Product White Paper

Kaspersky SIEM

kaspersky bring on the future

Contents

Security Information and Event Management Market

Cybersecurity leaders in organizations face numerous challenges, including a rising number of attempts to penetrate their infrastructure, a shortage of cybersecurity personnel, and increasingly complex attacks.

Furthermore, organizations must comply with regulatory requirements related to data retention, auditing and incident investigation, which impacts the global SIEM market.

Organizations are also under pressure to segregate cyberattack alerts by priority and triage them more efficiently due to their growth and increasing complexity.

In addition, remote working conditions have led companies to adopt SaaS applications and allow employees to bring their own devices (BYOD), highlighting the need to extend network visibility beyond the traditional perimeter.

Finally, finding qualified information security experts is a challenge in today's market. Companies are looking for ways to optimize their resources and improve cybersecurity efficiency. Consequently, organizations want easily accessible and actionable intelligence data for their SOC teams.

According to the Kaspersky Human Factor 360 Report

77% of companies experienced at least one cybersecurity breach, with many enduring up to six in that period

41% of companies feel they have gaps in their cybersecurity infrastructures and plan to increase investments in this area moving forward

Learn more

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.

Kaspersky Unified Monitoring and Analysis Platform includes the following components

A **Core** with a centralized graphical user interface for controlling and monitoring system component settings. The platform can be accessed from third-party solutions using the API.

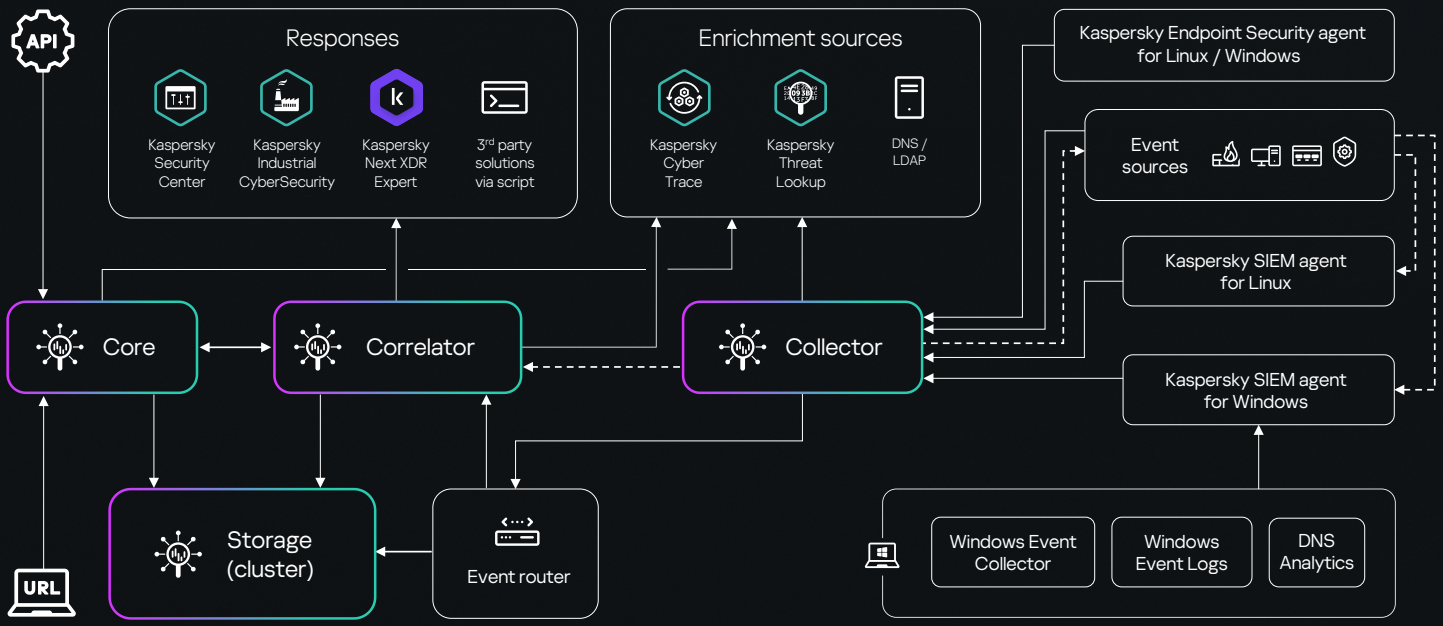
Correlation rules are used to detect specific sequences of processed events and take certain actions after recognition, such as creating correlation events/alerts or interacting with an active list. The **Correlator** uses active lists to carry out required actions after analyzing normalized events received from the collectors and generates alerts based on correlation criteria.

One or more **Collectors** receive events from external sources and pre-process them: normalize (change to a single format), filter, aggregate and enrich them with data from external sources using dictionaries, calls to the DNS service, and other tools.

Storage is used to store normalized events so they can be quickly and continually accessed from SIEM to extract analytical data.

Agents forward raw events from workstations and servers to SIEM collectors. Sending Windows log events straight to the collector is now possible in Kaspersky Endpoint Security for Windows 12.6 or Linux 12.2. This significantly lowers the amount of work needed to integrate event sources with the Kaspersky SIEM system.

Event routers reduce the load on links and number of ports opened on firewalls by receiving events steadily without delays when collectors are installed in remote offices with low-bandwidth or data links that are already busy.



Kaspersky SIEM functionality

Built-in and custom connectors to hundreds of sources from Kaspersky and third-party vendors with regular updates and improvements.

Integration of external event sources with free creation of additional connectors by the Kaspersky Professional Services team.

Fast search queries and ready reports on security events.

Local secure storage of logs for regulatory compliance and incident investigation.

Kaspersky SIEM supports event searches across multiple storages to help operators find relevant events in distributed storage clusters faster and easier.

Monitor, process and store information about security events

Kaspersky Unified Monitoring and Analysis Platform receives events from logs and normalizes data from different event sources to make it consistent. These information security events may include login attempts, database interactions, or sensor information broadcasts and are collected from across the company's entire protected IT infrastructure. While an individual event might not appear significant, taken as a whole, multiple single events paint a larger picture of malicious activity that can be used to spot security issues.

Data lake, our centralized local repository, provides a platform for collecting, indexing and analyzing logs from various sources, including security solutions (EPP, FW, IAM, etc.), operating systems, business applications (HR systems, office tools), physical security systems (automated access control systems), and other devices.

Events are transmitted to the correlator for analysis and storage for retention once they have been filtered and aggregated. To identify alerts, the collector receives events from sources, processes them and routes them to storage, correlator and/or third-party services. Raw events are forwarded from workstations and servers to SIEM collectors (in certain cases by agents) and can be sent to other systems for additional analysis.

Correlation events are produced by the solution upon recognition of a particular event or series of related events and are also analyzed and retained. If an event or sequence of events indicates a potential security threat, Kaspersky SIEM generates an alert with information about the threat and any other relevant information that security specialists need to consider.

Reliable transport protocols, with optional encryption, are used to transfer events between components. A data diode can be used by the system to collect data from isolated segments.

Kaspersky SIEM enables centralized asset management by providing a large inventory of servers, workstations and network devices. The platform can collect data about asset vulnerabilities from sources such as vulnerability scanners and correlate it with asset category data to identify threats. This provides security teams with visibility into the full asset landscape.

To support analysts, coverage of the MITRE ATT&CK matrix by rules is displayed to better assess the level of security.

650+ preconfigured correlation rules for detecting attack scenarios regularly updated by Kaspersky servers with MITRE mapping and response recommendations.

Improved data relevancy through enrichment with analytical data gathered from the Kaspersky Threat Intelligence Portal (using Kaspersky Threat Lookup and Kaspersky CyberTrace).

Data about assets and infrastructure is collected from Kaspersky Security Center and third-party sources.

Users can compare an event with grouped, aggregated, average, max, and minimal values for a specific time period using ClickHouse data mining functionality. This significantly expands the capabilities of detection logic without requiring the creation of numerous service rules.

To facilitate content creation and editing, we allow users to find out beforehand which correlation rules the intended change will apply to before making any changes to the filter criteria.

Real-time and historical correlation of security events

Kaspersky SIEM carries out near real-time cross-correlation using custom rules for identifying attacks and threats and hundreds of pre-defined rules developed by Kaspersky SOC, one of the most successful and experienced active threat hunting teams in the industry. Kaspersky SOC experts hold numerous certificates confirming their high level of expertise and knowledge.

Events are **correlated in real time**. The correlator analyzes normalized events, creates alerts in accordance with the correlation rules, and handles all active list operations.

The operating principle of the correlator is based on event signature analysis, meaning each event is handled in accordance with the user-specified correlation rules. The software generates a correlation event and sends it to storage when it finds a series of events that meet the requirements of the correlation rule. The user can tailor the correlation rules to be triggered by the outcomes of a prior analysis by sending the correlation event to the correlator for additional analysis. Correlation rule outcomes can be utilized by other correlation rules. For example, several minor alerts can generate a larger alert (several brute force attempts may be analyzed to uncover a mass brute force incident).

The platform uses historical data to spot trends, find threats that were previously unidentified, and pinpoint attacks that were overlooked by certain security elements, all of which improves overall threat detection.

Third-party solutions or integrated products like **Kaspersky Endpoint Detection and Response** carry out sensor-side detection. By adjusting product settings, users can control this process and obtain events and telemetry that these products have already processed through their own detection logic.

The solution's correlation engine incorporates platform-side detection. Thanks to the platform's powerful correlation engine, users can create adaptable correlation rules. Ready-made rules and normalizer packages are also available to support commercially accessible third-party products that are constantly being expanded and updated.

The operating principle of the correlator is based on event signature analysis, meaning each event is handled in accordance with the user-specified correlation rules. The software generates a correlation event and sends it to storage when it finds a series of events that meet the requirements of the correlation rule.

Threat hunting to discover previously unknown threats by allowing operators to analyze and correlate historical data using a powerful column-oriented database.

Users can easily locate filters, dictionaries, and rules that are all unified by a single tag by using the tag-based search function. Storing search query history enables the user to access previous inquiries with ease.

The platform can store data for an extended period without going over budget for pricey storage hardware thanks to hot and cold storage options using ClickHouse and the Hadoop Distributed File System (HDFS) or local discs.

Administrators can prevent space issues in the disk subsystem using flexible settings: the depth of event storage can be set in gigabytes as a percentage of disk space, in addition to days.

Security event data storage

Kaspersky SIEM's storage component is used to store normalized events in order to access analytical data quickly and continuously from **Kaspersky Unified Monitoring and Analysis Platform**.

ClickHouse guarantees continuity and speed of access. Storage is connected to a Kaspersky SIEM storage service via a ClickHouse cluster. Cold storage disks can also be added to ClickHouse clusters.

Users can add space in repositories to group stored events based on a specific attribute. This allows administrators to set different storage times for events based on their specific characteristics.

Kaspersky Unified Monitoring and Analysis Platform also handles data compression to dramatically reduce disk space usage without compromising data retrieval. Two areas are supported by the Kaspersky solution: one for fast data retrieval and the other for storing a large amount of data.

The platform has two distinct sections: one for cold storage that can be realized on the Hadoop Distributed File System or local discs, and the other for operational storage using ClickHouse. This separation is transparent for users.

Without having to flip between archives, operators can create search queries in a single interface and concentrate their full effort on the investigation. This **lowers the system's cost of ownership** while maintaining excellent user experience. The platform supports event searches across multiple storages to help operators find relevant events in distributed storage clusters faster and easier.

Organizations can stay compliant with regulatory requirements for data retention, auditing and incident investigation by securely collecting and storing logs from a variety of sources. Additionally, centralized and structured storage makes it easy for companies to retrieve and analyze logs as needed.

Integrated response capabilities

Built-in response functionality using Kaspersky products increases security efficiency. For example, to extend endpoint response capabilities, Kaspersky SIEM can be coupled with Kaspersky Endpoint Detection and Response to manage network isolation of assets and prevention rules or execute applications and scripts. These response actions can be carried out manually or automatically on assets with the Kaspersky Endpoint Security agent.

Automated inventory information collection (installed software, vulnerabilities, equipment, asset owners and so on) can help contextualize information security events and aid in incident investigations.

Kaspersky SIEM leverages Kaspersky CyberTrace, a full-featured threat intelligence platform that supports dozens of out-of-the-box threat data feeds (commercial and public) to stream event enrichment automatically in real-time with contextual information about indicators of compromise.

The artificial intelligence components of Kaspersky SIEM enable rapid detection of suspicious activity in the infrastructure

Artificial intelligence and machine learning tools

Kaspersky uses predictive algorithms, clustering techniques, neural networks, statistical modeling techniques, and expert algorithms to increase our products' effectiveness in detecting threats faster and prioritizing detections accurately.

Monitoring and response teams can prioritize alerts and zero in on preventing potential damage, verified by big data and AI systems. The AI module helps triage by analyzing historical data, prioritizing incoming alerts and providing AI-based risk scores for assets. This approach helps generate valuable hypotheses that can be used for proactive searches.

The platform uses user-defined correlation rules to link events in real time. Its correlation module applies artificial intelligence algorithms to detect anomalous activity such as sudden traffic spikes or multiple service accesses signaling a potential incident, allowing early detection before damage occurs.

Kaspersky SIEM also incorporates data from Kaspersky Threat Intelligence, generated using AI and big data technologies. The database is continuously enriched with the results of manual APT analysis, Darknet operational data, information from Kaspersky Security Network, and insights from regular new malware analysis.

All these technologies help users minimize potential harm caused by cyber-incidents, and increase MTTR and MTTD.

Outstanding visualization with dashboards and reports presents data in the most usable formats to identify trends, patterns and anomalous events.

With customizable widgets for the easy visualization and display of indicators, analysts can prioritize incidents, determine root causes and respond to threats more efficiently, while organizations can track the effectiveness of their security operations, identify trends and assess the overall health of their security system.

Users can enrich event field data with contents of dictionaries, tables, assets and account attributes and use this data for search and visualization. This helps build dashboards and reports with more contextual data.

This solution helps users make their own widgets with adjustable settings, as well as layouts with **various widget groups:**

Key alert metrics

(severity, priority, and status)

- Affected assets
- Recent notifications
- Top data sources with the most alerts
- Alerts allocated to specific operators
- Affected users and / or devices
- Alerts by policy

Key incident indicators

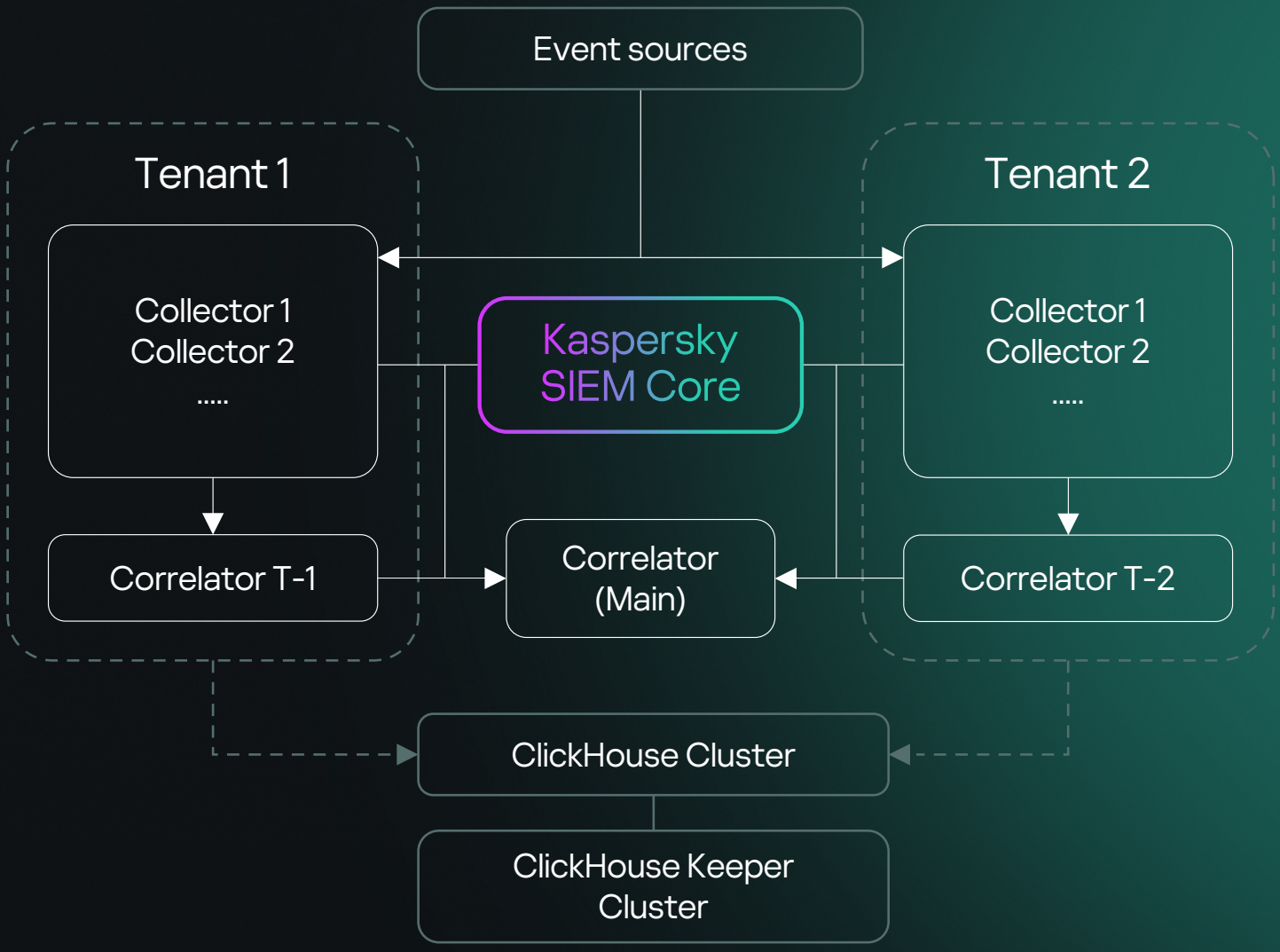
(severity and assignment)

- Affected devices
- Top internal and external IPs based on NetFlow traffic volume (BytesIn)
- Top nodes for remote management (ports 3389, 22)
- Total NetFlow bytes for internal ports
- Top sources based on number of events, categories, assets, and users

Multitenancy architecture

Kaspersky SIEM provides full multi-tenancy support, meaning users in one tenant can't see the data (events, alerts, incidents, etc.) of another tenant. In multitenancy mode, a single instance of the Kaspersky SIEM application deployed in the main organization enables the isolation of branches so they receive and process their own events.

The system is administered centrally via the main interface, and tenants operate independently with access only to their own resources, services and settings. Tenant-related events are stored separately. Users can access numerous tenants simultaneously. The general administrator can also specify which tenant data will be displayed in different parts of the web interface.



The platform offers a filter-based system for distributing events to spaces. User access to events is now set at the space level. This enables granular control of access to events within a single tenant.

The system is managed centrally through the main interface while tenants operate independently of each other and have access only to their own resources, services and settings. The events of tenants are stored separately.

Wide range of out-of-the-box integrations

Kaspersky Unified Monitoring and Analysis Platform is thoroughly integrated with Kaspersky solutions and technologies for the coordinated use of products with enhanced efficiency. Third-party 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.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response *

Kaspersky Security Center

Kaspersky Secure Mail Gateway

Kaspersky Web Traffic Security

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Automated Security Awareness Platform

and more

Integration with the rich portfolio of **Kaspersky Threat Intelligence** services helps identify and prioritize threats and get quick access to contextual information about new attacks, indicators of compromise and attacker tactics and techniques.

* Includes possible integrations with Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert

Kaspersky SIEM excels in receiving data (logs) from other systems and devices. To facilitate quick implementation without the added expense of setting up source parsing rules, the platform comes with a wide range of out-of-the box integrations for Kaspersky products and third-party products:

By security domain

- Endpoint Protection (EPP & EDR solutions)
- Email and web traffic protection (email protection, NDR, FW / NGFW, UTM, IDS)
- Security Awareness
- Cloud workload (CASB, CWPP)
- Threat Intelligence (CTI)
- Identity Security (IAM, PAM)
- OT / IoT Security
- Data loss prevention (DLP)

By data type

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Key-Value
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

By transport type

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch)
- File
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (DNS analytics)
- SNMP
- SNMP Traps
- VMware API
- MS Office 365

Additional integrations can be developed by the Kaspersky Professional Services team or partners, including using the APIs of connectable products. View the full list of supported event sources.

Full list

By vendor

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMware
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- etc.

Kaspersky Premium Support

Premium Support for Kaspersky SIEM

Kaspersky Premium Support for Kaspersky SIEM comes with both Premium and Premium Plus licenses, ensuring quick response and high-quality assistance for any issues to keep your Kaspersky SIEM running smoothly

Communication	Standard support	Premium license	Premium Plus license
Company Account (web portal)	●	●	●
Phone		●	●
Email		●	●

Service			
Custom parsers for Kaspersky SIEM		5	10
Remote assistance to diagnose problems		●	●
Priority escalation of support requests		High	Highest
Private patching			●
Dedicated Technical Account Manager (TAM)			●
Status reports from TAM			Quarterly report

Response times			
Critical issues	No SLA	2 hours (24/7)	30 min (24/7)
High level issues	No SLA	6 hours (8/5)	4 hours (24/7)
Medium level issues	No SLA	8 hours (8/5)	6 hours (8/5)
Low level issues	No SLA	10 hours (8/5)	8 hours (8/5)

Fast response

Requests are prioritized with strict SLAs for quicker and reliable issue resolution

Custom parsers

Custom parsers enable SIEM to process unique log formats from your specific data sources

Dedicated TAM

With Premium Plus license, a TAM manages all issues with elevated accountability

Private patches

Get custom fixes and patches, designed for specific issues, with Premium Plus license

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.

Enterprises worldwide rely on the Kaspersky Unified Monitoring and Analysis Platform to develop comprehensive information security processes that enhance cybersecurity efficiency.

Learn more

Kaspersky used its own SIEM to uncover previously unknown malware targeting iOS devices

While monitoring the network traffic of our own corporate Wi-Fi network dedicated to mobile devices using the Kaspersky Unified Monitoring and Analysis Platform, we detected suspicious activity originating from multiple iOS-based phones.

Because it is impossible to examine modern iOS devices from the inside, we created offline backups of the devices in question, examined them using the Mobile Verification Toolkit's mvt-ios and discovered traces of compromise.

Apple responded by releasing security updates to address four zero-day vulnerabilities identified by Kaspersky researchers:

CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990

These vulnerabilities affect a wide range of Apple products, including iPhones, iPods, iPads, macOS devices, Apple TVs, and Apple Watches. Kaspersky also informed Apple about the exploitation of a hardware feature, which the company subsequently mitigated.

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