host many of their attacks.

Given that no security control should be implemented as an island or silo, it is critical that email security systems be integrated with an organization’s other security systems. This bridging of security controls can provide tremendous opportunity for greater and faster insights and efficiencies through data integration and automation. The Mimecast strategy directly addresses this through an extensive open API as well many associated integrations with 3rd-party security applications.

It is important to start by debunking the myth that email security is only about inspecting and filtering email at the perimeter via a cloud-based gateway. While perimeter-centric security is and will remain foundational for email, to maximize efficacy and efficiency, security controls must also be applied inside the organization as well as beyond the organization’s perimeter. And, the email security system must be integrated with other elements of the organization’s security systems and processes. It must also provide coverage beyond just the email channel, since email is both a major point of interaction with people as well as a key point of access to the web. Attackers often combine email and the web, while also relying on human mistakes to accomplish their goals, thus defenders must design their defenses to address all of these elements.

At the same time the cloud is continuing its sweep through all of IT and security. It is not a secret that most organizations have or will be shifting most of their employees to Office 365 or GSuite as their email platform, from Microsoft Exchange on-premises. Thus, with Mimecast’s Email Security 3.0 strategy, it is also critical that the security controls also protect and leverage whatever email system, or combination of email systems, the organization might be using. As well as to help with the transition from one to the other.

If you ask any seasoned security person what the no. 1 factor is that determines an organization’s success or failure with a particular security control, they will typically call out the security maturity of the organization as the key factor. There is a lot of security technology out there, and much of it requires significant additional skills and resources to work. In addition, much of the technology works in isolation as point solutions. If just buying security technology was the primary determiner of security programs’ success, the rate of breaches would be much lower! The Mimecast Email Security 3.0 strategy specifically considers the broad spectrum of security expertise and maturity and enables organizations to grow into it at their own pace.
Drilling Down into the Components of the Mimecast Email Security 3.0 Strategy

At The Perimeter

When most security professionals think of today’s state-of-the-art email security systems, they generally think of cloud-based gateway services that inspect and filter inbound and outbound email for spam, malicious attachments and URLs, impersonations, and sensitive content that might be trying to exit the enterprise via email. These systems sit between the organization’s email system(s) and the internet and apply the organization’s security and email handling policies to each email that is entering or exiting the organization.

How Mimecast does it

Mimecast’s “at the perimeter” controls now provided as part of Mimecast Secure Email Gateway with Targeted Threat Protection, have massively evolved since 2003 to provide a comprehensive set of spam, malware and malicious URL, impersonation, and content related inspections and filters for our tens-of-thousands customers around the world. To explore how this part of the service works please read the paper Mimecast Cyber Resilience for Email Technical Deep Dive.
The core concept of the “at the perimeter” capabilities is graphically represented in figure 2 below which shows the inspection steps an inbound email must go through before it is delivered to employees’ inboxes. It is important to note that the majority of these steps are also applied to outbound as well as to internal email.
It is important to note that Mimecast can inspect and filter malicious URLs – via URL Protect for URLs embedded in emails – as well as web traffic more generally that is initiated from internet browsers or other applications (including malware) that use the http protocol and DNS services to operate. The details of the Mimecast Web Security product can be found in the Mimecast Web Security Technical Deep Dive paper. However, an overview of Mimecast Web Security’s web site and web application-oriented inspections can be seen in Figure 3 below.

**Figure 3:** Mimecast Web Security Inspection Funnel

- **Exception Bypass**: Trusted Domains
- **Block/Allow**: Explicitly defined domain & URLs
- **Targeted Threat Protection Managed URLs**: Domains & URLs defined identified by email security product
- **Newly Registered/Observed Domains**: Often associated with malicious activity
- **Application Control**: Identify, block, sanction and monitor cloud apps
- **Category Filtering**: Enforce web security & acceptable use policy
- **Domain Similarity Check**: URLs mimicking trusted brands, including foreign character-set deception
- **Anti-Virus/ File Analysis**: Proxy traffic from suspicious site to scan for malicious content
Inside The Network And The Organization

When an attacker of almost any level of sophistication attains a foothold in an organization, often by getting ahold of login credentials for the target organization or by getting remote access to the network, their first step generally is not to exploit the organization, but to gain an even larger foothold. And email is a typical way that they do this. How capable are most employees at being able to resist engaging with a phishing email that is truly coming from an actual colleagues’ corporate email account? What open and click rate would your organization expect when the attacker is already on the inside? Are your employees ready for this type of attack or the many other ways they can unwittingly be a direct contributor to a security incident or breach?

How Mimecast does it

Inside the network and organization Mimecast can detect and remove malicious emails – those with malware or malicious URLs – inspecting those emails that never leave the organizations’ email system and thus don’t directly traverse the Mimecast cloud gateway service. This is where Mimecast’s Targeted Threat Protection product, Internal Email Protect, comes into play. By applying much of the same inspection steps shown in Figure 2 above and by leveraging direct integrations with Exchange and Exchange Online in Office 365, Mimecast can detect and remove malicious, unwanted, or inappropriate emails that may be internally traversing an organization’s email.

And lastly, there are the employees in your organization. While many security incidents and breaches can be traced to human error, it doesn’t necessarily have to be this way. It is possible turn the natural human tendency for error - and the cybercriminals knowledge of how to take advantage of it - into a valued part of your security program, improving your critical last line of defense, your people.
Mimecast does this through an integrated security awareness training product known as Mimecast Awareness Training, which consists of a broad library of entertaining yet informative videos with various security messages that are easy for any employee to understand and internalize.

Integration with the rest of the Mimecast platform enables the users’ training and related activity to become an integral part of broader security controls, reporting, and policies.

Figure 4: Mimecast Awareness Training Videos
Beyond The Perimeter

A common misperception is that the only way to protect your organization from phishing and related web attacks is to block them when they arrive at the organization. Following this line of thinking this means you must wait for the attacker to execute and direct the attack at you before engaging your security defenses. This is missing the opportunity to move your defensive response earlier in the **Cyber Kill Chain**. The earlier attacks can be detected and diffused the less likely they are to do damage or to accomplish their goals.

In addition, what about attacks that impersonate your brand, but are directed at your business partners, customers, or others that trust your brand on the internet? How can you stop an attack that doesn’t even arrive at your organization? Best practice calls for having strong perimeter defenses that are extended with security controls that extend beyond your perimeter.

It is true that the global, dynamic, and decentralized internet has historically given the advantage to malicious actors, but all is not lost. While domain registrars and hosting services are not equipped to continually police their millions of customers, they very often will do the right thing and take down bad actors when presented with credible evidence of malicious intent or activity.

This is exactly what the “beyond the perimeter” portion of the Mimecast strategy addresses. The key is to find, block, and remove the attackers’ email and web domains and infrastructure before they can launch their campaigns at your organization or your business partners and customers. This enables Mimecast customers to move beyond being 100% reactive and to more proactively protect their online brands.

*How Mimecast does it*

Mimecast addresses the misuse of online brands in two closely related ways, one for email and the other for the web.
Mimecast DMARC Analyzer

Mimecast DMARC Analyzer leverages the growing network effect of organizations and email service providers that enforce and report on email delivery problems using DMARC. The DMARC standard helps domain owners whitelist legitimate email senders and as a result in effect blacklist and ultimately block senders that are abusing the organization’s email domain(s).

DMARC adds a reporting collection, management and policy layer on top of the two well established DNS Authentication standards, SPF and DKIM, and in effect tells email receiving organizations what to do with emails that are received but that have failed these authentication checks. Mimecast DMARC Analyzer is an application and an associated optional professional service offering that helps organizations deploy, manage, optimize, and monitor their implementation of DMARC by consuming DMARC reports sent by email receivers.

Using DMARC for an organization is best enabled with an application that accelerates the process of moving from “p=none” (just report failed DNS Authentications to the domain owner, but don’t change enforcement) to “p=reject” (report and block emails that fail DNS Authentication). DMARC Analyzer does this by collecting DMARC Reports to learn about the existence and DNS Authentication status of emails that are being sent on the behalf of the legitimate domain owner. Using these reports, the email domain owner can whitelist senders that are legitimately sending on their behalf, and by default, when they set their DMARC entry to “p=reject”, block all other, illegitimate email senders. The use of DMARC is an excellent way to protect your organization’s online email brand from direct spoofing.

Figure 5: Mimecast DMARC Analyzer
Mimecast Brand Exploit Protect

As easy it is to directly spoof an email domain and brand it is even easier to setup a fraudulent web site that looks and acts like the legitimate one. Often used in conjunction with a spear-phishing attack, fraudulent web sites are regularly used to steal login credentials, collect other sensitive information, steal brand equity, or drop highly targeted malware on unsuspecting people. Given how easy it is to register similar domains to the legitimate ones – given the vast number of top-level domains and the use of international characters in domains - and to deploy web sites made up of cloned content, how can this attack technique be detected, blocked, and ultimately removed from the web?

How Mimecast does it

This is exactly where Mimecast Brand Exploit Protect comes into play. This Mimecast product combines automated web scanning, the analysis of feeds of new domain registrations and new TLS certificate issuance, and the tracking of web site cloning, with automated site blocking, content flooding and domain and site takedowns, to defend against the misuse of online brands on the web. It is hard for a cybercriminal to get much utility from a malicious web site if it is down before they can launch the campaign!

Underneath it All - The Mimecast Platform

The Mimecast capabilities described above do not live in technical silos. Just the opposite. Mimecast products leverage and depend on a global network of identical cloud-based, multi-tenant, datacenters that provide the underlying compute power, storage, scalability, reliability, and management for all the analytics, threat intelligence, administration, reporting, workflow, and APIs. Referred to collectively as MIME|OS, this platform is a key element of what makes the Mimecast products different and better.

Equally important as the MIME|OS global platform are the security and IT operations professionals that oversee the ongoing tuning of its security detection and analytic capabilities. On a 24x7 basis the operation and security detection capabilities of the platform are monitored and enhanced to keep up with current events and attacks.
Mimecast also clearly recognizes that our security products, while extensive, are only a portion of the security controls that will be in use by customers. To maximize efficiency and to reduce risk it is important that security controls work well together, and that relevant data is exchanged between systems in real-time. To support this, Mimecast has an extensive and regularly expanding list of integration partners covering key security control areas such as SIEMs, SOARs, Security data lakes, and endpoints, well as an open API that is available to customers and partners to integrate with systems of their choosing.

The Core Problems Organizations Face and How Mimecast Can Help Address Them

Most organizations are under protected, but their IT and security teams are overwhelmed, and thus most organizations are vulnerable to attacks from even moderately sophisticated attackers. The only question is when it will happen.

Beyond the specifics of attacks and the technologies and services that are available on the market to help address them, organizations need to wrestle with core structural challenges to their security programs.

These challenges include:

- A heavy and growing dependence on IT systems, applications, and related automation – growing faster than they can secure them.
- Limited budget for security systems, people, and expertise. Not keeping up with the growth and sophistication of the attacks or the spread of their data and applications.
- Security staff that, due to limited integration and automation of their security systems, must spend too much time on repetitive and low value tasks.
- Separately managing the multiple security control silos present in most organizations limits the efficiency and the effectiveness of the controls.
- Limited appreciation from other parts of the business of what the security team is doing and the value that they are delivering to the organization.

How Mimecast Can Help Address Them

While there are no security silver bullets on the horizon, there are favorable trends underway with the movement of security controls to the cloud that can help dramatically improve security programs and reduce risk. Mimecast’s Email Security 3.0 strategy leverages and helps deliver on all of them:

- **Outsourcing much of the security control management and enforcement via cloud-deployed security services.** This helps to elevate IT & security teams to being risk managers/advisors and security control portfolio managers. Reducing the amount of time spent on repetitive, low-value tasks and gaining overall leverage on security spend. In fact, the worlds of cloud-based security controls and Managed Security Service Providers (MSSPs) are blurring.

- **The re-factoring of security controls for the cloud from the way they were deployed in the purely on-premises days.** Replacing disparate, siloed security controls with greater combinations of integrated security controls sourced from the cloud. And extending this model through extensive integrations with third-party cloud and on-premises security systems. These integrations enable positive feedback loops so activity in one control area can inform the policies in other control areas.

- **Greater automation from detection to response to reduce the load on the security staff.** Helping to address the skill shortage by better leveraging existing security staff.

- **Eased and more business relevant reporting covering the current security posture of the organization.** Helping security teams to more easily communicate and collaborate with other parts of organization.

- **Increased and faster threat intelligence generation, consumption, and sharing both within the security cloud-service, across the industry, and across the organization to drive better detection and response.** Also helping to address the skills shortage by better leveraging the existing staff as well as improving the speed of response to new and emerging threats.
Mimecast's Email Security 3.0 strategy, covering at the perimeter, inside the network and organization, and beyond the perimeter, provides a broad, comprehensive, and integrated approach that enables organizations to use what they need now while having the expansion room to evolve and mature their security programs as their businesses grow and change.

Mimecast's Email Security 3.0 strategy helps organizations address email-borne attacks more comprehensively and proactively.