Trellix

DATA SHEET

Trellix® SecondSight Threat Hunting Service

Highlights

Multi-product Availability
Trellix SecondSight provides specialized hunting expertise for Trellix EDR, NDR, and Email Security – Cloud customers alike.

Defined Outcomes
Trellix SecondSight Enterprise offers a clear, predictable quota of custom and validation hunts for direct tactical support.

Deep Forensic Expertise
Built for organizations that require expert human analysis of complex telemetry to distinguish between admin activity and attacks.

See what others miss. Hunt what others ignore.

Trellix SecondSight is a premier threat hunting service designed to augment your existing security operations. While your team manages daily alerts, SecondSight hunters dive into the "gray space" of low-confidence signals within your Trellix endpoint, network, or email telemetry. By combining Trellix's global AI-driven analytics with elite human expertise, we identify the subtle indicators of an active breach that automated tools often surface but cannot fully interpret.

The "human-in-the-loop" philosophy

At Trellix, we know that automated products are excellent at surfacing telemetry and weak signals. However, attackers often hide in the noise of legitimate administrative activity.

- **The Starting Point.** Our hunters use the specialized telemetry generated by your Trellix products—signals which may not yet trigger a "critical" alert—as the catalyst for an investigation.
- **The Expert Difference.** We apply human knowledge to the product data to understand the intent behind the signal. This allows us to confirm if a specific behavior within the endpoint, network, or email environment actually constitutes an active, sophisticated breach. By sifting through the gray space of your product data, we find the critical evidence of an intruder that automated filters might overlook as background noise.

Augmented intelligence

SecondSight is not a replacement for your SOC; it is a force multiplier for your team. While your analysts focus on managing and monitoring your environment, Trellix hunters work in parallel, providing a "second set of eyes" on your product telemetry to ensure that subtle, sophisticated movements don't go unnoticed.

Trellix Core and Enterprise tiers

Available in Core and Enterprise tiers, Trellix SecondSight provides the proactive notifications and specialized hunting capabilities needed to stop sophisticated attackers. Trellix SecondSight Core is included with Trellix Endpoint Detection and Response (EDR), Trellix Email Security – Cloud, and Trellix Network Detection and Response (NDR). It provides proactive alerts upon the discovery of threats.

Trellix SecondSight Enterprise delivers high-touch threat hunting services with direct tasking and reporting. Available as an annual subscription, it enables you to move beyond passive monitoring and direct your defense with precision. With four custom hunts and four validation hunts available per quarter, you can task Trellix hunters to investigate specific concerns within your telemetry or confirm that a remediation effort was 100 percent successful.

Feature	Trellix SecondSight Core	Trellix SecondSight Enterprise
Availability	Included with Trellix EDR, Email Security – Cloud and/or NDR	Annual subscription / Add-on
Notification	Proactive alert upon discovery of threats	Prioritized “front-of-line” investigations and notifications
Custom hunts	Not available	Four requests per quarter
Validation hunts	Not available	Four requests per quarter
Reporting	Not available	Weekly activity reports

To learn more about Trellix SecondSight threat hunting service, please visit trellix.com/secondsight.