Cofense Plus Microsoft: Better Together

What is Happening in Cybersecurity?

IT and security executives are between a rock and a hard place. Externally, bad actors are developing more complex attacks and launching them more frequently while internally CFOs and boards are calling for IT budgets and vendors to be cut.

These forces pose a difficult question to CIOs and their CISOs, **"How can I reduce my risk while simultaneously reducing the cost and complexity of my security posture?"**

Nowhere is this question more applicable than in email security, the most active and successful threat vector. **94% of malware** is delivered via email with phishing attacks accounting for over **80% of reported security incidents**. The current status quo of "My SEG will protect me" fails to keep up with the evolving threat landscape.

While legacy SEGs such as Proofpoint and Mimecast block around 98% of emails with malicious attachments (file-based attacks), they miss **half of all phishing attacks** (fileless attacks). Bad actors are taking advantage of this gaping hole in perimeter defenses and are developing more complex attacks, including Business Email Compromise (BEC) and credential phish, which make up **70% of phishing attacks**.

This increase in fileless attacks, paired with the failure of legacy SEGs to stop today's attacks, has led Forrester to say they "are slowly becoming dinosaurs" in their most recent email security wave.

IT and security executives need a comprehensive solution that accomplishes three objectives:

1. Reduce an organization's risk, cost, and complexity across their entire security posture
2. Facilitate the digital transformation of Enterprise IT and OT
3. Help overwhelmed SOCs reduce time focused on email security

How Can IT Departments Fill These Needs?

For organizations trying to accomplish these objectives, Cofense plus Microsoft is the best solution to protect against the most active and successful threat vector and strengthen your entire security posture.

Microsoft offers organizations good built-in protection with Exchange Online Protection (EOP) and offers more extensive features with Microsoft Defender that block the same number of attacks at the perimeter as legacy SEGs.

For organizations trying to accomplish these objectives, Cofense plus Microsoft is the best solution to protect against the most active and successful threat vector and strengthen your entire security posture.

But, while Microsoft attempted to improve their phishing defense with a multi-layered architecture, these features do not truly improve their effectiveness. If they couldn't catch the threat the first time, how will they help you catch it the second? Gartner agrees, and recommends organizations augment the built-in email security of their Microsoft license with a third-party email vendor.

This where Cofense comes in. Cofense enables organizations with a comprehensive anti-phishing solution that improves threat remediation time, reduces the need for additional email security vendors, and strengthens the entire security posture. This solution is called Phishing Detection and Response, or PDR, and consists of PhishMe, a phishing simulator that conditions end-users to identify IOCs and report; Cofense Reporter, which enables end-users to report suspected phish with one click and provides instant feedback on simulation; and highly automated threat remediation tools like Triage and Vision which categorize reported emails based on IOCs.

Cofense's solution is multi-dimensional and offers a unique view into the threat landscape:

- **Network Effect:** Join an almost **30-million-strong network** of human reporters around the world and across multiple industries reporting suspected phish that make it past Microsoft's and legacy-SEGs. **Over 50%** of the threats reported in your environment are reported somewhere else first, immediately arming you with the necessary IOCs to instantly remediate the threat in your environment.
- **Real-Time Posture:** Cofense Intelligence arms your Security Team with **100% Cofense-vetted intelligence** that is shared across industry leading TIPs, SIEMs, and SOARs to strengthen your entire security posture. This intelligence updates in real-time, evolving your security alongside the threat landscape.

PDR can be deployed as a managed service or by your security team.

With Managed PDR, your organization offloads your phishing defense needs to Cofense's Phishing Defense Center (PDC). The PDC is the only phishing-dedicated SOC and has multiple locations around the world:

- **Effectiveness:** The PDC responds to every reported email, and on average, accurately categorizes a reported email in **under 2 minutes at 99.998% accuracy**.
- **Availability:** Phishing attacks never stop. The PDC is designed to support global operations and is **available 24/7** to remediate reported emails.
- **SOC Operations:** Offloading the email workload from your security team allows them to focus on other threats facing your organization.

For organizations requiring a do-it-yourself approach, PDR arms your organization with all the same tools our PDC has, ensuring your security team is adequately prepared for the threat landscape:

- **Automation:** Cofense's threat remediation tools, Triage and Vision, are highly automated and help security analysts analyze and remediate threats in **under 8 minutes**.
- **Known IOCs:** With AutoQuarantine, emails with known IOCs are automatically removed from the environment.
- **Ask an Expert:** When your security team is overwhelmed or needs help with a complex attack, you can utilize our PDC to remediate the backlog.

With PDR, organizations enable their security team to detect, analyze, and remediate threats in-house.

Visit our website for more information on how Cofense plus Microsoft can help your organization respond to the evolving threat landscape. www.cofense.com

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of close to 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175