Kaspersky Unified Monitoring and Analysis Platform

Datasheet

Kaspersky SIEM

The centerpiece of your security system

According to the Kaspersky Human Factor 360 Report 2023

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.

Security Information and Event Management Market

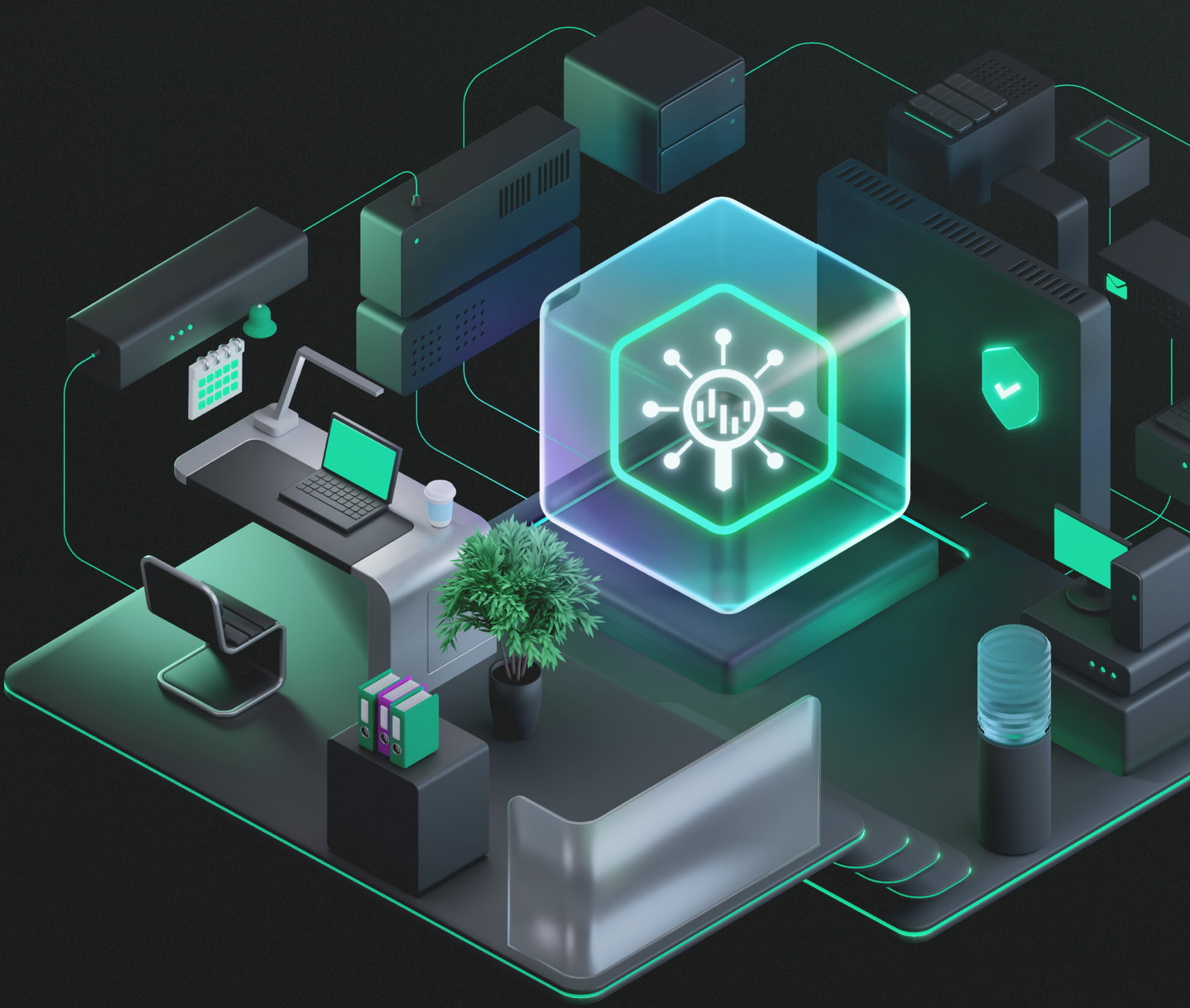
Cybersecurity leaders in organizations face numerous challenges, including a rising number of attempts to penetrate their infrastructure, a shortage of cybersecurity personnel, and increasingly complex attacks.

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.



Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Unified Monitoring and Analysis Platform is a next-generation SIEM solution for managing security data and events. It analyzes information security events in real time, significantly increasing situational awareness.

The platform collects, aggregates, analyzes and stores log data from the entire IT infrastructure. It also provides contextual enrichment and actionable threat intelligence insights used by IT security experts for various use cases, including governance, compliance, and rule-based correlation for suspicious activity. The solution also supports automation of response to generated alerts.

Kaspersky SIEM is designed to help organizations with established information security processes increase their efficiency in the following tasks:

Centralized log management

Collecting and storing events from multiple sources in a central repository for future analysis.

Incident response

Coordinating the response workflow, supporting analyst collaboration, and reducing mean time to respond (MTTR) to contain and remediate incidents.

Threat hunting

Quickly identifying previously unknown threats using a powerful column-oriented database.

Compliance

Complying with regulations, reporting incidents to national CERTs and gaining immediate visibility into security posture.

Threat detection (security monitoring)

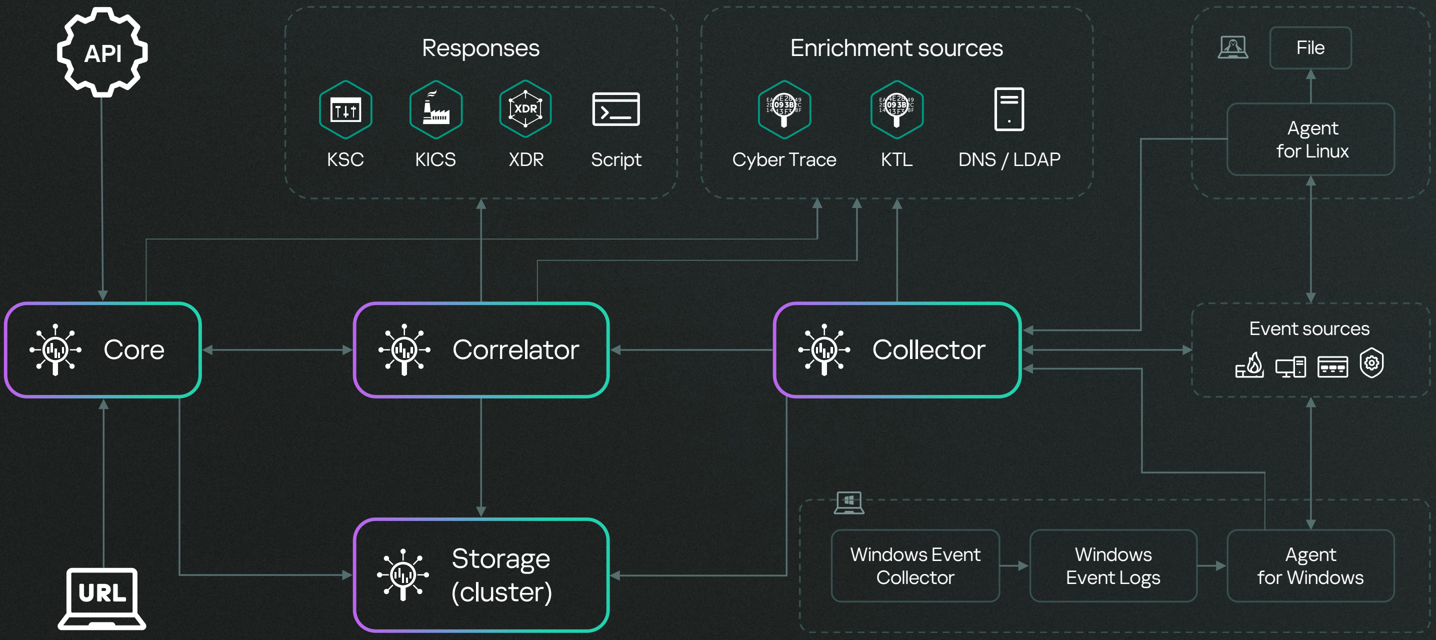
Analyzing and correlating events in real time and receiving alerts about potential internal and external threats, while quickly detecting and prioritizing threats and reducing mean time to detect (MTTD).

The platform elevates threat detection accuracy and improves alert triage with actionable context information.

Kaspersky SIEM architecture

Kaspersky Unified Monitoring and Analysis Platform receives security events from multiple sources, such as operating systems, IT and security tools, third-party applications and Kaspersky products.

The platform correlates these events based on rules and enriches data with threat intelligence feeds to identify suspicious activity in corporate network infrastructure. It also provides timely notification of security incidents. By collecting logs from the protected infrastructure and correlating the resulting data in real time, Kaspersky SIEM aggregates all the necessary information for incident investigation and response.



The architecture of Kaspersky Unified Monitoring and Analysis Platform includes the following components:

- The Core provides a graphical interface to monitor and manage the system component settings.
- One or more Collectors receive messages from event sources and parse, normalize, and, if necessary, filter and/or aggregate them.
- A Correlator that analyzes normalized events received from Collectors, performing necessary actions with active lists*, and generating alerts in accordance with correlation rules.
- The Storage that contains normalized events and registered incidents.
- Agents or services used to forward raw events from servers and workstations to SIEM destinations.

Events are transmitted between components over reliable transport protocols, which can be optionally encrypted. The system can also handle isolated segments using a data diode.

Kaspersky SIEM integrates Kaspersky products and third-party solutions into a centralized information security system. It is a key component in implementing a comprehensive defense approach capable of securing corporate and industrial environments, as well as the IT/OT systems junction most exploited by attackers, from today's cyberthreats.

* A bucket for data that is used by Kaspersky SIEM correlators for analyzing events based on correlation rules.

Competitive advantages

Kaspersky SIEM is built on over 25 years of global experience in creating cybersecurity tools to protect information, counter targeted attacks and analyze malware.

Kaspersky Unified Monitoring and Analysis Platform offers the following competitive advantages:

High performance and low system requirements

The solution is designed to function in today's dynamic and highly loaded IT environments. The powerful correlation streaming engine and the modular microservice architecture enable easy configuration changes, high scalability, fault tolerance, minimal cost of ownership and flexible deployment options.

Thanks to "hot" and "cold" storage options available with ClickHouse and Hadoop Distributed File System (HDFS), the platform enables long-term data storage without the need for expensive storage hardware.

Contextual information for incident response

Automated collection of inventory information (installed software, vulnerabilities, equipment, asset owners, etc.) can provide context for information security events and aid in incident investigation. Workplace agent management assists in the process of responding to identified incidents.

Response actions enable faster detection and investigation and can be performed manually or automatically when Kaspersky SIEM is integrated with Kaspersky Endpoint Detection and Response and Active Directory. This integration goes beyond the capabilities of just endpoint response.

MSSP and large enterprise ready

The multitenant architecture of Kaspersky SIEM ensures full data delimitation. This means that users of one tenant cannot access data (events, alerts, incidents, users) of other tenants. However, the master administrator (or MSSP) has access to its subordinate tenants.

Simple and flexible licensing policy

Kaspersky SIEM relies solely on the EPS (event-per-second) metric when it comes to licensing. We track average flow of EPS per day after aggregation and filtering to limit overruns and do not limit access to Kaspersky SIEM in case they happen, we also allow for unlimited NetFlow* and avoid pay-per-use cloud policies to keep the price reasonable and predictable.

24/7 premium support and services

Professional help is available when you need it. Operating in more than 200 countries from 34 offices around the world, we are there for you 24/7/365. Take advantage of our premium support packages or our professional services to ensure you get the most out of your Kaspersky security installation.

Premium support

Learn more

Professional services

Learn more

* Included with NetFlow module purchase

340+

correlation rules

Developed by Kaspersky SOC, one of the most successful and experienced active threat hunting teams in the industry. The team's high level of expertise and knowledge is confirmed by numerous certificates.

Regularly updated via Kaspersky servers with MITRE mapping and response recommendations.

200+

sources supported out of the box

with regular additions and improvements.

Wide range of out-of-the-box integrations

Kaspersky Unified Monitoring and Analysis Platform shares information with Kaspersky solutions and technologies, enabling the integration of existing products into a unified system and enhancing their efficiency:

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Security Center
- Kaspersky Secure Mail Gateway
- Kaspersky Web Traffic Security
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial Cyber Security for Networks
- Kaspersky Industrial Cyber Security for Nodes
- Kaspersky Automated Security Awareness Platform

Tight integration with the rich portfolio of Kaspersky Threat Intelligence services makes it possible to identify and prioritize threats and get one-click access to contextual information about new attacks, indicators of compromise, and the attackers' tactics and techniques.

Kaspersky SIEM excels in its ability to receive 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 with both 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)
- Cloud workload (CASB, CWPP)
- Threat Intelligence (CTI)
- Identity Security (IAM, PAM)
- OT / IoT Security
- Security Awareness

By data type

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

By transport type

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird)
- File
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP Traps
- VMware API

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.

Additional integrations can be developed by Kaspersky Professional Services representatives or partners, including the use of API capabilities of connectable products. View the full list of supported event sources.

Full list

Learn more

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.

www.kaspersky.com

#kaspersky
#bringonthefuture