eSENTIRE

Microsoft Partner Gold Security Microsoft

Member of Microsoft Intelligent Security Association Microsoft

DATA SHEET

eSentire MDR with Microsoft Defender for Office 365

Managed email threat prevention, detection, and response

Improve ROI on Security Spend

We combine leading email security technology with our team's industry leading security expertise to optimally configure Microsoft Defender for Office 365. Get improved ROI and reduce your risk of email threats.

Deeper Investigation Capabilities

Get streamlined user-reported phishing investigations and feedback. Our Elite Threat Hunters and 24/7 SOC teams analyze suspicious "grey area" security events and correlate additional detections in multi-signal MDR investigations.

Complete Response and Containment

Enhance your MDR strategy with more points of threat containment and response enforcement. You get 24/7 coverage from our expert SOC analysts who respond to email threats like phishing and business email compromise (BEC) around-the-clock.

Strengthen Your Security Posture

Complete feedback loops and encourage a positive security culture among your users. Our leading Threat Research Unit works tirelessly to make sure you stay ahead of the evolving threat landscape.

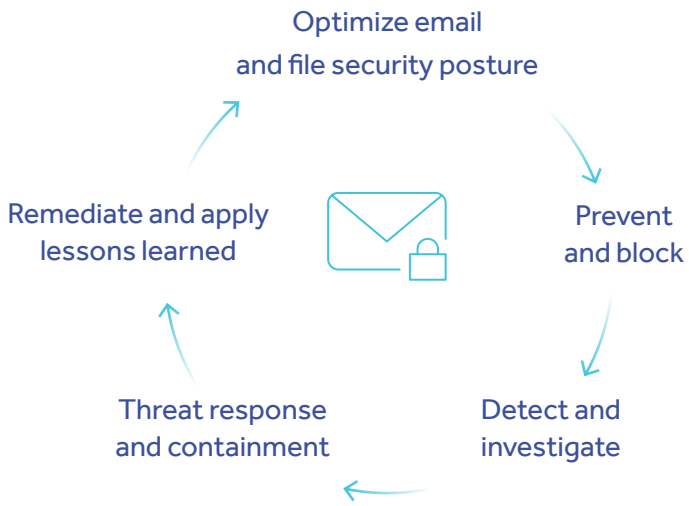
Your Challenges

Email attacks are accelerating	**#1** Threat Action in Breaches[1]	**#1** Vector for Malware
Increased attack volume & sophistication	**$1.8B** lost to Business Email Compromise (BEC) in 2020[2]	**53%** increase phishing attacks post-COVID 19
Your team lacks the cybersecurity resources to investigate and respond 24/7	**40** phishing attack remediations per day on average[3]	**6.5 hrs** per day investigating assuming 10 minutes per remediation for alone
You're dealing with vendor sprawl and budget constraints	**39%** of organizations receive alerts from seven or more tools[4]	**51%** are concerned about security spending post-COVID

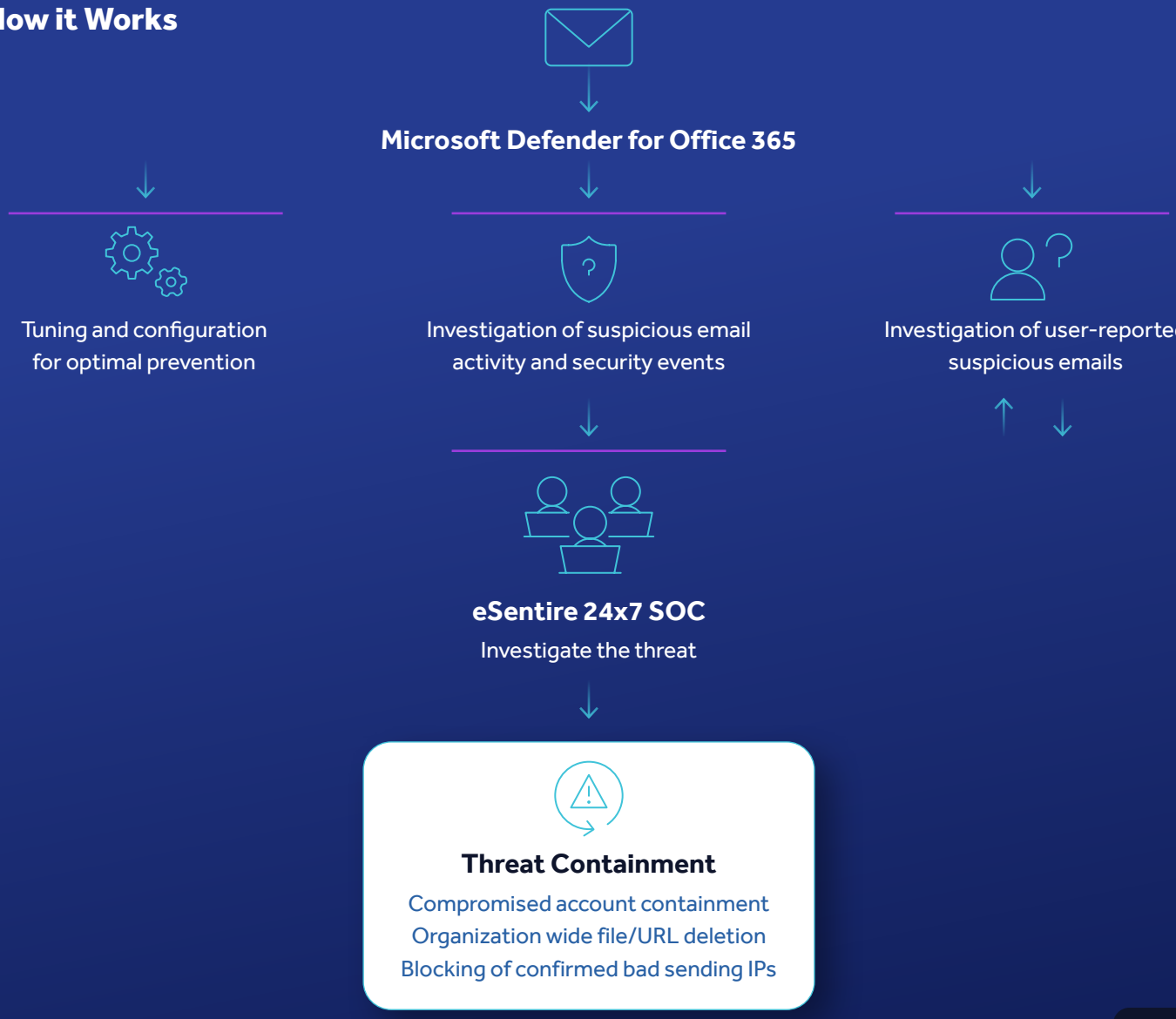
[1]2020 Verizon Data Breach Investigations report,[2] FBI IC3 Report, 2020 Phishing Attack Landscape Report,
[3]2020 Phishing Attack Landscape Report,[4] ISC2, Neustar, 2020

The Solution

eSentire MDR with Microsoft Defender for Office 365 provides robust email threat detection, investigation, and complete response on a 24/7 basis. Our dedicated security experts from eSentire's global Security Operations Centers (SOC) leverage Microsoft Defender for Office 365's highly integrated email security solution to detect and hunt both common and sophisticated email threats before they disrupt your business.



How it Works



Features

Automated Blocking and Prevention
Help prevent a wide variety of volume-based and targeted attacks from impacting your business, including business email compromise, phishing, and malware.

Expanded Threat Detection and Containment
Email sandboxing, account isolation, and malicious email and file deletion are among the containment actions available to help stop threats.

User-reported Phishing Investigations
Help augment or create a positive user-escalation feedback loop for suspicious emails. Our experienced team investigates suspicious emails reported by users and investigate threats.

Integrated Threat Intelligence
We connect Microsoft Defender for Office 365 with eSentire's dynamic threat intelligence to help block emerging threats and improve outcomes.

Microsoft Defender for Office 365 Optimization
We include professional services and guidance on the configuration of the Microsoft Defender for Office 365 email and file security tool.

24/7 Coverage
Our expert analysts monitor, investigate, and help respond to events around the clock from eSentire's two global Security Operations Centers (SOC).

Complete Response and Full Incident Lifecycle Support
We respond to and help eradicate threat actor presence with co-managed remediation from initial detection to confirmation of hardening and monitoring for re-entry.

Atlas XDR Cloud Platform
Our machine learning powered XDR platform ingests and correlates signals from network, logs, cloud environments and Microsoft 365 Defender. Patented machine learning eliminates noise, enables real-time detection and automatically help blocks threats on your behalf.

Enhanced by the eSentire Threat Response Unit
Our elite threat team manages counter-threat research and development, deployment, and maintenance to help keep your organization ahead of the threat landscape.

MITRE ATT&CK Mapped
From the broad tactic categories down to individual technique IDs, all detectors and runbooks are mapped to the MITRE framework to optimize investigations.

The eSentire Difference

Many MDR and MSSP providers ingest alerts from common email security vendors. eSentire MDR goes beyond alerts and delivers superior security outcomes. With eSentire MDR for Microsoft Defender for Office 365 we deliver integrated investigations, multi-signal detection, complete containment and response, and posture hardening for email threats.

	Other MSSP/MDR	eSentire MDR with Microsoft Defender for Office 365
Configuration and tuning	✔	✔
Direct API integration	✖ (Typically log collection only)	✔
User-reported phishing investigations	✖	✔
Email account containment	✖	✔
Malicious file and URL deletion	✖	✔
XDR Integrated	✖	✔

Maximize Your Investment in the Microsoft Security Stack with eSentire MDR

Microsoft Defender for Office 365 is a part of the Microsoft 365 Defender extended detection and response (XDR) tool set that is included in Microsoft 365 E5 level licencing.

eSentire MDR for Microsoft combines our multi-signal detection, 24/7 threat hunting, deep investigation, and industry leading response capabilities with your existing investment in the Microsoft 365 ecosystem. You can significantly reduce overall security spend and maximize ROI while substantially reducing risk of suffering a business-disrupting breach.

Outcomes

- ✔ Rapid deployment and quick time to value
- ✔ Maximizes ROI on Microsoft 365 investment
- ✔ Optimized and hardened state of email security
- ✔ Automatic blocking of commodity email threats
- ✔ Improved defenses against business email compromise
- ✔ Improved MITRE ATT&CK coverage
- ✔ Robust, rapid response
- ✔ 15 minute Mean Time to Contain
- ✔ Reduced security total cost of ownership (TCO)
- ✔ Minimized incident recovery timeframe
- ✔ Mitigation of potential business disruption

If you're experiencing a security incident or breach contact us 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, 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, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.