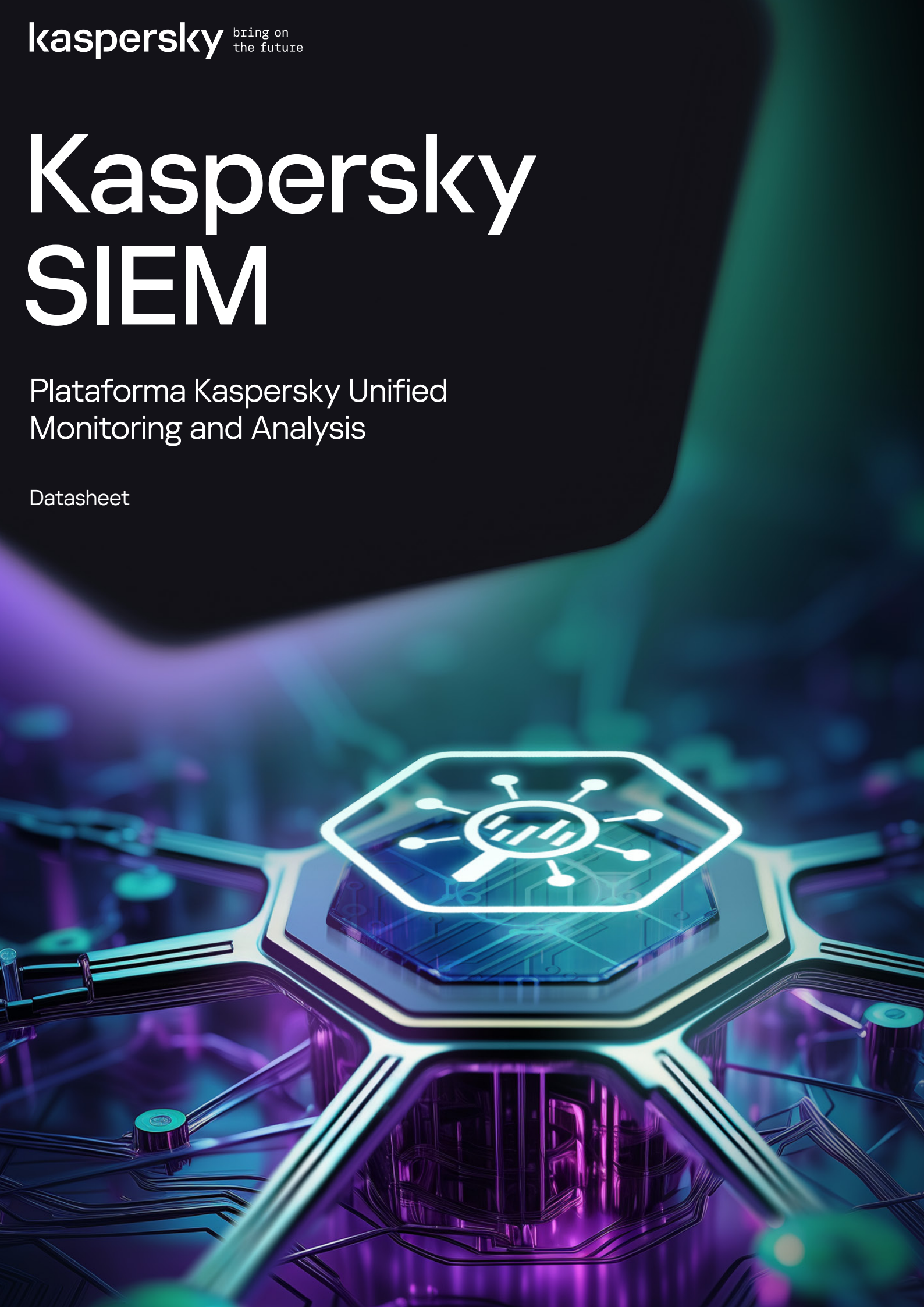
kaspersky bring on the future

Kaspersky SIEM

Plataforma Kaspersky Unified Monitoring and Analysis

Datasheet



Sobre o Kaspersky SIEM e sua arquitetura

A Kaspersky Unified Monitoring and Analysis Platform é uma solução SIEM integrada de última geração para gerenciamento de dados e eventos de segurança. Ele se destaca em receber, processar e armazenar eventos de informações de segurança, e analisar e correlacionar os dados recebidos. A plataforma também possui um recurso de busca, gera alertas quando ameaças potenciais são detectadas e suporta respostas automatizadas aos alertas gerados e à caça de ameaças.

Alta performance arquiteturamodular permite processar centenas de milhares de eventos por segundo (EPS) em cada instância e reduzir o custo total de propriedade (TCO) otimizando os requisitos do sistema.

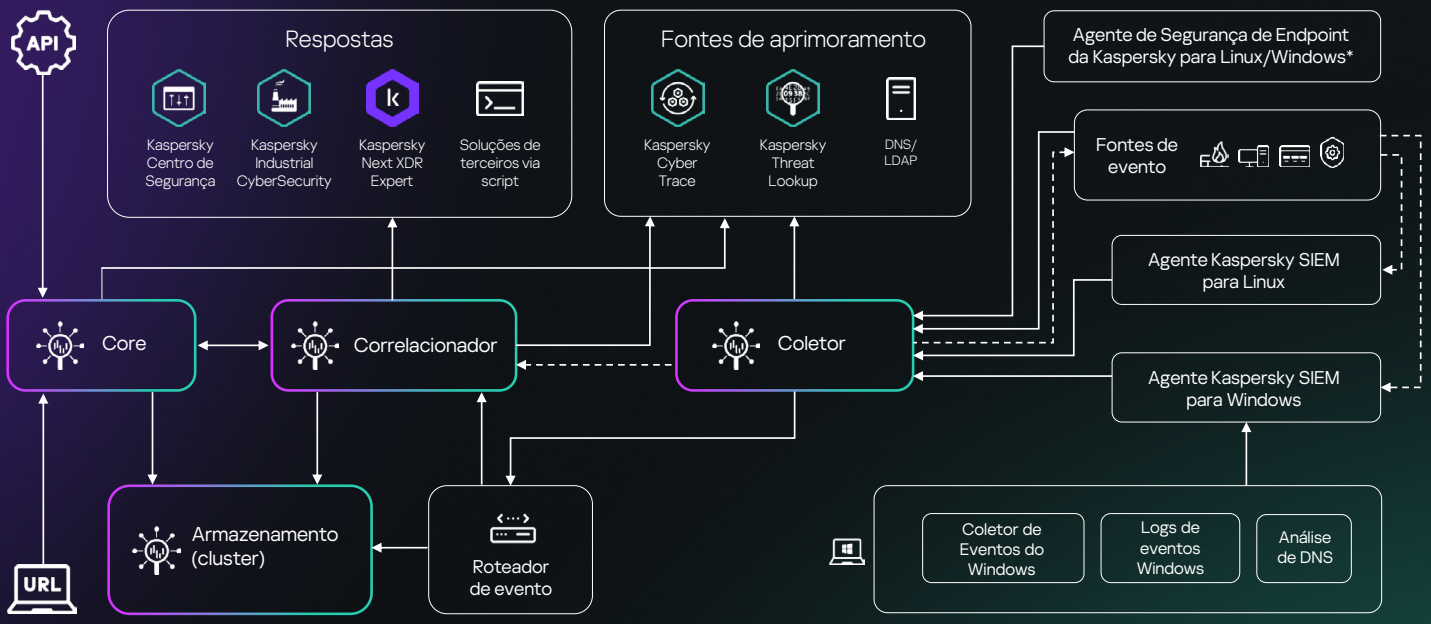
Ao incorporar produtos de terceiros e da Kaspersky em um sistema centralizado de segurança da informação, o Kaspersky SIEM é uma parte essencial de uma estratégia de defesa abrangente capaz de proteger ambientes corporativos e industriais, além de detectar ciberataques que começam em sistemas de TI e passam para sistemas de OT.

Graças à arquitetura de microsserviços da solução, os administradores podem criar e configurar os microsserviços que precisam para usar o Kaspersky SIEM como um sistema SIEM completo ou um sistema de gerenciamento de logs.

A solução recebe eventos de segurança de várias fontes, incluindo produtos da Kaspersky, sistemas operacionais, aplicativos de terceiros, ferramentas de segurança e vários bancos de dados, correlaciona os eventos entre si e os enriquece com dados de feeds de inteligência de ameaças para identificar atividades suspeitas nas infraestruturas de rede corporativa e fornecer notificação oportuna de incidentes de segurança.

Ao coletar registros de todos os controles de segurança e fazer a correlação dos dados em tempo real, o **Kaspersky SIEM reúne e proporciona toda a informação necessária para examinar e responder ao incidente.**

Além disso, o Kaspersky SIEM permite que os caçadores de ameaças descubram ameaças previamente desconhecidas, permitindo que os operadores analisem e correlacionem dados históricos, além de estabelecer bases estatísticas para identificar anomalias.



Por que nos escolher

Economize até 50% nos requisitos de instalação de hardware ou virtualização e diminua o TCO com uma solução modular de alto desempenho que constantemente supera os fornecedores de SIEM legados em termos de eficiência e custo, além de tratar de milhares de EPS em cada instância.

Tenha flexibilidade com nossas opções de licenciamento. Além disso, também rastreamos o fluxo médio de EPS por dia após a agregação e a filtragem para limitar os excessos e não restringir o acesso ao Kaspersky SIEM caso eles ocorram.

Aproveite uma ampla variedade de integrações da Kaspersky e de terceiros com opções de resposta integradas. Nenhum outro fornecedor supera o nosso nível de integração simplificada com nossos próprios produtos, incluindo uma única interface para a integração com o Threat Intelligence, a capacidade de usar sensores de endpoint como agentes SIEM e muito mais.

Armazene dados localmente de forma econômica e sem comprometer a qualidade, sem ultrapassar o orçamento por um período prolongado, com opções de armazenamento quente e frio usando o ClickHouse e o Hadoop Distributed File System (HDFS) ou discos locais, sendo capaz de pesquisar rapidamente em ambas as áreas simultaneamente.

Aumente a relevância dos dados, acelere a detecção e a triagem graças ao enriquecimento com a inteligência de ameaças tática, operacional e estratégica fornecida pelo Kaspersky Threat Intelligence Portal por nossa equipe de pesquisadores e analistas líderes mundiais.

Pronto para MSSP com suporte multilocação nativo, em que uma única instalação de SIEM na infraestrutura principal das organizações permite a criação de SIEM isolado para locatários que recebem e processam seus próprios eventos.

Por que a Kaspersky?

O Kaspersky SIEM aproveita anos de conhecimento acumulado e habilidades refinadas dos 5 Centros de Excelência.

Saiba mais

27

Por **mais de 27 anos**, temos construído ferramentas e fornecido serviços para mantê-lo seguro com nossas tecnologias mais testadas e premiadas.

Saiba mais

Somos uma **empresa global de cibersegurança privada** com milhares de clientes e parceiros ao redor do mundo e comprometidos com transparência e independência.

Saiba mais

Kaspersky Unified Monitoring and Analysis Platform

Saiba mais

www.kaspersky.com.br

© 2024 AO Kaspersky Lab.
As marcas comerciais registradas e as marcas de serviço pertencem aos seus respectivos proprietários.

#kaspersky
#bringonthefuture