Uma plataforma
de segurança para
sustentabilidade e
transformação digital
das empresas industriais

Kaspersky Industrial CyberSecurity Platform

kaspersky PREPARADOS PARA O FUTURO

Atacado por malware

Desde o início de 2022, quase 30% dos computadores relacionados ao ICS foram atacados por malware, quase 10% a menos que no ano anterior

Kaspersky ICS-CERT, Junho de 2022

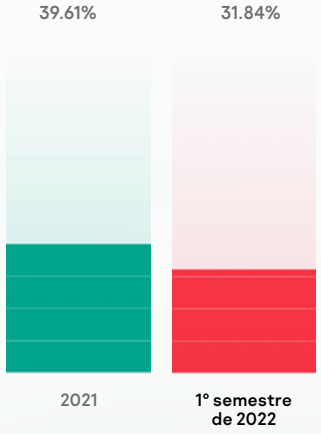
Saiba mais

As empresas industriais abordam a cibersegurança em suas infraestruturas de TI e TO (tecnologia operacional) de maneira diferente. A maioria das empresas já contam com medidas estabelecidas de detecção e resposta em suas redes corporativas, mas quando se trata de TO, elas geralmente contam com uma abordagem desatualizada. As empresas industriais estão se tornando mais "digitais" à medida que investem cada vez mais em tecnologias inteligentes, em novos sistemas de automação e na adoção da transformação digital. Essas tecnologias preenchem a lacuna tradicional entre os ambientes de TI e TO, uma lacuna que costumava impedir que ciberameaças chegassem aos sistemas de automação e controle industrial.

Você pode ser um alvo, mas não seja uma vítima

Você não precisa ser um alvo para se tornar vítima de violações acidentais de lacuna de ar ou infecção por malware. Uma única unidade flash, celular, e-mail de phishing ou ransomware trazido para o ambiente de ICS pode afetar seriamente o negócio principal de uma empresa. Ao mesmo tempo, um grupo de hackers motivado pode penetrar nas redes de TO e causar danos consideráveis a equipamentos, processos, produção, segurança e qualidade ou roubar informações valiosas.

Porcentagem de computadores de ICS nos quais objetos mal-intencionados foram bloqueados desde o início de 2022



Cibersegurança essencial para TO

Proteção de endpoints

para sistemas autônomos e conectados. Uma solução segura e testada deve ajudar a aplicar políticas de segurança, dar suporte à conformidade, realizar auditorias de segurança, gerenciar inventário, realizar tarefas de correção e coletar telemetria precisa como um sensor de endpoint

Proteção de rede

para proporcionar visibilidade de comunicação, detecção de ameaças e gerenciamento de ativos. O Sistema de análise de tráfego de rede e a Detecção de invasões controla a eficiência das configurações de firewall, segmentação de rede e conformidade de uso de rede e ajuda a fornecer uma resposta manual segura

Programas de treinamento

para os funcionários reduzirem os acidentes e minimizarem o fator humano (erro humano).

Serviços especializados

para investigar a infraestrutura e fazer análises especializadas ou mitigar o impacto de um incidente

Reconhecimento global

A Frost and Sullivan concedeu à Kaspersky o prêmio 2020 Global Company of the Year com base na análise do mercado global de cibersegurança industrial (TO/ICS)

Na pesquisa global anual da **VDC**, a Kaspersky foi o principal fornecedor na categoria de cibersegurança industrial, com base nas classificações gerais de mais de 250 profissionais qualificados na comunidade de automação industrial

O que a Kaspersky oferece

A plataforma Kaspersky Industrial CyberSecurity (KICS) de tecnologias integradas nativamente, combinada com nosso portfólio de treinamento e serviços especializados, atendem a todas as necessidades de cibersegurança de empresas industriais e operadores de infraestrutura crítica.

A plataforma é um elemento essencial em um ecossistema único para empresas industriais que conta com:

- As melhores soluções corporativas da Kaspersky, que oferecem uma verdadeira convergência TI-TO, além dos vários benefícios de uma abordagem de um único fornecedor
- Várias soluções especializadas para cibersegurança, segurança de IOT industrial, aprendizado de máquina, espaço de trabalho remoto seguro e muito mais, oferecendo capacidade de expansão ágil e ilimitada

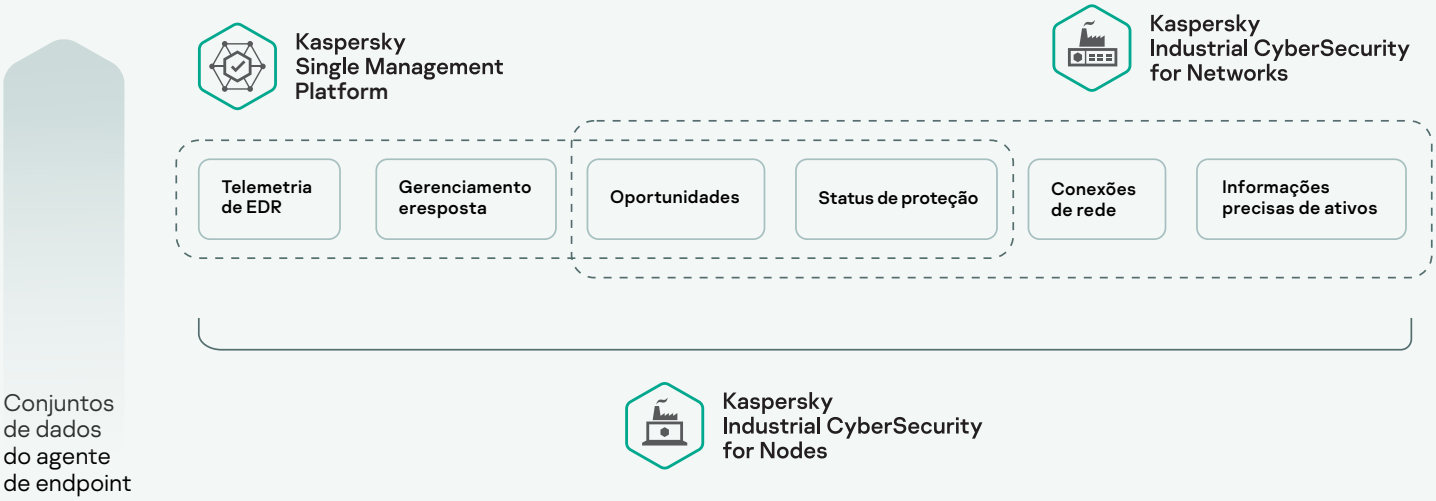
A plataforma Kaspersky Industrial CyberSecurity é líder nas seguintes categorias:

- Segurança de endpoint de TO
- Monitoramento e visibilidade de rede de TO
- Detecção de anomalias, resposta a incidentes e relatórios
- Serviços de segurança de TO

Produtos

Quando usado em conjunto, o usuário vê o panorama geral em um contexto mais amplo: cadeia de incidentes no nível da rede e do endpoint, parâmetros precisos de ativos, comunicação de rede e mapas de topologia, incluindo os segmentos onde o espelhamento de tráfego ainda não está disponível, e muito mais.

O KICS é uma plataforma de cibersegurança de TO projetada para oferecer proteção abrangente aos principais componentes de automação industrial e sistema de controle em todos os níveis. A integração perfeita entre os componentes da plataforma fornece visibilidade total de várias redes de TO geograficamente distribuídas e dos sistemas de automação, proporcionando experiência avançada ao cliente, reconhecimento de situação e flexibilidade de implantação.



O KICS for Nodes é um software de proteção, detecção e resposta de endpoint com auditoria de conformidade e funcionalidade de sensor de endpoint.

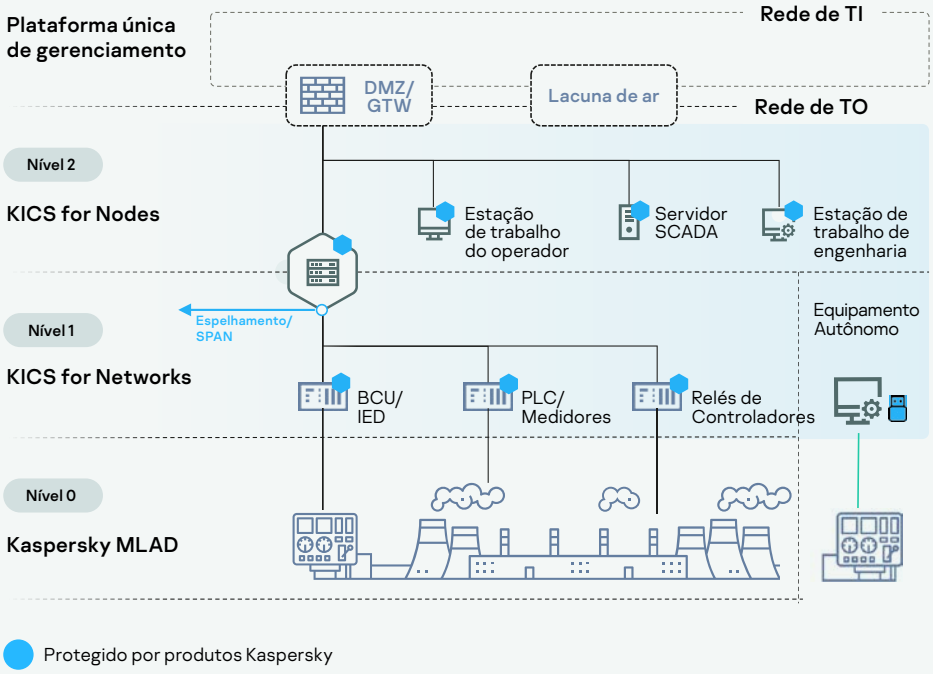
O KICS for Networks foi desenvolvido para análise, detecção e resposta de tráfego de rede de TO.

A Plataforma única de gerenciamento disponibiliza uma interface de EDR avançada e capacidade de expansão rápida para vários locais.

Outras funções

A solução oferece várias funções adicionais. A **Pesquisa ativa** de rede permite a coleta rápida e precisa de topologia de rede e configurações de ativos. A função **Auditoria de endpoint** ajuda a garantir a conformidade com a política de segurança, incluindo a segurança das configurações atuais, e a controlar vulnerabilidades. O método de entrega **Scanner portátil** do KICS for Nodes ajuda a estabelecer as melhores práticas de auditorias autônomas de segurança de equipamentos com lacuna de ar. **O Aprendizado de máquina para detecção de anomalias** é um sistema de detecção precoce de anomalias enraizado no processo tecnológico.

Arquitetura da solução



Recursos

Descoberta de ativos
Identificação passiva e inventário de ativos de TO

Inspeção profunda de pacote
Análise quase em tempo real da telemetria do processo técnico

Controle da integridade da rede
Detecta hosts e fluxos de rede não autorizados

Sistema de detecção de invasões
Envia alertas sobre atividades de rede mal-intencionadas

Controle de comando
Inspeciona comandos sobre protocolos industriais

Integração externa
A integração flexível da API adiciona recursos de detecção e prevenção

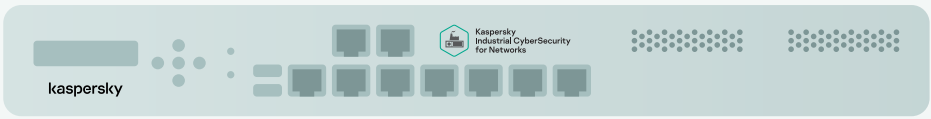
Aprendizado de máquina para detecção de anomalias (MLAD)
Encontra anomalias cibernéticas ou físicas por meio de telemetria em tempo real e mineração de dados históricos (rede neural recorrente)

Gerenciamento de vulnerabilidades
Banco de dados atualizável de vulnerabilidades em equipamentos industriais, com a tecnologia Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

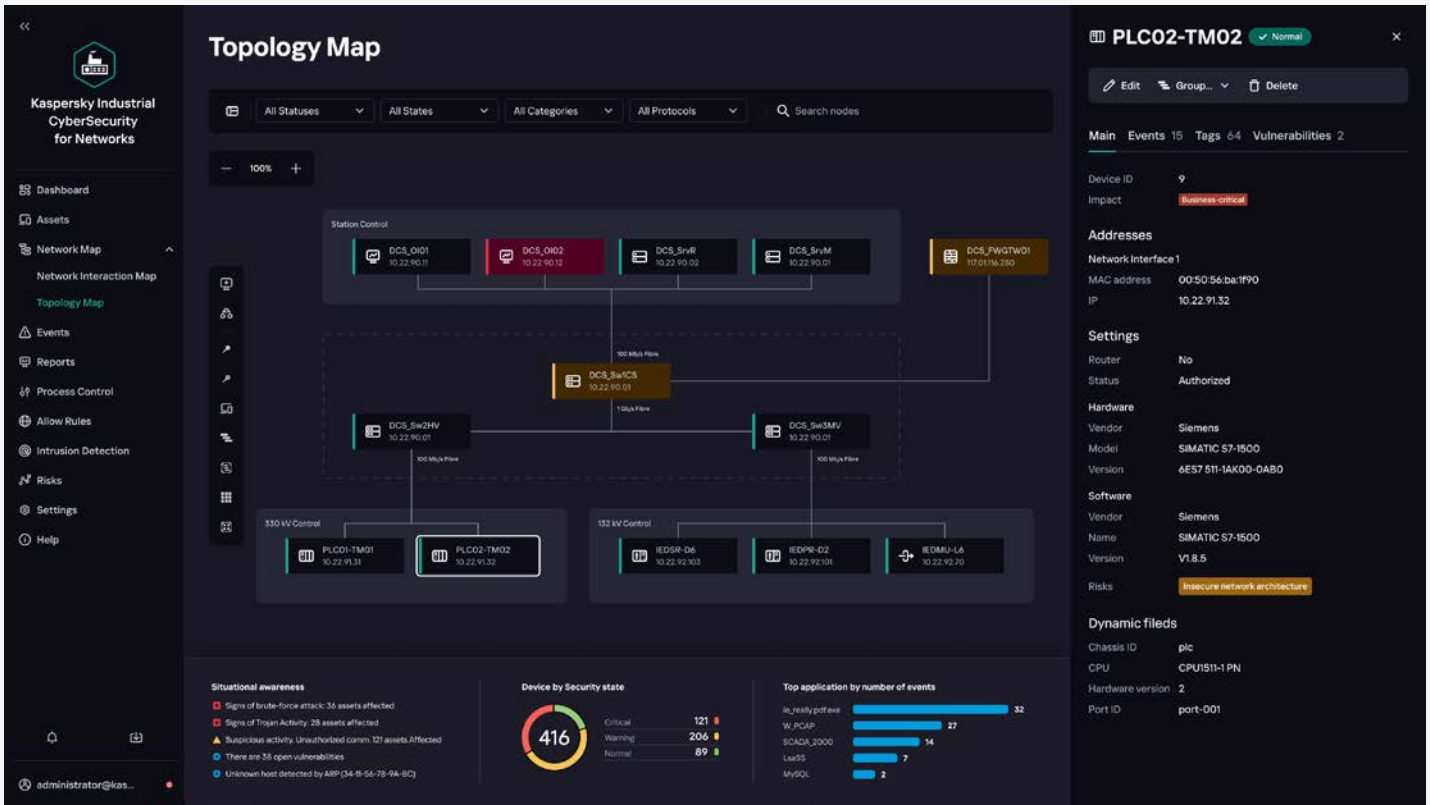
Análise, detecção e resposta de tráfego de rede de TO. Visibilidade clara de risco com monitoramento passivo de tráfego, sondagem ativa e sensores de endpoint.

Detecta anomalias e invasões nas redes de ICS em seus estágios iniciais e garante que as ações necessárias sejam tomadas para evitar qualquer impacto negativo nos processos industriais.



Solução independente de dispositivos que pode ser integrada de forma rápida e otimizada às práticas estabelecidas de fornecimento, integração e garantia de nossos clientes.

Interface



O KICS for Nodes foi desenvolvido especificamente para os exigentes requisitos de sistemas de automação distribuídos: ambientes mistos e complicados, tempo de operação prolongado, casos de uso autônomos e conectados, instâncias assistidas e sem manutenção e prioridade de disponibilidade de controle a todo custo

Kaspersky Industrial CyberSecurity for Nodes

Proteção, detecção e resposta de endpoint de nível industrial, testada e certificada. Uma solução de baixo impacto, compatível e estável para Linux, Windows e sistemas autônomos.

Proteção, detecção e resposta para endpoints industriais

Protege todos os endpoints de um sistema de automação moderno, digital, gerenciado e distribuído. Revela novos níveis de visibilidade de incidentes no processo de análise de causa raiz. O agente coleta a telemetria do endpoint para criar uma representação visual clara e detalhada do progresso de um incidente em estações de trabalho, servidores, gateways e outros endpoints, garantindo aos administradores do sistema de automação que um incidente foi totalmente resolvido e não acontecerá novamente.

Vantagens

Baixo impacto
no dispositivo protegido para o melhor desempenho do sistema

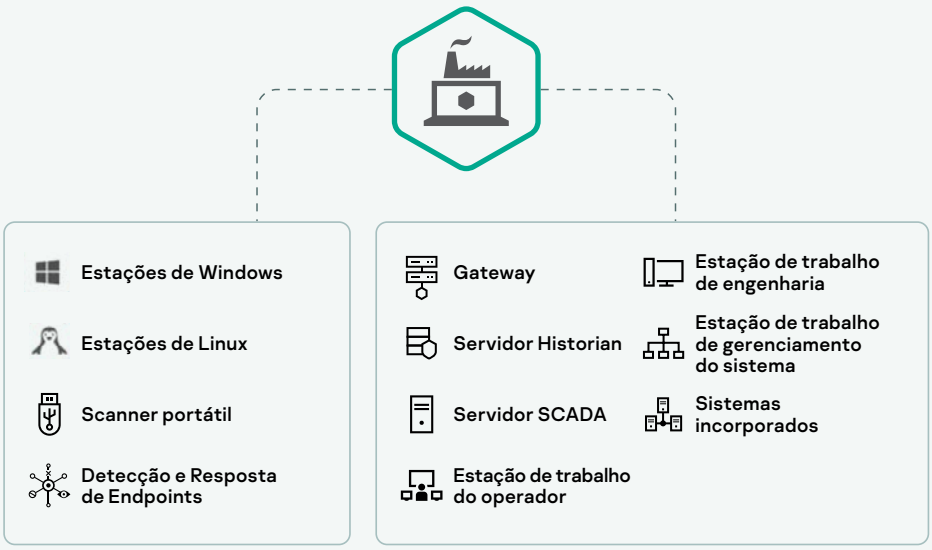
Compatível
com computadores de baixo desempenho de gerações anteriores e sistemas do Windows XP SP2 e Windows Server 2003 SP1 e superior

Ciclo de vida mais longo
com licenciamento de até 5 anos e suporte estendido

Funcionalidade completa
para todos os sistemas operacionais MS Desktop, Server e Windows Embedded

Implantação modular
com opções flexíveis e configurações não intrusivas seguras

Compatível com infraestruturas mistas
como variantes portáteis, Windows e Linux



Scanner portátil do KICS for Nodes
Aplica uma política de cibersegurança em máquinas autônomas, sistemas de automação ou equipamentos nos quais o software de segurança não pode ser instalado. O que há de mais novo em consciência situacional e visibilidade de TO, mesmo em uma infraestrutura independente.

Solução sem instalação
O KICS for Nodes pode ser ativado em várias unidades flash adicionais do Scanner portátil. Isso ajuda a fazer verificações sob demanda simultâneas em várias máquinas durante as janelas de manutenção, o que permite coletar dados do endpoint e organizá-los em um relatório prático resumido.

Conformidade regulatória e política interna
O Scanner portátil do KICS for Nodes faz verificações de conformidade antimalware de equipamentos que acessam um site de TO, incluindo computadores de terceiros contratados. Ele ocupa pouco espaço e não interfere nas soluções de segurança existentes.

Vantagens

Consciência da situação

Gerenciamento de sistemas/ políticas

Kill-chain e resposta

Relatórios e notificação

Integração com SIEMs

Integração com HMI/MES

Kaspersky
Single Management
Platform

A Plataforma única de gerenciamento é uma solução de gerenciamento de segurança centralizada para orquestração de segurança de toda a infraestrutura de TO, com um mapa de todos os ativos distribuídos geograficamente enriquecidos com eventos, análise de incidentes e muito mais. Ela aumenta a eficiência de equipes mistas de segurança de TO e TI. Também cria um local onde todos os controles de segurança funcionam em harmonia, possibilitando uma resposta rápida e precisa.

Serviços especializados

Nosso conjunto de serviços é uma parte importante do portfólio KICS. Oferecemos o ciclo completo de serviços de segurança, de avaliações de cibersegurança industrial à resposta a incidentes.

> Em comparação com outros fornecedores, a experiência que possuem em cibersegurança de ICS, junto ao profissionalismo e à complexidade da solução, nos ofereceram grande valor e garantem um futuro brilhante para a estratégia de segurança da nossa empresa.
>
> Ondřej Sýkora,
> Gerente da C&A,
> Plzeňský Prazdroj

Avaliação de cibersegurança industrial

Avaliação de cibersegurança industrial: a Kaspersky fornece uma avaliação de cibersegurança industrial minimamente invasiva, incluindo testes de penetração internos e externos, avaliação de segurança de TO e avaliação de segurança de soluções de automação. Os especialistas da Kaspersky fornecem insights relevantes sobre a infraestrutura de uma empresa e recomendações sobre como fortalecer a postura de cibersegurança do ICS.

> Ao realizar o exercício e aprender com o conhecimento da equipe da Kaspersky, aumentamos nossa proteção contra ameaças à cibersegurança.
>
> Yu Tat Ming,
> CEO, PacificLight

Threat Intelligence

Análises atualizadas coletadas por especialistas da Kaspersky ajudam a melhorar a proteção do cliente contra ataques cibernéticos industriais direcionados. Fornecidos como feeds de TI ou relatórios personalizados, elas atendem às necessidades específicas do cliente de acordo com os parâmetros regionais, do setor e do software de ICS.

Resposta a incidentes

Em caso de incidente, os especialistas da Kaspersky coletam e analisam dados e malware, reconstroem a linha do tempo do incidente, determinam possíveis fontes e motivações e desenvolvem um plano de correção detalhado. O plano inclui recomendações sobre como remover malware dos sistemas do cliente e reverter suas ações mal-intencionadas.

Treinamento e conscientização

> Contar com a Kaspersky foi a nossa melhor escolha para oferecer treinamento profissional em habilidades de cibersegurança industrial para nosso grupo de ICS.
>
> Søren Egede Knudsen,
> Diretor Técnico

Treinamento de conscientização sobre cibersegurança industrial

Treinamento interativo presencial e on-line e jogos de cibersegurança para funcionários que trabalham com sistemas informatizados industriais e seus gestores. Os participantes obtêm novos insights sobre o atual cenário de ameaças e os vetores de ataque direcionados especificamente a ambientes industriais, exploram cenários práticos e adquirem habilidades de cibersegurança.

Programas de treinamento especializado

Os cursos de treinamento Teste de penetração de ICS e Perícia digital de ICS são voltados para profissionais de cibersegurança. Os participantes obtêm todas as habilidades avançadas necessárias para realizar testes de penetração abrangentes ou perícia digital em ambientes industriais.

Ecossistema de soluções especializadas

Kaspersky IoT Infrastructure Security

Protege a Internet das Coisas no nível do gateway com base na abordagem de ciber imunidade da Kaspersky

Saiba mais

Kaspersky Antidrone

Protege o espaço aéreo de drones em instalações de qualquer tamanho

Saiba mais

Kaspersky Secure Remote Workspace

Infraestrutura de thin client funcional com Ciber Imunidade

Saiba mais

Kaspersky Security CAD

Modelagem digital de sistemas de segurança da informação para as fases de projeto e operação

Saiba mais

Kaspersky Machine Learning for Anomaly Detection

Sistema de detecção precoce de anomalias em processos tecnológicos industriais

Saiba mais

Kaspersky Industrial CyberSecurity

Saiba mais

www.kaspersky.com.br