eSENTIRE

CASE STUDY

How eSentire Accelerated Email Security Efficiency with Microsoft Defender for Office 365

Overview

Phishing and spoofing attack volume has increased substantially since the onset of the COVID-19 pandemic.[1] With over 1000 customers globally and our own 24/7 operations to safeguard, maintaining an effective email security posture is extremely important. To that end, in 2020 eSentire deployed Microsoft Defender for Office 365 as our primary enterprise email security tool. The following is a summary of the results eSentire's enterprise security team has seen so far.

Company Snapshot

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, human expertise, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale.

Business and Security Outcomes

- ~$60K annual savings in software licences
- Reduction of average phishing attack investigation time from ~20 minutes to ~1 minute
- ~25% increase in automatically blocked phishing attacks
- ~80% reduction in time spent preparing and configuring quarterly phishing testing on eSentire employees

> Investigations that used to take 10, 20, or 30 minutes because of manual processes became as little as a single button click in a lot of cases.
>
> - Jason Westahaver
> Technical Lead, Enterprise Security

[1] 2020 Cybersecurity Insiders Phishing Attack Landscape Report

The Challenge

Security leader

Accounting for and mitigating the risk of human error as much as possible without impeding business operations.

Security practitioner

Dealing with increased workload due to more volume of phishing and business email compromise (BEC).

Phishing attacks in all their forms remain as frequent as ever because human error is inevitable. This is true for small companies and large companies across all industry verticals, including cyber security companies. Being a cyber security service provider for over 1000 customers globally makes eSentire a prime target for attackers. By extension, eSentire needs to have the ability to successfully defend a substantial amount of phishing attacks on a daily basis. At a high level, this entails keeping eSentire employees hyper vigilant through regular testing and training while maintaining an ongoing robust detection and response operation.

The Selection of Microsoft Defender for Office 365

Security leader

Microsoft Defender for Office 365 is highly integrated with Microsoft Exchange Online and critical business applications, minimizing friction while increasing visibility and protection.

Security practitioner

The high degree of integration with the rest of the Microsoft security platform and automation of phishing investigations made for an easy choice.

eSentire made the decision to fully invest in Microsoft 365 E5 in 2019. From there, the enterprise security team looked at opportunities to consolidate existing solutions under Microsoft security functions on a case-by-case basis. In the context of email security, eSentire tested Microsoft Defender for Office 365 against its existing enterprise email solution for several months and the benefits became very apparent early on.

~90%
Decrease in phishing investigation times

~25%
Increase in phishing test email delivery rate

"Before (Microsoft Defender for Office 365), phishing investigations were much more manual. Manual processes and manual correlation," said Jason Westhaver, eSentire's Technical Lead for Enterprise Security. "Investigations that used to take 10, 20, or 30 minutes because of manual processes shrunk down to as little as a single button click in a lot of cases."

Workflows around regular employee phishing testing were highly streamlined as well. Typically, the experience of making sure phishing tests make it through email security preventative measures can take several hours of trial and error, navigating allow/deny lists, sandboxing measures, and email tagging. Even then, getting to approximately 75% delivery was often considered a victory. Conversely, Microsoft Defender for Office 365 has the benefit of being directly integrated with the Microsoft Exchange cloud email platform and as a result, the hours long tuning process is completely circumvented. 100% delivery rates are now the norm, ensuring every employee is tested and human error risk across the company is properly quantified.

Finally, Microsoft Defender for Office 365 exists as one component of a greater suite of threat prevention, detection, and response tools that encompasses endpoint, cloud, and identity risk data that can be easily accessed, driving further investigation efficiencies.

Outcomes

Security leader
Less complexity, reduced risk of email threats, and improved ROI on security spend.

Security practitioner
Substantial time and resources saved from better prevention and streamlined investigations.

Moving email security under Microsoft Defender for Office 365 allowed eSentire to save approximately $60,000 per year by moving on from its previous enterprise email security solution. A 90% decrease in average phishing investigation times also created substantial operational savings. Consistent and 100% delivery of phishing testing allows for the reliable tracking and reporting of employee risk over time, informing enterprise security strategy. Overall, cost analysis have shown that the investment in the overall Microsoft 365 Defender suite of tools has contributed to a 50% total reduction in enterprise security costs.

> Employee resilience to email threats is of upmost importance to our security program. Microsoft's tools give us the data we need to inform and improve this aspect of our posture.
>
> - Peter Romano, CISO

Following the successful deployment, eSentire's Enterprise Security team worked closely with the product team in the development of an email Managed Detection and Response service, which is now generally available and allows customers to increase their resilience against email attacks while maximising ROI on investments in Microsoft 365 security tools.