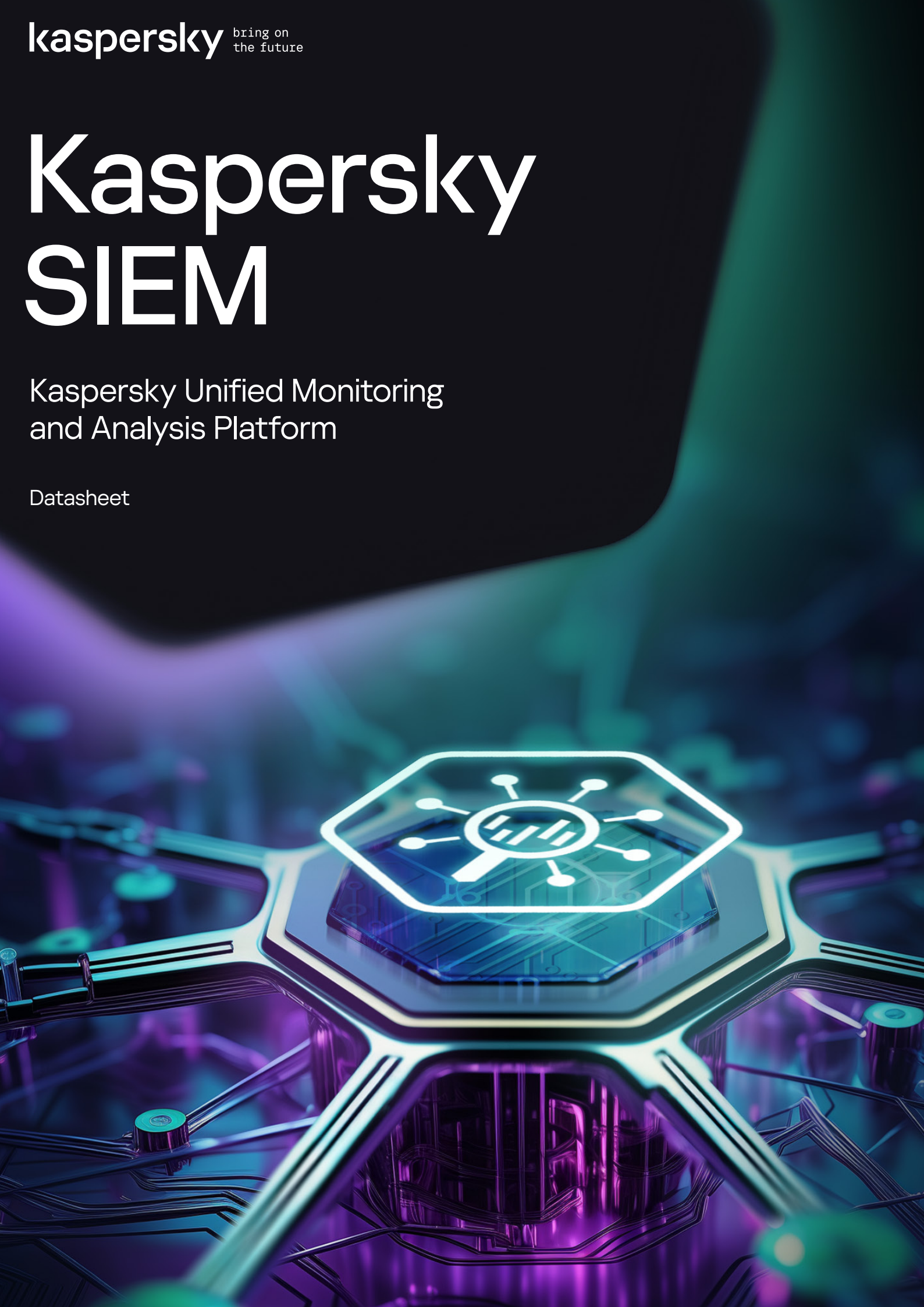
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Datasheet



About Kaspersky SIEM and its architecture

Kaspersky Unified Monitoring and Analysis Platform is an integrated next-generation SIEM solution for managing security data and events. It excels in receiving, processing and storing security information events, and analyzing and correlating incoming data. The platform also has a search feature, generates alerts when potential threats are detected, and supports automated responses to generated alerts and threat hunting.

High-performance modular architecture allows to process hundreds of thousands of events per second (EPS) on each instance and reduce total cost of ownership (TCO) by optimizing system requirements.

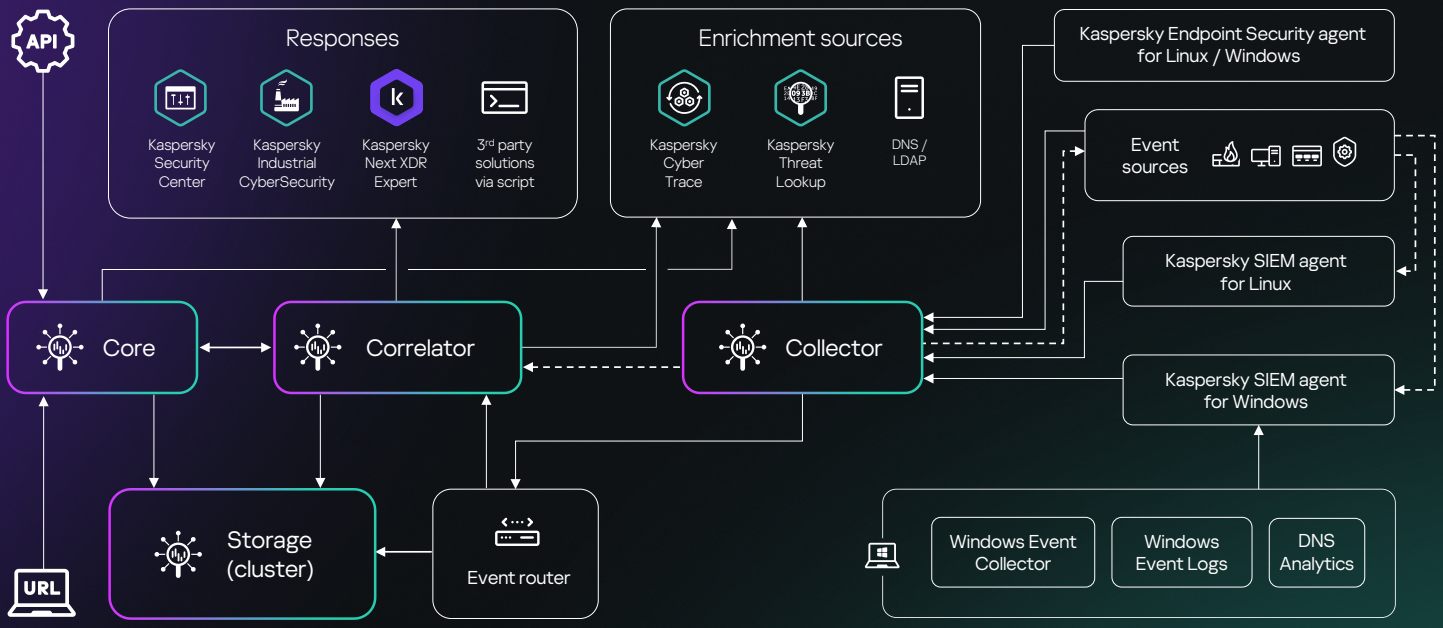
By incorporating third-party and Kaspersky products into a centralized information security system, Kaspersky SIEM is an essential part of a comprehensive defense strategy capable of securing corporate and industrial environments, as well as detecting cyberattacks that start in IT and transition to OT systems.

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

The solution receives security events from various sources, including Kaspersky products, operating systems, third-party applications, security tools, and various databases, and correlates events with each other and enriches them with data from threat intelligence feeds to identify suspicious activity in corporate network infrastructures and provide timely notification of security incidents.

By collecting logs from all security controls and correlating the data in real time, **Kaspersky SIEM aggregates and provides all the information needed for incident investigation and response.**

Furthermore, Kaspersky SIEM enables threat hunters to discover previously unknown threats by allowing operators to analyze and correlate historical data, as well as establish statistical baselines to identify anomalies.



Why choose us?

Save up to 50% on hardware or virtualization installation requirements and reduce TCO with a high-performance modular solution that consistently outperforms legacy SIEM vendors in terms of cost efficiency and can handle hundreds of thousands of EPS on each instance.

Stay flexible with our licensing options. We track average flow of EPS per day after aggregation and filtering to limit overruns and do not restrict access to Kaspersky SIEM in case they happen.

Benefit from a wide range of both Kaspersky and third party integrations with built-in response options. Other vendors cannot match our level of seamless integration with our own products, which includes a single interface for Threat Intelligence integration, the capacity to use our endpoint sensors as SIEM agents, and much more.

Store data locally in a low-cost, uncompromised fashion without going over budget for an extended period with hot and cold storage options using ClickHouse and the Hadoop Distributed File System (HDFS) or local disks, while being able to search quickly across both areas simultaneously.

Improve data relevancy, speed up detection and triage thanks to enrichment with tactical, operational and strategic Threat Intelligence provided via Kaspersky Threat Intelligence Portal by our world-leading team of researchers and analysts.

Leverage built-in multitenancy with an MSSP and large enterprise ready solution that offers native multitenancy support where a single SIEM installation in the main infrastructure of organizations enables the creation of isolated SIEM for tenants that receive and process their own events.

Why Kaspersky?

Kaspersky SIEM levareges years of accumulated knowledge and refined skills of the 5 Centers of Expertise.

Learn more

27

For **more than 27 years** we have been building tools and providing services to keep you safe with our most tested, most awarded technologies.

Learn more

We are a **global private cybersecurity company** with thousands of customers and partners around the world and committed to transparency and independence.

Learn more

Kaspersky Unified Monitoring and Analysis Platform

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture