

Scheda tecnica

# Kaspersky SIEM

Trasformate le vostre operazioni di sicurezza con la nostra soluzione di nuova generazione, basata sull'intelligenza artificiale e potenziata con threat intelligence di livello mondiale

kaspersky cybersecurity true to business



Kaspersky SIEM è pensato per le organizzazioni con infrastrutture IT complesse, elevati volumi di dati e rigorosi requisiti normativi. Il prodotto è ideale per gli MSSP.

Queste organizzazioni riconoscono che una sicurezza efficace non dipende solo dalla prevenzione, ma anche dalla capacità di rilevare, analizzare e rispondere alle minacce in tempo reale su diversi sistemi.

# Ottimizzate l'impatto delle vostre operazioni di sicurezza

Le grandi organizzazioni si trovano ad affrontare un numero crescente di attacchi mirati avanzati. Nel 2025, gli attacchi mirati human-driven hanno rappresentato il 24% degli incidenti di gravità elevata[1]. Le conseguenze sono costose e vanno dall'interruzione dell'attività alle perdite finanziarie e ai danni reputazionali a lungo termine.

I team di sicurezza sono sottoposti a una pressione senza precedenti. I sistemi di protezione generano enormi volumi di dati, facendo aumentare i costi di archiviazione e rendendo costose le implementazioni SIEM. Gli esperti qualificati sono scarsi, mentre i team esistenti sono già ridotti all'osso. Il 42% delle organizzazioni segnala una carenza di personale IT qualificato [2]. Oltre a ciò, la complessità dell'amministrazione dei sistemi SIEM grava ulteriormente sulle risorse già limitate.

Anche i SOC più esperti rischiano di perdere efficienza e impatto senza gli strumenti basati sull'intelligenza artificiale di oggi che li aiutano a distinguersi e a concentrarsi su ciò che conta di più.

# Fornite al vostro team un SIEM basato sull'intelligenza artificiale supportato da threat intelligence di livello mondiale*

Kaspersky SIEM è una soluzione di nuova generazione progettata per aiutare il vostro team di sicurezza a gestire e analizzare i dati di sicurezza in entrata. Eccelle in:

- Raccolta, elaborazione e archiviazione di eventi provenienti da diverse fonti, tra cui prodotti Kaspersky, sistemi operativi, applicazioni di terze parti, strumenti di sicurezza e database.
- Analizzando e correlando i dati in arrivo in tempo reale, arricchendoli con threat intelligence leader del settore per rilevare attività sospette.
- Fornire avvisi tempestivi per consentire indagini e risposte rapide agli incidenti.
- Archiviazione dei dati per lunghi periodi senza che i costi aumentino di pari passo, grazie a livelli di archiviazione "hot" e "cold" con ricerca simultanea su entrambi.

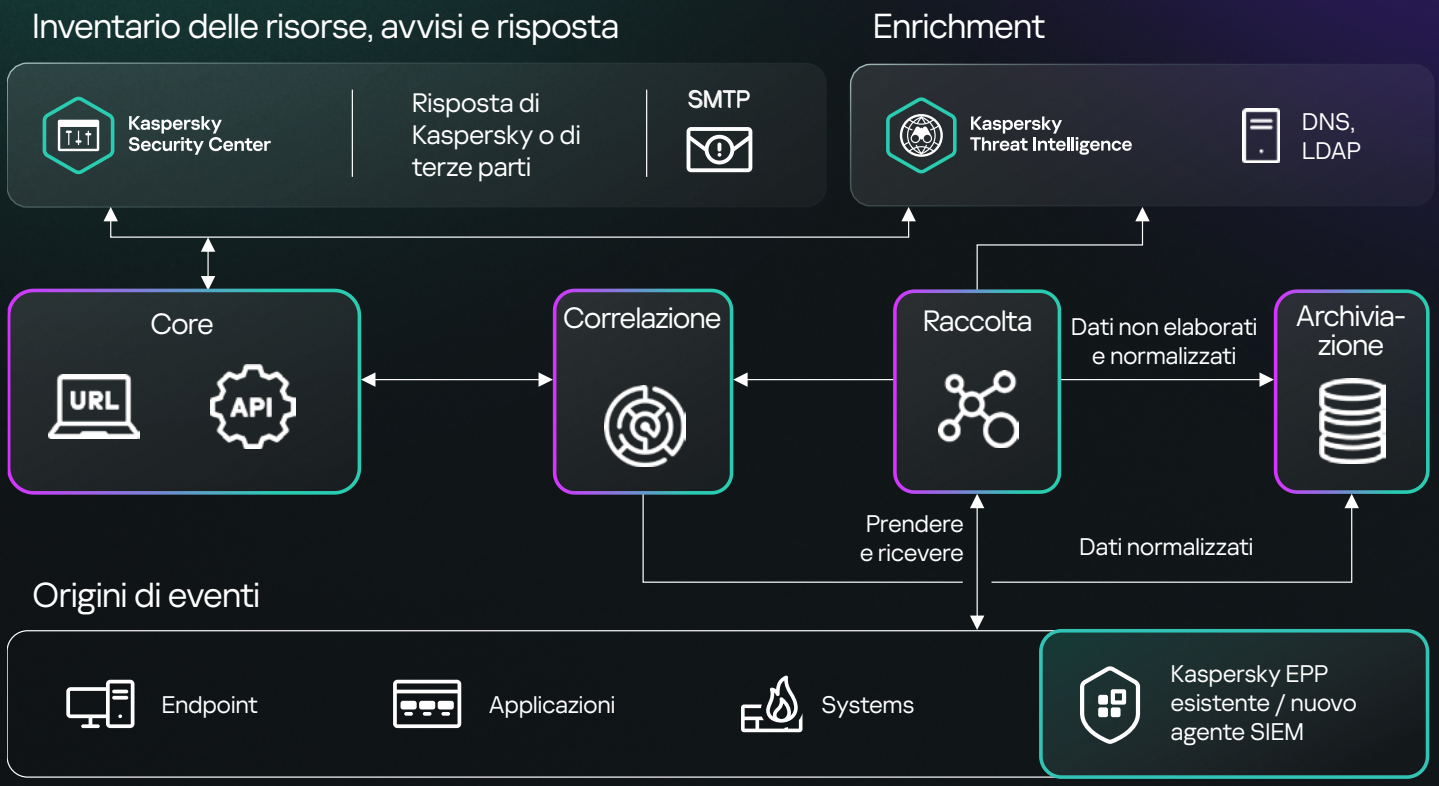
Unificando i log provenienti da fonti di sicurezza e correlandoli in tempo reale, Kaspersky SIEM fornisce agli analisti la visibilità completa e il contesto necessari per rispondere in modo efficiente.

Offre funzionalità di ricerca e analisi avanzate che consentono ai ricercatori di scoprire minacce precedentemente sconosciute. L'analisi dei dati storici e la baseline statistica con il set di regole di rilevamento UEBA aiutano il vostro team a identificare anomalie e a bloccare attacchi sofisticati.

Con Kaspersky SIEM, il SOC ottiene la visibilità, l'intelligence e l'efficienza di cui ha bisogno per trasformare dati enormi in informazioni di sicurezza fruibili Distribuita on-premises, la soluzione può funzionare senza connettività Internet, garantendo la piena sovranità dei dati.

1 "Anatomia del mondo digitale", Report globale di Kaspersky Security Services 2026
2 Kaspersky Supply Chain Security Study, 2026
* La disponibilità delle funzionalità di threat intelligence varia a seconda del modello di implementazione

## Come funziona




Grazie all'architettura a microservizi della soluzione, gli amministratori possono creare e configurare i microservizi necessari per utilizzare Kaspersky SIEM come strumento completo o come sistema di gestione dei log.

Kaspersky SIEM è basato su una Open Single Management Platform[3], che integra sia i prodotti Kaspersky che quelli di terze parti in un sistema di sicurezza centralizzato. Costituisce una parte essenziale di una strategia di difesa completa, proteggendo gli ambienti aziendali e industriali e rilevando i cyberattacchi che si spostano dai sistemi IT a quelli OT. Kaspersky SIEM è disponibile in due modelli di implementazione: on-premises, che include ambienti isolati e non connessi alla rete, e cloud, fornito e gestito da Kaspersky.

## Quali sono le caratteristiche distintive di Kaspersky SIEM

### Ottimizza le prestazioni e riduce al minimo i costi

Riducete i costi di hardware e virtualizzazione fino al 50% on-premises, oppure eliminateli completamente con il cloud. Un SIEM modulare ad alte prestazioni che supera le soluzioni tradizionali e gestisce centinaia di migliaia di EPS per istanza.

### Un unico ecosistema Kaspersky integrato

Sfruttate oltre 350 integrazioni preconfigurate con Kaspersky e terze parti con opzioni di risposta integrate. Il nostro ecosistema senza soluzione di continuità offre un'unica interfaccia per threat intelligence, utilizza sensori endpoint come agenti SIEM e fornisce funzionalità di integrazione ineguagliabili rispetto ad altri fornitori.

### Esperienza SOC integrata

Accedete a oltre 900 regole di rilevamento preconfigurate, aggiornate trimestralmente con mappatura MITRE e indicazioni di risposta, tutte sviluppate da Kaspersky SOC, uno dei team di ricerca delle minacce più esperti del settore.

### Rilevamento delle minacce basato su AI

I componenti ottimizzati dall'IA migliorano la precisione del rilevamento, riducono i falsi positivi e riducono al minimo l'impatto degli incidenti informatici, contribuendo a migliorare MTTD e MTTR[4].

### Implementate la soluzione in base alle vostre esigenze

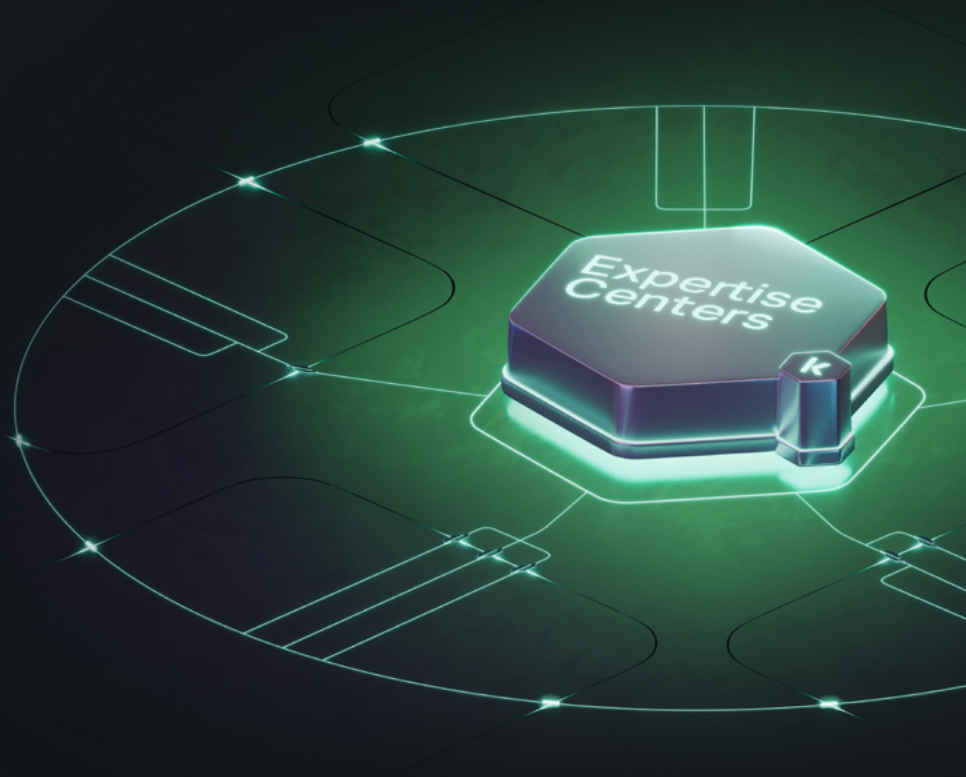
On-premises, air-gapped o cloud: un'unica piattaforma, un unico stack di rilevamento. Le organizzazioni con requisiti di residenza o sovranità dei dati mantengono l'elaborazione dei dati all'interno del proprio perimetro. Chi non ne fa uso ottiene un ritorno sull'investimento più rapido, senza dover dimensionare o eseguire la manutenzione delle infrastrutture.

3 Kaspersky Next XDR Expert, basato su questa piattaforma, amplia le capacità con funzionalità avanzate di ricerca delle minacce, playbook automatizzati e gestione semplificata dei casi.

4 Le funzionalità IA richiedono una licenza aggiuntiva per le implementazioni on-premises e sono incluse nella licenza cloud.

Kaspersky SIEM si avvale di anni di conoscenze e competenze accumulate dai Centri di competenza Kaspersky, cinque centri specializzati dedicati al progresso della sicurezza informatica.

Maggiori informazioni




Kaspersky SIEM offre supporto e servizi Premium 24 ore su 24, 7 giorni su 7, incluse integrazioni personalizzate realizzate da Kaspersky Professional Services o da partner di fiducia.

Forniamo implementazione completa, supporto per la migrazione senza interruzioni e competenza continua per garantire di ottenere il massimo valore dalla implementazione SIEM.

# Kaspersky SIEM

**www.kaspersky.it**

© 2026 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.

Maggiori informazioni

#kaspersky
#truetobusiness