Email Security 3.0

Extending Protections Beyond Your Perimeter

Zone 3

What You Don’t Know Can Hurt You

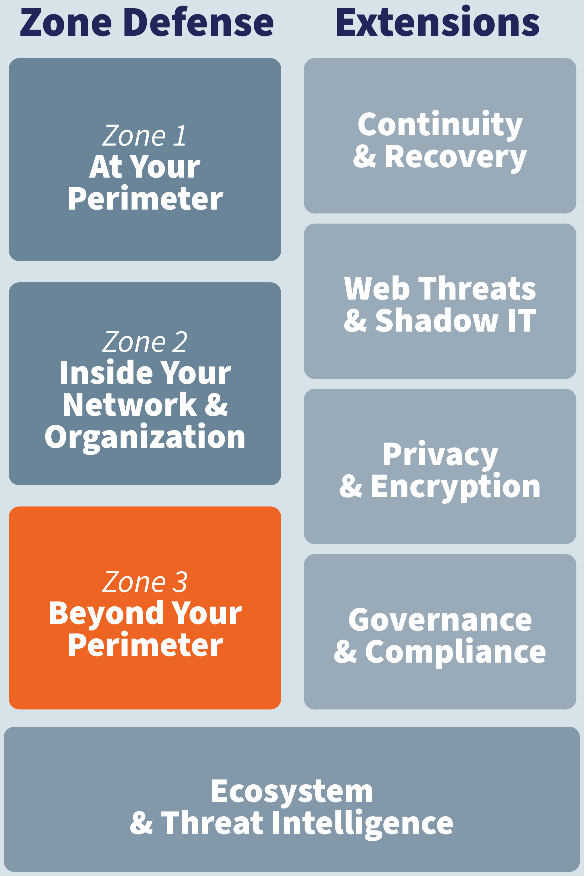
Brand impersonation attacks that exploit your good name to compromise customers and partners are devastating. They destroy trust, are extremely difficult to uncover, and even harder to shut down. And unfortunately, they’re all too easy for criminals to create.

Even unsophisticated attackers can simply register similar domains and host websites designed to trick unsuspecting visitors, damaging the brand equity it may have taken you years or decades to build. The time has come to move from defense to offense.

Protecting your organization from brand abuse is the foundation of Mimecast’s email security strategy in Zone 3 – beyond your perimeter. Essential steps include implementing DMARC to protect the domains you own, while also proactively hunting for and remediating attacks that rely on fraudulent, lookalike domains.

Email Security 3.0

Mimecast Email Security 3.0 helps you evolve from a perimeter-based security strategy to one that is comprehensive and pervasive, providing protection across three zones. These protections are enhanced by a wide range of complementary solutions, actionable threat intelligence, and a growing library of APIs.



Protecting Against Brand Imitation

When it comes to brand impersonation attacks, cyber criminals have historically been in the driver's seat. These attacks occur beyond your perimeter where visibility is low or non-existent and where remediation efforts are difficult and time-consuming. Mimecast Brand Exploit Protect is engineered to put the power back in your hands.

Using a combination of machine learning and quadrillions of targeted scans that can identify even unknown attack patterns, Brand Exploit Protect helps you detect attacks in their early stages and block them before they go live. When live attacks are discovered, they can be remediated quickly to minimize damage. The solution is engineered to help you:

- Protect customers, partners, and employees from phishing scams using similar domains.
- Identify and protect against attacks that clone your website, irrespective of the hosting domain.
- Block and take down both suspicious sites and active scams.

Integration with Mimecast's email and web security services further strengthens these defenses by allowing you to block any potentially malicious domains and URLs in your Mimecast solution at the click of a button.

Defending Owned Domains

A key component of brand exploitation attacks is often abuse of owned domains. Because many organizations have a lot of active and dormant domains, tracking and controlling them is challenging. Attackers take advantage of this complexity to send emails that appear to be from a trusted source.

Real-World Scenario

A university in Australia was being scammed by attackers who had set up a fake website, sent phishing emails to students, and harvested credentials when they logged in. How did they figure out it was happening? They didn't. Even though they weren't a customer, Mimecast detected the attack and alerted them to the situation. The university initially elected to handle it on their own; but several days later, the site was still live. They turned to Mimecast for help, and the site was taken down in less than an hour. And a few weeks later when another fake website was created, Mimecast detected it before anyone else could fall for the scam.

Protect Your Greatest Asset

Move from defense to offense with brand protection that helps you:

- Defend against imitation-based threats that target customers, suppliers, and partners.
- Extend phishing protection beyond your perimeter.
- Prevent planned brand imitation attacks.
- Quickly resolve live attacks.
- Get visibility of email traffic using your owned domains, both active and dormant.
- Move to a DMARC reject policy faster and more confidently.
- Take proactive action on suspicious and actively malicious domains and URLs.

DMARC is an industry-standard email authentication protocol that allows organizations to publish DMARC records for all their owned domains with their DNS provider. These records can be used as markers for detecting illegitimate activity and implementing DMARC reject policies.

Mimecast DMARC Analyzer is a cloud-based tool that is engineered to simplify the process of implementing, managing, and reporting on DMARC policies, helping you:

- Get better visibility of owned domains, both active and dormant.
- Simplify the process of publishing DMARC records.
- See who is sending emails on your behalf – both legitimately and illegitimately.
- Implement DMARC “reject” policies to prevent delivery of emails from illegitimate sources.
- Ensure legitimate mail is NOT blocked by DMARC policies.

One of Mimecast DMARC Analyzer’s primary benefits is the ability to maintain trust in your domains. If customers regularly receive fake emails that appear legitimate, the likelihood that they will ignore them or become suspicious is high. Mimecast DMARC Analyzer helps you get the visibility, analytics, and tools needed to easily and confidently apply DMARC policies.

Get an Integrated Approach from Mimecast

By combining full DMARC visibility, reporting, and enforcement with proactive hunting of brand abuse, Mimecast helps you protect against the malicious use of owned domains, as well as spoofing that relies on unowned domains. That’s end-to-end email and brand exploit protection from a single, trusted leader in the market.