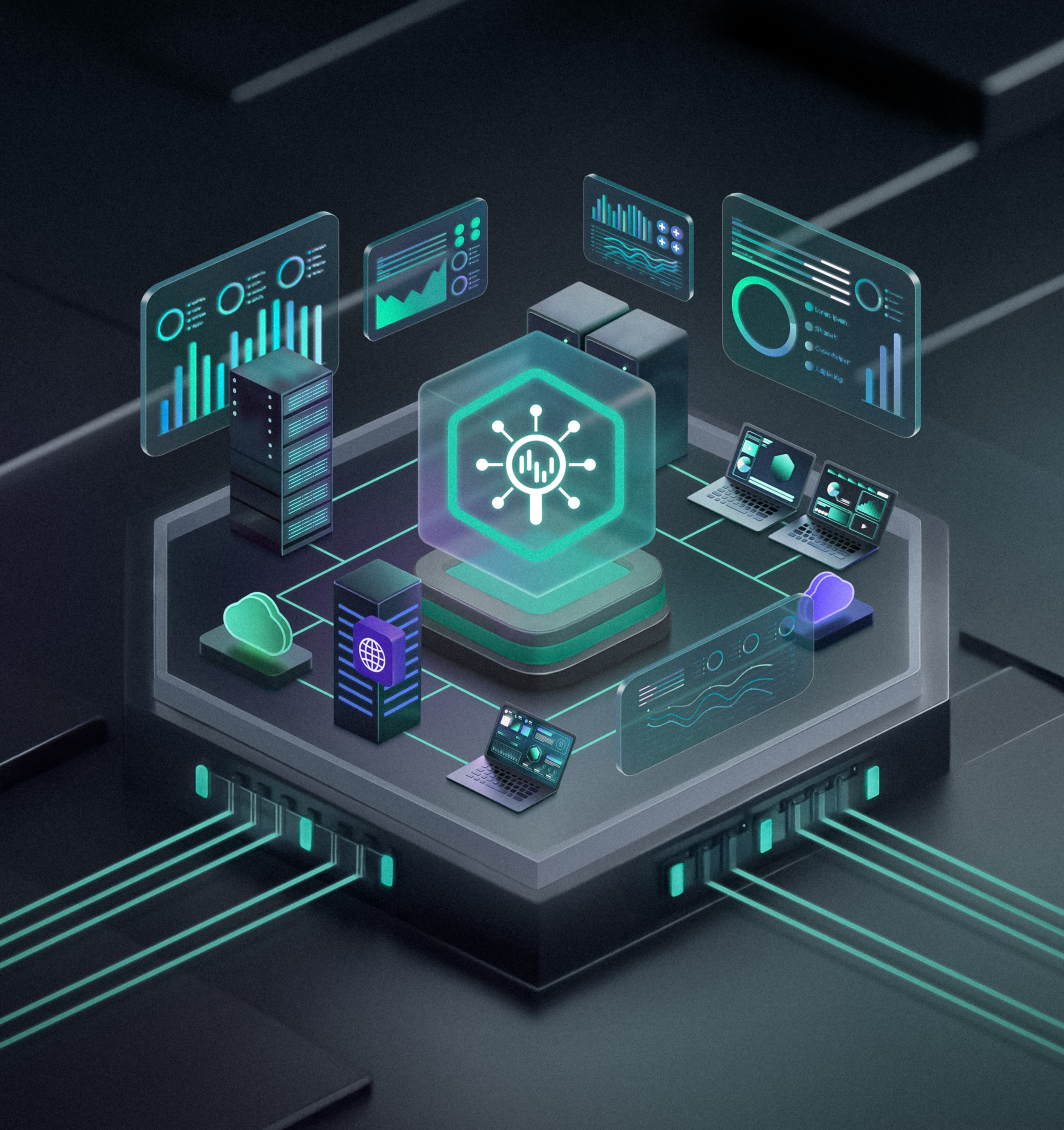


Datasheet

Kaspersky SIEM

Transform your security operations with our next-generation solution, powered by AI and enhanced with world-class Threat Intelligence

kaspersky bring on the future

Maximize the impact of your security operations

Large organizations are facing a growing number of Advanced Persistent Threats (APT). In 2024, APTs were detected in one in four businesses and accounted for 43% of all high-severity incidents[1]. The consequences are costly, ranging from business disruption to financial losses and long-term reputational damage.

Security teams are under unprecedented pressure. Protection systems generate massive data volumes, driving up storage costs and making SIEM deployments expensive. Skilled experts are scarce, while existing teams are overwhelmed — 70% of Security Operation Centers (SOC) struggle to keep pace with the flood of alerts[2]. On top of this, the complexity of administrating SIEM systems further strains already limited resources.

Even the most experienced Security Operation Centers risk losing efficiency and impact without today's AI-driven tools to help them cut through the noise and focus on what matters most.

Kaspersky SIEM is for organizations with complex IT infrastructures, high volumes of data and strict regulatory requirements. The product is MSSP-ready with built-in multitenancy support.

These organizations recognize that effective security depends not only on prevention but also on the ability to detect, analyze and respond to threats in real time across diverse systems.

Equip your team with an AI-powered SIEM backed by world-class Threat Intelligence

Kaspersky SIEM is a next-generation solution designed to help your security team manage and analyze incoming security data. It excels at:

- Collecting, processing and storing events from diverse sources, including Kaspersky products, operating systems, third-party applications, security tools and databases.
- Analyzing and correlating incoming data in real time, enriching it with industry-leading Threat Intelligence to detect suspicious activity.
- Providing timely alerts to enable rapid incident investigation and response.
- Storing data for an extended period without going over budget for pricey storage hardware — thanks to hot and cold storage options with seamless simultaneous search functionality.

By unifying logs from security sources and correlating them in real time, Kaspersky SIEM empowers your analysts with the full visibility and context needed to respond efficiently.

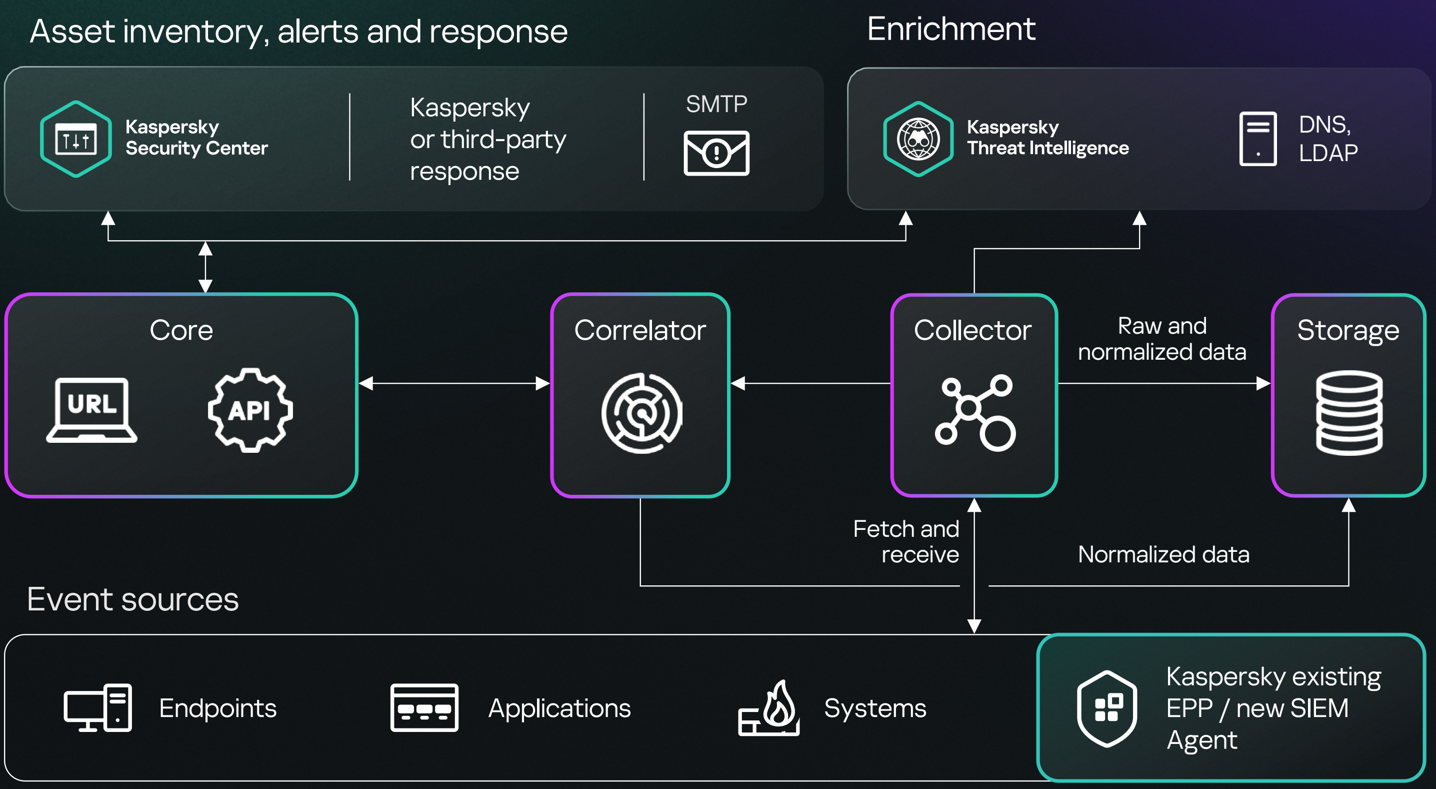
It offers advanced search and analytics capabilities that allow your threat hunters to uncover previously unknown threats. Historical data analysis and statistical baselining with the UEBA detection ruleset help your team identify anomalies and stop sophisticated attacks.

With Kaspersky SIEM, your SOC gains the visibility, intelligence and efficiency it needs to turn overwhelming data into actionable security insights. The solution can operate without internet connectivity, ensuring full data sovereignty.

[1] Kaspersky Managed Detection and Response analyst report for 2024

[2] Kaspersky Report: The portrait of modern information security professional, 2024

How it works


Asset inventory, alerts and response
Kaspersky Security Center
Kaspersky or third-party response
SMTP
Enrichment
Kaspersky Threat Intelligence
DNS, LDAP
Core
URL
API
Correlator
Collector
Raw and normalized data
Storage
Fetch and receive
Normalized data
Event sources
Endpoints
Applications
Systems
Kaspersky existing EPP / new SIEM Agent

Thanks to the solution's microservice architecture, your administrators can create and configure the microservices they need in order to use Kaspersky SIEM as a full-fledged SIEM tool or a log management system.

Kaspersky SIEM is built on an Open Single Management Platform[3], integrating both Kaspersky and third-party products into a centralized security system. It forms an essential part of a comprehensive defense strategy, protecting corporate and industrial environments and detecting cyberattacks that move from IT into OT systems.

What makes Kaspersky SIEM stand out

Maximizes performance, minimizes costs

Cut hardware and virtualization costs by up to 50% and lower TCO with a high-performance, modular SIEM that outperforms legacy solutions and handles hundreds of thousands of EPS per instance.

Built-in SOC expertise

Access 700+ pre-configured detection rules, updated quarterly with MITRE mapping and response guidance — all developed by Kaspersky SOC, one of the industry's most experienced threat hunting teams.

One integrated Kaspersky ecosystem

Leverage 200+ pre-configured Kaspersky and third-party integrations with built-in response options. Our seamless ecosystem offers a single interface for Threat Intelligence, uses endpoint sensors as SIEM agents and delivers integration capabilities unmatched by other vendors.

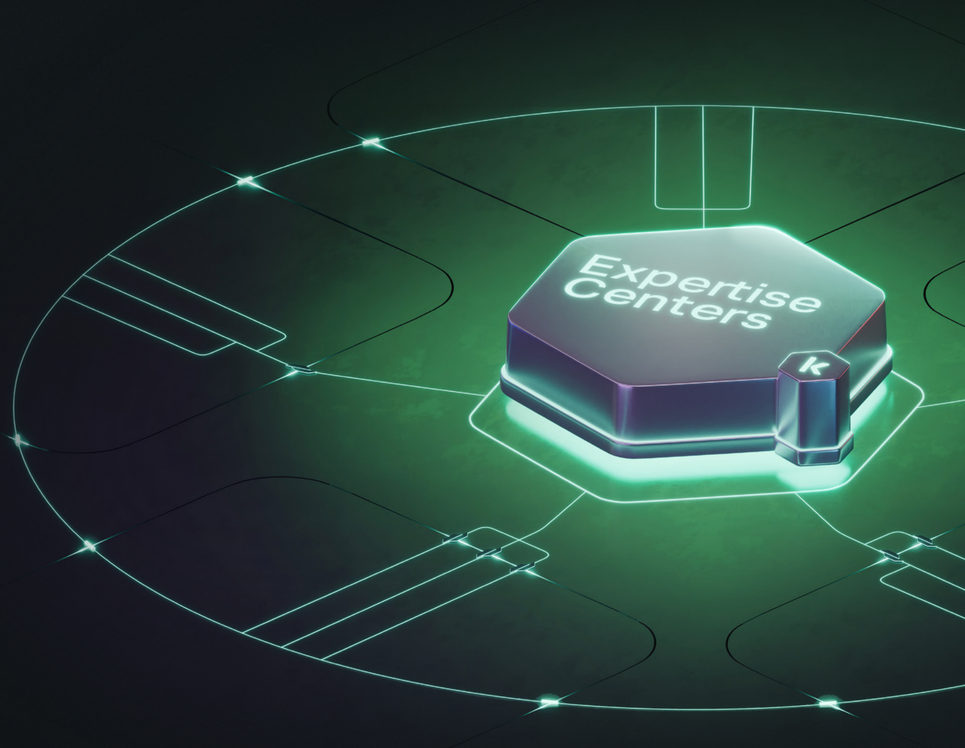
AI-Powered Threat Detection

AI-enhanced components rapidly identify suspicious activity across your infrastructure, with AI detection of DLL-hijacking, AI-based risk scoring of assets and more. These features improve detection accuracy, reduce false positives and minimize the impact of cyber incidents, helping to improve your MTTD and MTTR.

[3] Kaspersky Next XDR Expert, powered by this platform, extends capabilities with advanced threat hunting, automated playbooks, and streamlined case management.

Kaspersky SIEM leverages years of accumulated knowledge and refined skills of Kaspersky Expertise Centers — five specialized, united hubs dedicated to advancing cybersecurity.

Learn more



Kaspersky SIEM comes with 24/7 Premium Support and Services, including custom integrations delivered by Kaspersky Professional Services or trusted partners, leveraging the API capabilities of connected products.

We provide turnkey implementation, seamless migration support and ongoing expertise to ensure you gain maximum value from your SIEM deployment.

Kaspersky SIEM

www.kaspersky.com

Learn more

#kaspersky
#bringonthefuture