kaspersky BRING ON THE FUTURE

Kaspersky Threat Hunting

Most security teams take an alert-driven approach to cybersecurity incidents, reacting only after an incident has already taken place. Meanwhile, new threats move in under the radar, leaving you with a false sense of security – literally. Businesses are increasingly recognizing the need to proactively hunt out threats lying undiscovered but still active within their corporate infrastructures.

Product benefits:

- The reassurance of knowing that you are continuously protected against even the most innovative threats
- Reduced overall security costs without the need to employ a range of in-house security specialists
- Focusing expensive in-house resources on those critical tasks that really require their involvement
- All the major advantages from having your own security operations center without having to actually establish one

Kaspersky Threat Hunting delivers advanced, round-the-clock protection from the growing volume of threats circumventing automated security barriers, providing relief to organizations struggling to find specialized staff or with limited in-house resources.

Its superior detection and response capabilities are supported by one of the most successful and experienced threat hunting teams in the industry. Unlike similar offerings on the market, Kaspersky Threat Hunting leverages patented machine-learning models, unique ongoing threat intelligence and a proven track record of effective targeted attack research. It automatically strengthens your corporate resilience to cyberthreats while optimizing your existing resources and future IT security investments.

Product highlights

- Fast, scalable turnkey deployment enables an instantly matured IT security function without the need to invest in additional staff or expertise
- Superior protection against even the most complex and innovative non-malware threats prevents business disruption and minimizes overall incident impact
- Completely managed or guided incident response provides a swift reaction while keeping all response actions within your full control
- Real-time visibility across your assets and their protection status delivers ongoing situational awareness through various communication channels

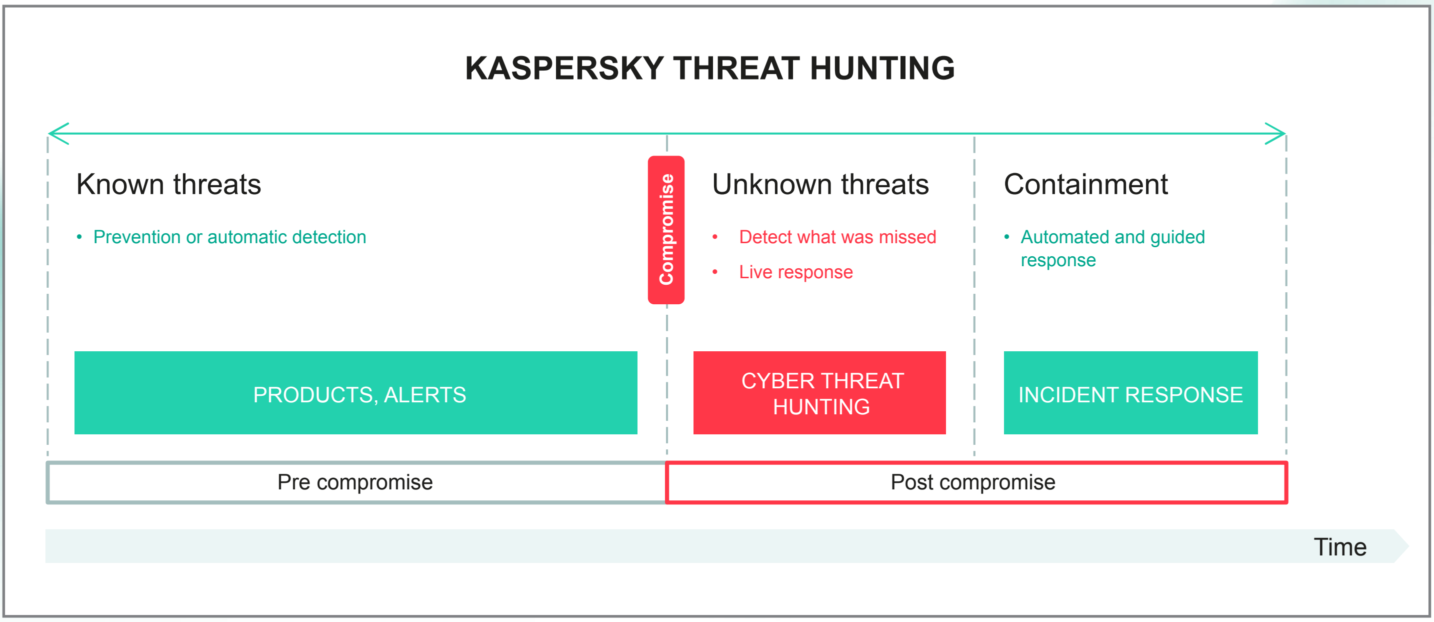


Figure 1. Kaspersky Threat Hunting

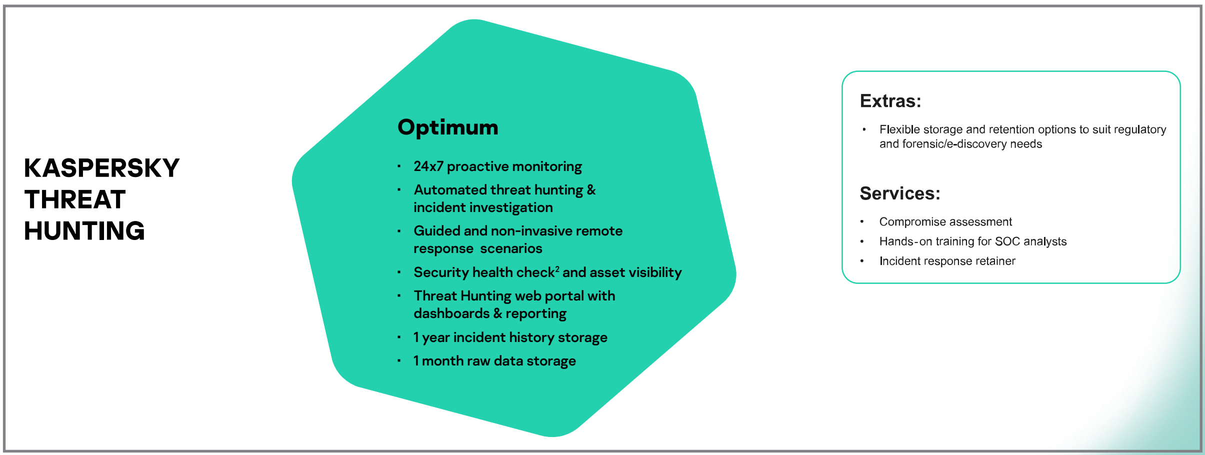
Supported products:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac[1]
- Kaspersky Security for Windows Server
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

How it works

Kaspersky Threat Hunting validates product alerts to ensure the effectiveness of automatic prevention and proactively analyzes system activity metadata for any signs of an active or impending attack. This metadata is collected via Kaspersky Security Network, and is automatically correlated in real-time with Kaspersky's unequalled threat intelligence to identify the tactics, techniques and procedures used by attackers. Proprietary Indicators of Attack enable the detection of stealthy non-malware threats mimicking legitimate activity. The product adapts to your infrastructure during the first 2-4 weeks, to ensure zero false positive rates, confirming with you what is legitimate and what is not.

Kaspersky Threat Hunting features multiple deliverables to suit the needs of organizations of every size and industries with varying IT security maturity levels (Figure 2). **Kaspersky Threat Hunting Optimum** instantly raises your IT security capability without the need to invest in additional staff or expertise and provides resilience to evasive attacks through its fast, turnkey deployment.



KASPERSKY THREAT HUNTING

Optimum

- 24x7 proactive monitoring
- Automated threat hunting & incident investigation
- Guided and non-invasive remote response scenarios
- Security health check[2] and asset visibility
- Threat Hunting web portal with dashboards & reporting
- 1 year incident history storage
- 1 month raw data storage

Extras:

- Flexible storage and retention options to suit regulatory and forensic/e-discovery needs

Services:

- Compromise assessment
- Hands-on training for SOC analysts
- Incident response retainer

Figure 2. Kaspersky Threat Hunting details

Automated threat hunting included in Threat Hunting Optimum uses automatic detections made by proprietary Indicators of Attack for further validation, investigation and identification of new threats.

A set of complementary optional elements tailor the functionality of the product to your specific requirements, providing enhanced flexibility when needed:

- Flexible storage and retention options to suit regulatory and forensic/e-discovery needs
- An incident response retainer, bringing the full weight of Kaspersky's expertise to bear on the resolution of your security incident
- A comprehensive compromise assessment to verify that your existing security controls are sufficient
- Hands-on training for SOC analysts to ensure your overall incident preparedness

Countering targeted attacks requires extensive experience as well as constant learning. As the first vendor to establish, almost a decade ago, a dedicated center for investigating complex threats, Kaspersky has detected more sophisticated targeted attacks than any other security solution provider. Leveraging this unique expertise, Kaspersky Threat Hunting maximizes the value of your Kaspersky security solutions by delivering a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one.

[1] Planned to be supported in Q2 2021

[2] Planned to be supported in Q1 2021

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.