

Managed Defense for Microsoft Defender for Endpoint

Highlights

- Protect and defend in minutes**
 Deploy quickly and easily to gain immediate coverage.
- Quickly disrupt and respond**
 Support your response with the collective knowledge and experience of Mandiant.
- Know more about attackers**
 Get immediate access to intelligence aligned to SOC needs.
- Add dedicated experts**
 Mandiant experts advise your team and elevate your program.
- Gain transparency**
 Track alerts, investigations and hunt missions in real time via Managed Defense portal.

Managed detection and response (MDR) service delivered by frontline experts

Security teams are overwhelmed by a relentless flood of alerts, far exceeding their capacity to respond effectively. Even with powerful tools that detect advanced attacks and help manage response, organizations often lack the needed experience to prioritize events that matter.

Microsoft Defender for Endpoint customers can enhance their technology with the support of experts who routinely respond to and protect against motivated adversaries. Mandiant Managed Defense is a managed detection and response (MDR) service that protects and defends with frontline experts and nation-grade threat intelligence.

Protect and defend with Mandiant experts

Microsoft Defender for Endpoint customers can join forces with experienced Managed Defense professionals who are constantly fueled by Mandiant's global cyber threat intelligence and incident response experiences gained on the frontlines of the world's most consequential cyber attacks. This combination of knowledge and experience drives more effective monitoring and detection to address the impactful events and use proven response tactics so you can take swift, decisive action.



How it works

With simple, quick onboarding, Managed Defense offers around-the-clock monitoring and alert prioritization. Mandiant experts swiftly scope, investigate and prioritize alerts with context from nation-grade threat intelligence.

Fueled by up-to-the-minute threat intelligence, Managed Defense's threat hunting team designs and executes hunt missions to reveal the stealthiest threat actors. Mandiant threat hunting combines powerful data analytics, automation and elite experts with intuition and frontline experience. You can follow our hunters as their work unfolds in the Managed Defense portal. Each mission is mapped to MITRE ATT&CK® and includes related intelligence so you can take decisive action throughout your environment.

You are notified immediately when evidence of compromise has led to an investigation. Managed Defense partners with your team to contain compromised assets and quickly scope and investigate incidents. Together we form actionable remediation recommendations for an effective response.

Benefits

- **See alerts that matter.** Mandiant experts identify, investigate and prioritize alerts saving you time and effort.
- **Gain threat context.** Mandiant threat intelligence enriches priority alerts to inform decision making.
- **24x7 coverage.** Around-the-clock alert monitoring from our global Managed Defense Security Operation Centers.
- **Expose hidden threat actors.** Benefit from ongoing hunt missions driven by up-to-the-minute threat intelligence and mapped to MITRE ATT&CK® framework.
- **Contain impacted hosts.** Reduce the overall impact to your organization by containing impacted hosts quickly.
- **Rapid Response.** Mandiant experts quickly assess and contain threats, helping you resolve incidents without the added cost of full incident response.
- **Effective remediation.** We perform rapid investigation and remediation based on the collective knowledge of Mandiant.
- **Elevate your defenses.** Improve your security posture with ongoing assessment and real-world strategies.

Why Managed Defense

- **Experience**
Draw on the experience of Mandiant incident response teams, who spend 200,000+ hours per year on the most impactful breaches
- **Swift detection and response**
Investigate, remediate and respond in minutes, not hours
- **Cost effective**
Development and maintenance of in-house capabilities can take a lot of time, money and resources
- **Intelligence**
Access to nation-state grade intelligence collection supported by 300+ intelligence analysts
- **Effective defense**
 - More than 2,700 unique detection rules created from frontline observations in 2023