Mandiant

DATASHEET

Managed Defense for Trellix

Benefits

- **Supercharge existing technology investments**
  Get more from your security controls with expert monitoring and investigation by Mandiant defenders.
- **Add needed expertise**
  Receive 24x7 coverage and critical guidance from experts who detect and respond to the most impactful global breaches every day.
- **Rapidly discover active attacks**
  Reduce dwell time with Mandiant threat hunters who leverage the latest indicators of compromise to find sophisticated attackers in your environment.
- **Accelerate response**
  Contain and remediate threats before they impact the business with actionable response guidance.
- **Understand high-impact threats**
  Access nation-grade threat intelligence operationalized through each phase of detection and response.
- **Gain security transparency**
  Track alerts, investigations and hunt findings in real-time via the Mandiant Advantage portal.

Expertise for 24x7 monitoring across endpoint, network, email and cloud

Maintaining visibility and control over the entire enterprise is crucial to detecting and responding to sophisticated attacks. For security teams that lack threat insights and skilled resources, Mandiant Managed Defense combines Mandiant expertise with industry leading protection, detection and response technologies from Trellix to protect and defend your business.

"We know that Mandiant is doing a great job and our internal teams canfocus on their core objectives without worrying."

— Director of Risk and Controls, US-based Healthcare Company

Managed Defense complements internal security teams with dedicated experts who provide organizations with 24x7 monitoring of your Trellix endpoint, network and Helix technologies to identify anomalous behavior and prioritize critical threats. This service uses the latest threat intelligence and indicators of compromise (IOCs) collected from Mandiant incident responders on the frontlines every day to detect high-impact threats in an environment. Organizations gain access to advanced security capabilities such as attacker behavior investigation and analysis, proactive threat hunting and incident response.

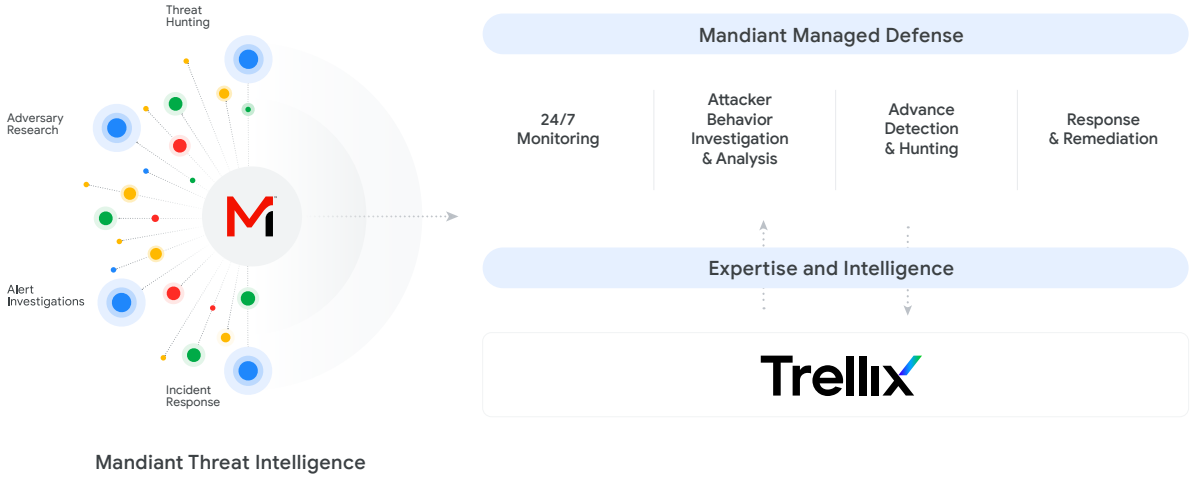

FIGURE 1. How Mandiant Managed Defense works with Trellix.

Expertly enable your critical technologies

Managed Defense integrates with a range of security tools, giving you the option to retain your existing controls or modernize to preferred tools at your own pace. The Managed Defense Portal enables your in-house security teams to see targeted threats and follow Managed Defense experts as they investigate and respond to those threats.

Take a decisive, intelligence-led approach

Managed Defense uses up-to-the-minute threat actor, malware and vulnerability tracking to help prioritize your alerts and understand attacker motivations behind associated security events. With this intelligence-led approach, your security team can focus on what matters most and learn how to respond to and remediate critical threats more effectively.

Expose hidden adversaries with proactive hunting

The Managed Defense threat hunting team designs and conducts hunt missions to reveal the stealthiest threat actors. Mandiant threat hunting brings powerful data analytics and automation together with elite, battle-tested experts. Each mission is mapped to the MITRE ATT&CK® framework and includes related intelligence so you can take decisive action throughout your environment.

Protect and defend with Mandiant experts

The Mandiant team of veteran defenders, analysts, and threat hunters work with your security team to effectively monitor, detect, triage and investigate incidents.

- **Security operations center (SOC) analysts** from all four of our global facilities operate like detectives. They gather contextual clues from your event data to form a complete picture of a threat and identify an intrusion at the earliest stage possible.
- **Threat hunters** systematically combine knowledge, intuition, and automation to proactively search for covert signs of an active or attempted compromise. They apply front-line knowledge of how threat actors operate and successfully conduct missions for all Managed Defense customers.
- **Detection engineers** codify and use real-time knowledge of attacker tactics, techniques and procedures. They implement detection logic to ensure rapid identification and eradication of threats.
- **Incident responders** help your organization by responding to threats identified within your environment. They determine the full scope of the attack, assess root cause and guide you through remediation and recovery.
- **Managed Defense consultants** serve you in an advisory capacity. They acquire deep knowledge of your environments and manage investigation and response.