FORTRA

SOLUTION BRIEF (ALERT LOGIC)

Alert Logic & Microsoft Defender for Endpoint

Enhancing the Security Value of Microsoft Defender

Microsoft Defender for Endpoint provides protection, detection, and response capabilities as a key component of any security strategy. But it lacks 24/7 monitoring, rapid investigations, proactive threat hunting, and coverage beyond endpoints. The result? Threat actors can circumvent EDR technologies and find a way to your critical assets and users.

Avoid this result by enhancing Defender for Endpoint with a solution that reduces the likelihood of and impact of compromise and elevates your security outcomes.

Better Together: Protect, Detect and Respond with Fortra XDR & Defender for Endpoint

You're facing modern-day multi-vector threats that necessitate a streamlined, integrated, and comprehensive security strategy.

Take your Defender for Endpoint to the next security level by integrating it with Fortra XDR. Built off Fortra's Alert Logic's 20 years of trusted experience in the managed services arena, Fortra XDR provides 24/7 monitoring through our global security operations center (SOC) experts for rapid threat detection, threat hunting, containment, and guided remediation. This ensures breaches are halted from progressing, minimizing their impact, and bolstering your security posture to withstand future threats. And our coverage is across the entire attack surface including endpoint, network, identity, and cloud.

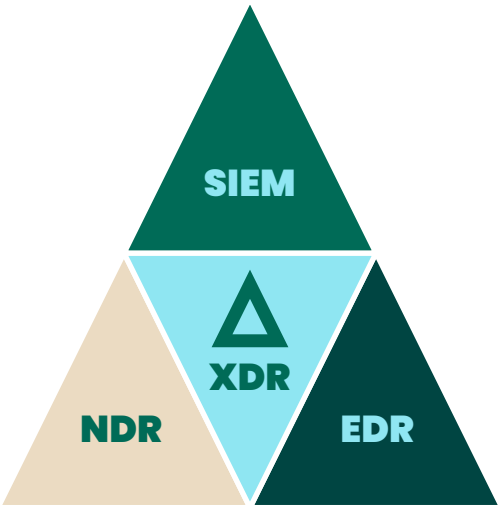
By integrating Microsoft Defender for Endpoint with Fortra XDR, you immediately scale your security capabilities beyond just the endpoint, enabling you to:

- Enrich your Defender for Endpoint alerts with Fortra EDR telemetry, network traffic inspection, enhanced logging, and file integrity monitoring and applied threat intelligence
- Correlate threats across the entire IT environment, including identity, cloud, containers, network devices, and third-party security tools
- Coordinate response across multiple security tools and sources including endpoint, network, and cloud sources
- Receive SOC investigations into Defender for Endpoint alerts to identify ongoing compromises, contain threats, and provide comprehensive remediation plans

PRODUCT SUMMARY

Key Benefits

- Enhance your visibility with EDR, network IDS, logs, FIM, and applied intelligence
- View your security alerts in a single console
- SOC validation and enrichment of Defender for Endpoint alerts
- Automated and managed response playbooks
- Remediate post compromise activity detected by Defender for Endpoint



Why Organizations Chose Fortra XDR to Enhance Defender for Endpoint

Complete Visibility

A single pane of glass for your alerts providing security insights, dashboards, and audit-ready reports across your entire IT environment

Managed tuning

Expert-tuning exercises are conducted with users, combining our security expertise with contextual insights into your IT operations to minimize noise and limit missed attacks

SOC investigation under 15-minute SLA

Critical detections and blocks triggered by Defender for Endpoint are quickly investigated to guarantee rapid threat validation

Enriched with additional telemetry (endpoint and beyond)

SOC-enriched Defender for Endpoint alerts with network traffic events and logs across your infrastructure, identity services, cloud, and other security controls

Multi-vector threat correlation

Combine endpoint detections with deep analytics across your entire IT environment for comprehensive threat detection and accurate response

Managed threat containment

24/7 threat containment to disrupt attackers and prevent further infection (while remediation plan is applied)

Enhanced response capabilities

Combine Defender for Endpoint response with automated response playbooks actions across identity, perimeter, and cloud to take the right containment action to prevent threats from progressing

Fortra Threat Intelligence

Global intelligence and shared machine learning engines are aggregated across tens of thousands of Fortra customers to provide deep analytics and empower analysts to make timely and accurate decisions

Cost effective

Leverage existing licenses from Microsoft E3 and E5 and deliver on the security outcomes of Microsoft tooling

Avoid vendor lock in

With Alert Logic, you'll have a security ally that augments your evolving security strategy today and tomorrow, with broad integrations into third-party security tools, overlayed threat intelligence, and native capabilities. Unlike other managed solutions, if you change your EDR solution in the future, you'll still be able to integrate with Fortra XDR. We're with you for the long term as you evolve your security strategy.

For more information, please visit **AlertLogic.com.**

How It Works

Collection

As part of the managed onboarding process, security-relevant sources will be configured for collection. An API integration will be configured to collect Defender for Endpoint data from Azure Event Hub. Collection allows for search and reporting for customers and SOC analysts via the Alert Logic console, creating a single pane of glass security view.

Detection

Alert Logic's broad and deep analytical coverage of logs and network IDS events integrates with Defender for Endpoint as a standard feature of our detection and response solutions. In addition to Defender for Endpoint alerts, potential incidents addressed via this integration include:

- Malicious tools
- Malware/virus spread to multiple hosts
- PowerShell and living off the land (LOTL) attacks

Although Defender for Endpoint blocks certain attacks, some of its alerts are only triggered on potentially malicious activity and take no action. Even an alert where a block was triggered can be indicative of an attacker already having access to a machine, user, or network. When Defender for Endpoint has identified post-compromise activity, it is crucial that alerts are investigated so initial access can be identified and remediated.

Alert Logic SOC analysts provide peace of mind by investigating alerts, validating the findings, scrutinizing surrounding data, and cross-correlating with additional alert sources. This provides a complete picture of the compromise to trigger appropriate containment actions and guide you through conclusive remediation to prevent reinfection.

Response

Alert Logic's automated response helps organizations minimize the impact of a breach with the right balance of automation and human interaction. The embedded SOAR capabilities can be configured to trigger the "isolate host" action in Defender for Endpoint when the pre-defined triggers are met. Effective automated response is about taking the appropriate action to contain a threat, which is why we advise on recommended triggers for each response playbook. Additionally, playbooks can disable a compromised Azure or on-premises active directory account and block external attackers at the perimeter.

As well as using Defender for Endpoint in automated response playbooks, our SOC can take managed containment actions via the Fortra agent, stopping threats in their tracks.

Alert Logic provides a robust, scalable, and seamlessly integrated approach to fortify your Defender for Endpoint solution and protect your entire IT estate. By combining automated response with expert guidance, we equip you with the necessary tools to reduce time-to-resolution for security-strapped teams, thereby mitigating potential damage to your business. Maximize your investment in Microsoft's Defender for Endpoint with Alert Logic's detection and response solutions.

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.