Kaspersky OT CyberSecurity

Um ecossistema de segurança ciberfísico para indústrias

kaspersky BRING ON THE FUTURE

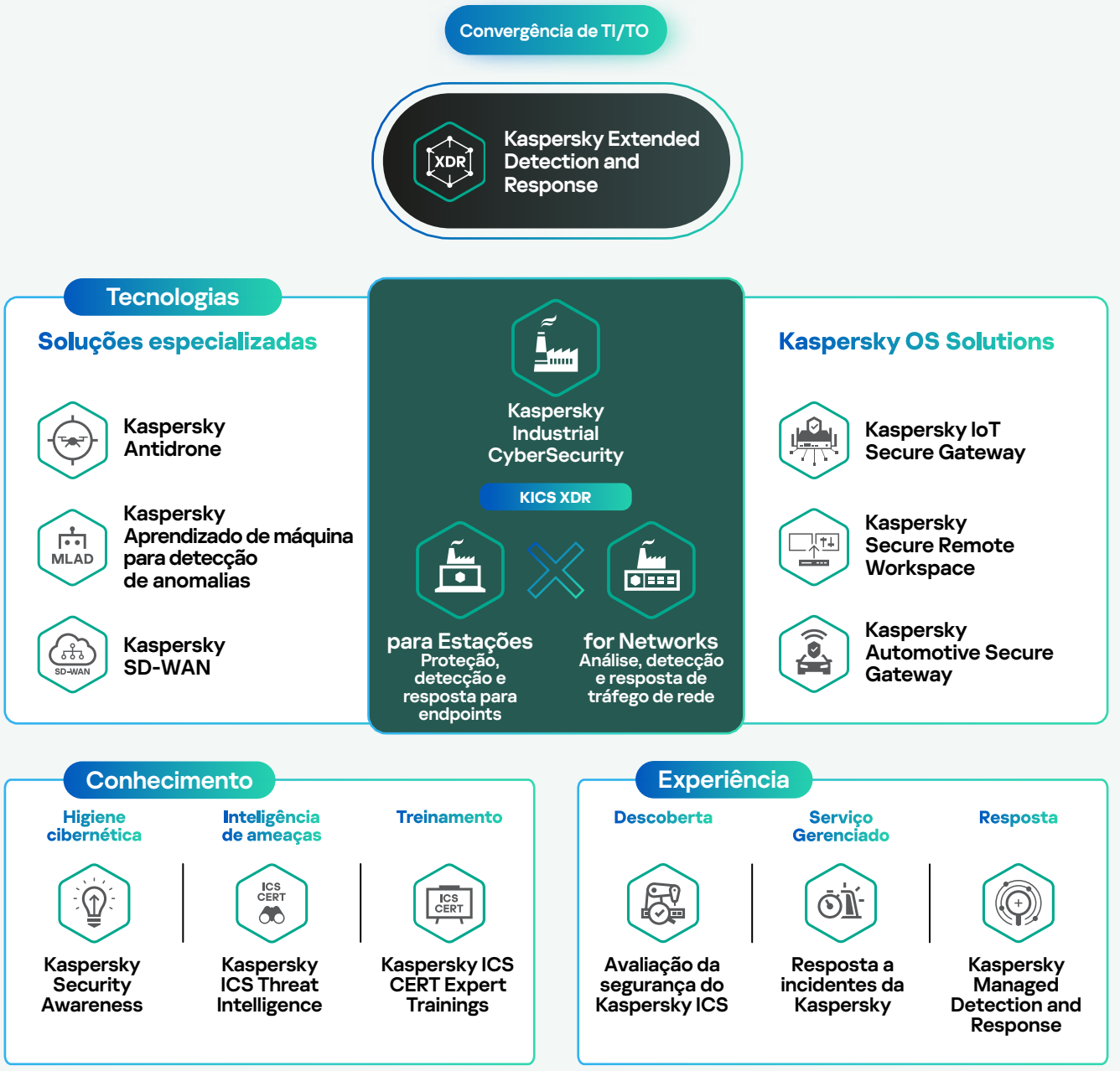
Kaspersky
OT CyberSecurity

Conceito de segurança industrial unificada

Tecnologias
Uma seleção robusta de soluções de segurança industrial testadas, em conformidade a aprovadas

Conhecimento
Análise de ameaças confiável e treinamento abrangente em cibersegurança industrial.

Experiência
Uma gama completa de serviços profissionais para cibersegurança industrial abrangente



Kaspersky OT CyberSecurity

Convergência de TI/TO

Kaspersky Extended Detection and Response

Kaspersky IoT Secure Gateway

Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

KICS XDR

for Nodes
Proteção, detecção e resposta para endpoints

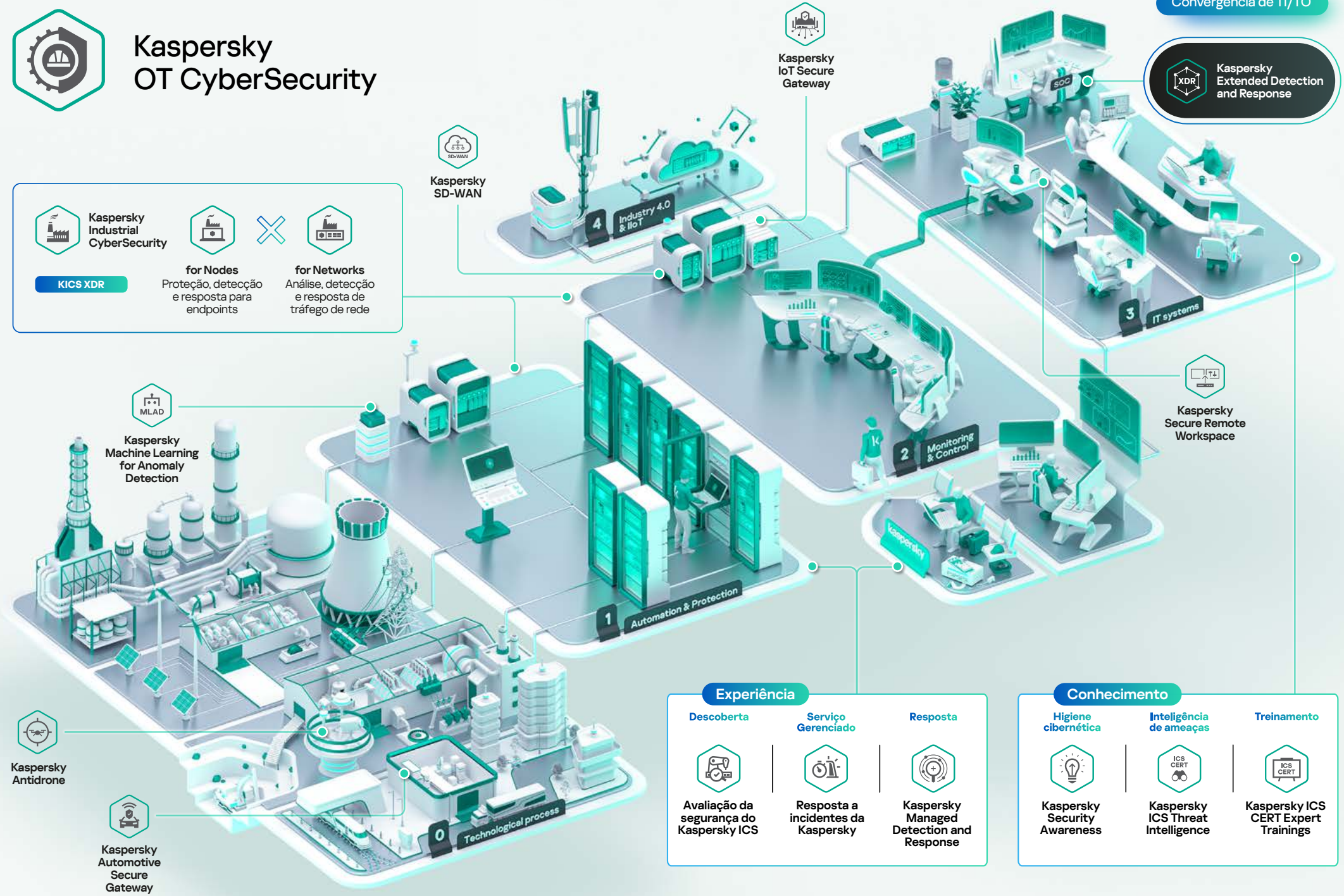
for Networks
Análise, detecção e resposta de tráfego de rede

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Secure Remote Workspace

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway



Experiência

Descoberta
Avaliação da segurança do Kaspersky ICS

Serviço Gerenciado
Resposta a incidentes da Kaspersky

Resposta
Kaspersky Managed Detection and Response

Conhecimento

Higiene cibernética
Kaspersky Security Awareness

Inteligência de ameaças
Kaspersky ICS Threat Intelligence

Treinamento
Kaspersky ICS CERT Expert Trainings

Visitar site

Kaspersky Industrial CyberSecurity

XDR

SAFE MONEY

Plataforma XDR nativa para proteger sistemas de automação

- Revela ameaças ocultas, anomalias, vulnerabilidades e tentativas de intrusão muito antes que se tornem perigosas para suas operações
- Certificado por fornecedores de automação e reguladores
- Nenhum efeito adverso nos processos tecnológicos. Evita danos inaceitáveis
- Facilita a gestão de infraestrutura de automação complexa e distribuída e a resposta a incidentes
- Ajuda a mitigar riscos e manter um registro de violações

Vantagens da plataforma XDR

Cobertura de ponta a ponta para sistemas de automação e controle industrial (IACS). Proteção para Linux, Windows, computadores isolados ou de terceiros, bem como detecção de anomalias e ameaças na rede.

Auditoria de segurança ativa e/ou passiva de endpoints e de redes. Gestão centralizada de riscos, política de segurança e gerenciamento de ativos em todos os níveis do IACS.

Excelente visibilidade de sistemas e de redes. Investigação e reconstrução de toda a "kill chain". Visualização da progressão de incidentes em redes industriais e em diferentes nodos.

Adquirir com um parceiro Solicite uma demo Folheto

Visitar site

XDR

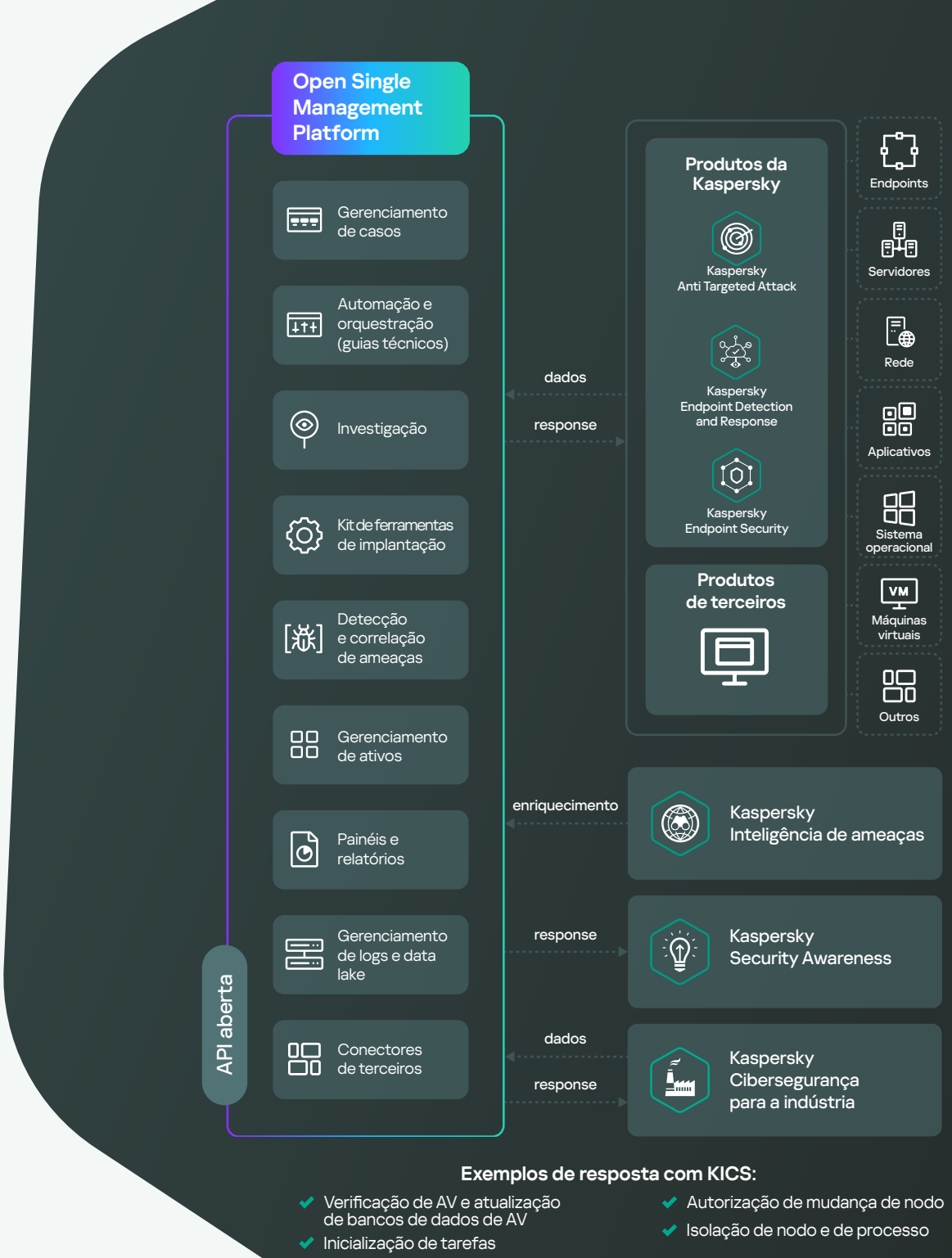
Kaspersky Extended Detection and Response

SAFE MONEY

Cibersegurança unificada em todos os segmentos industriais e corporativos da sua empresa

Por meio da integração próxima com o Kaspersky Extended Detection & Response, a plataforma Kaspersky Industrial CyberSecurity possibilita novos cenários que incluem interações com soluções de terceiros, com capacidades aprimoradas de investigação e de resposta. A plataforma também ajuda a proteger o seu negócio não apenas em ambientes industriais, mas também onde os ambientes industriais e corporativos se sobrepõem. Isso é alcançado graças ao trabalho em conjunto com o portfólio de cibersegurança de TI de ponta da Kaspersky.

Dessa forma, as equipes de segurança podem formar uma imagem holística do desenvolvimento de um incidente e identificar suas causas raiz para prevenir incidentes semelhantes no futuro.



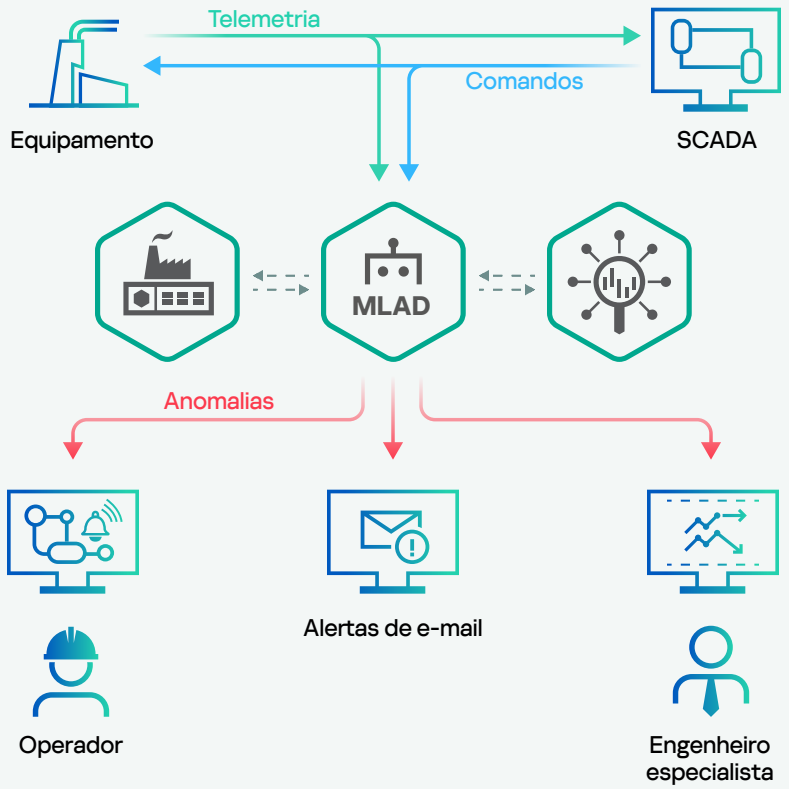
Fale conosco Folheto

Visitar site

MLAD

Kaspersky Machine learning for Anomaly Detection

SAFE MONEY



Detecção precoce de anomalias e análise preditiva

- Detecta falhas de equipamentos e erros humanos muito antes de se tornarem críticos, ajudando a prevenir falhas e acidentes
- Identifica ações atípicas de funcionários ou operações de equipamentos como sinais de um ataque especializado ou sabotagem
- Combina a detecção de anomalias com a análise preditiva da condição e ciclo de vida do equipamento

Ecossistema e inteligência artificial

Integração com KICS para Redes e KUMA: recebe telemetria e eventos desses sistemas e envia alertas sobre anomalias detectadas

Aplica regras de diagnóstico aos sintomas predefinidos do problema e aprendizado de máquina para detectar quaisquer desvios de comportamento do equipamento

Utiliza inteligência artificial para analisar a telemetria do processo e eventos relacionados às ações dos funcionários

Visitar site

SD-WAN

Kaspersky SD-WAN

SAFE MONEY

Recursos do Kaspersky SD-WAN:

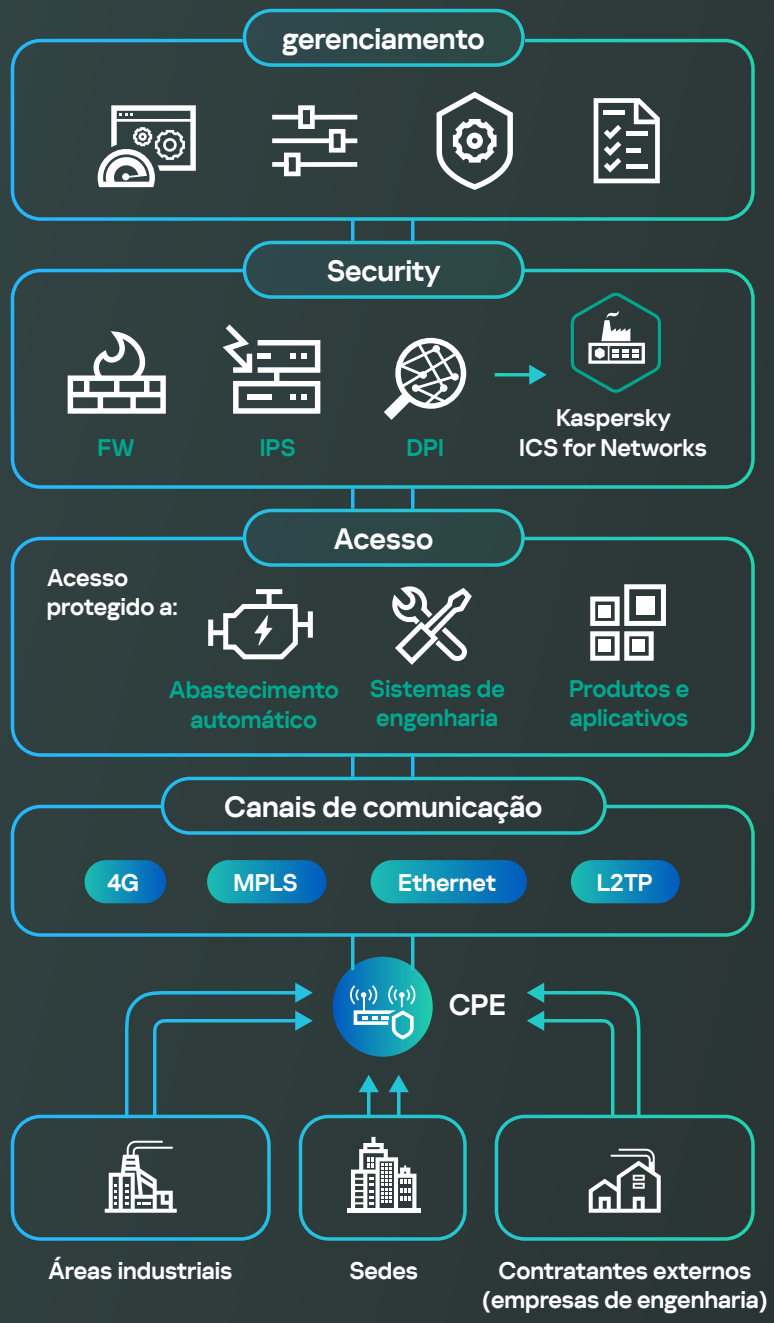
- Fácil escalabilidade
- Gerenciamento conveniente
- Otimização de custos
- Segurança centralizada

Uma única solução para redes industriais confiáveis

O Kaspersky SD-WAN permite que as empresas construam uma rede geograficamente distribuída e tolerante a falhas com gerenciamento centralizado, garantindo a continuidade dos processos de produção. A arquitetura Kaspersky SD-WAN permite que você integre facilmente as ferramentas de segurança da Kaspersky e de terceiros por meio do gerenciador de funções de rede virtual (VNFs).

Usando a infraestrutura SD-WAN com o Kaspersky ICS for Networks, você pode organizar um sistema de monitoramento e de proteção centralizado para inúmeras instâncias industriais distribuídas.

Fale conosco



Visitar site

Kaspersky Antidrone

SAFE MONEY

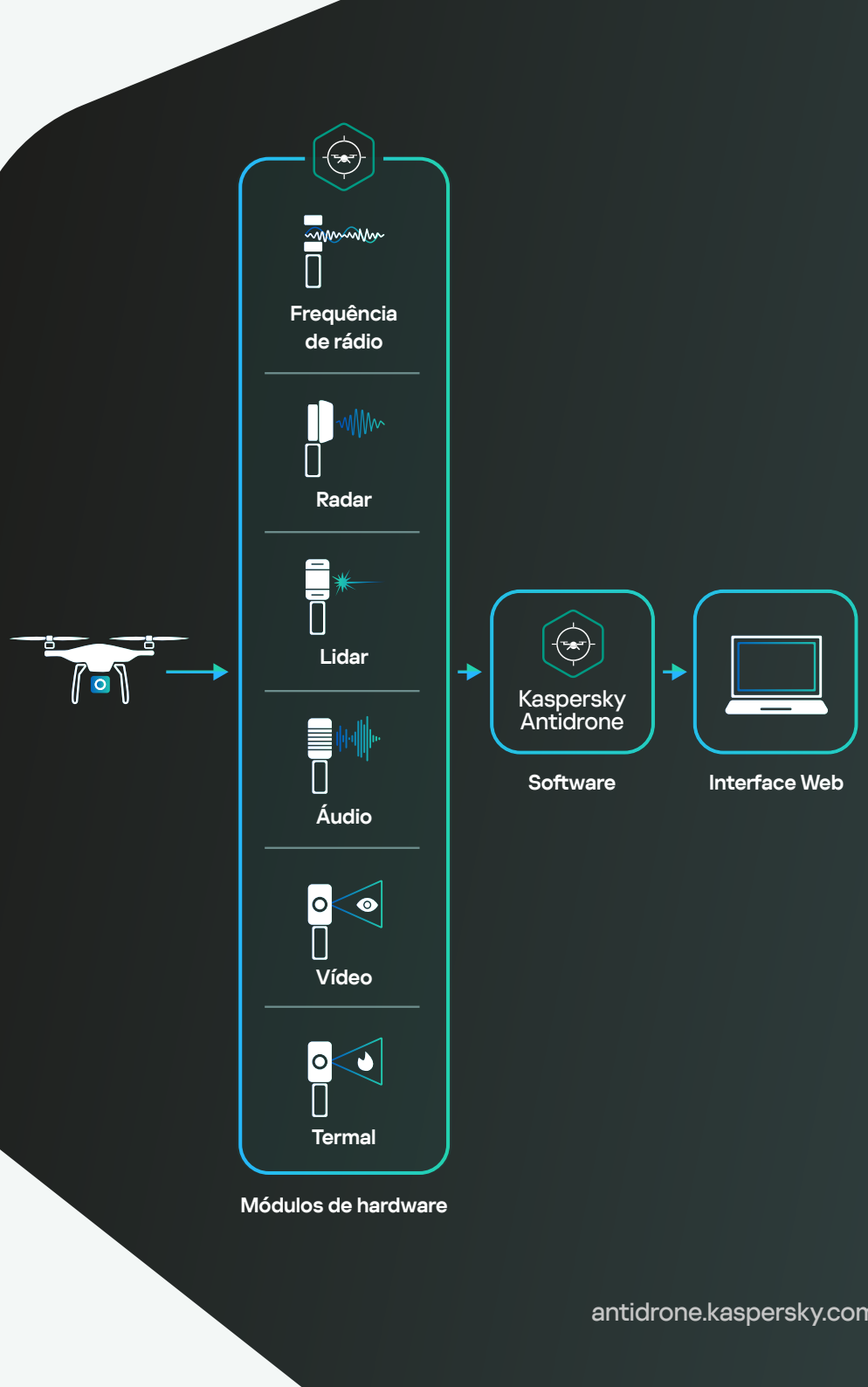
Principais recursos

- Detecção e rastreamento por drone
- Classificação de drones usando redes neurais
- Jamming direcional e omnidirecional

Solução de monitoramento e de defesa por drone

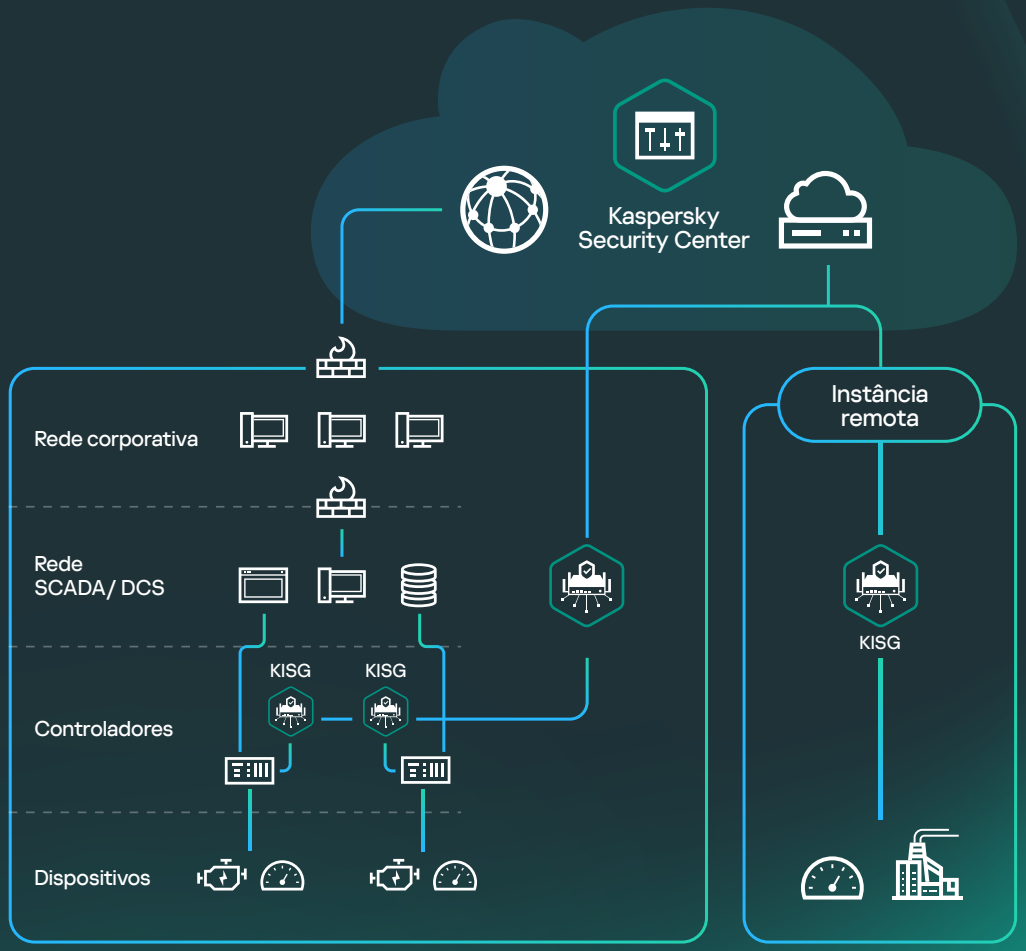
O Kaspersky Antidrone reduz a probabilidade de paralisações de processos em empresas industriais, impedindo que drones não autorizados entrem em seu território. O sistema verifica automaticamente o espaço aéreo, detectando e classificando drones. As informações sobre o que está acontecendo são exibidas na interface web. Em caso de ameaça, e com as permissões apropriadas, o operador pode neutralizar o drone.

A solução Kaspersky Antidrone é modular e pode ser aplicada em locais industriais de qualquer tamanho. A solução também suporta o modo de operação "amigo ou inimigo", permitindo que clientes usem seus próprios drones e evitem a intervenção de veículos aéreos não tripulados ilícitos.



Solicite uma demo Folheto

antidrone.kaspersky.com



aprotech

O desenvolvimento técnico e comercial desta solução é realizado pela Adaptive Production Technologies LLC (Aprotech, uma subsidiária da Kaspersky).

Fale conosco Solicite uma demo Folheto

Visitar site

Kaspersky
IoT Secure
Gateway

SAFE MONEY

Principais recursos

- Coleta e transporte seguro de dados de dispositivos IoT para plataformas digitais e na nuvem
- Kaspersky Cyber Immunity, com base no KasperskyOS, oferece resistência "inata" à grande maioria dos tipos de ciberataques sem a necessidade de ferramentas de segurança adicionais.
- Transparência da infraestrutura, gerenciamento centralizado de eventos e otimização da produção

Dados confiáveis para o desenvolvimento de negócios na indústria 4.0

A solução consiste em Kaspersky IoT Secure Gateways baseados no KasperskyOS e no console de gerenciamento do Kaspersky Security Center (KSC). Os gateways coletam e transferem dados de forma segura do equipamento para plataformas digitais e na nuvem, fornecendo inteligência empresarial de alta qualidade para otimizar a produção e prevenir incidentes. O console permite mapear eventos de diferentes fontes e gerenciar até 100.000 estações de trabalho físicas, virtuais e na nuvem.

Visitar site

Kaspersky Secure Remote Workspace

SAFE MONEY

Aplicação do produto

Risco

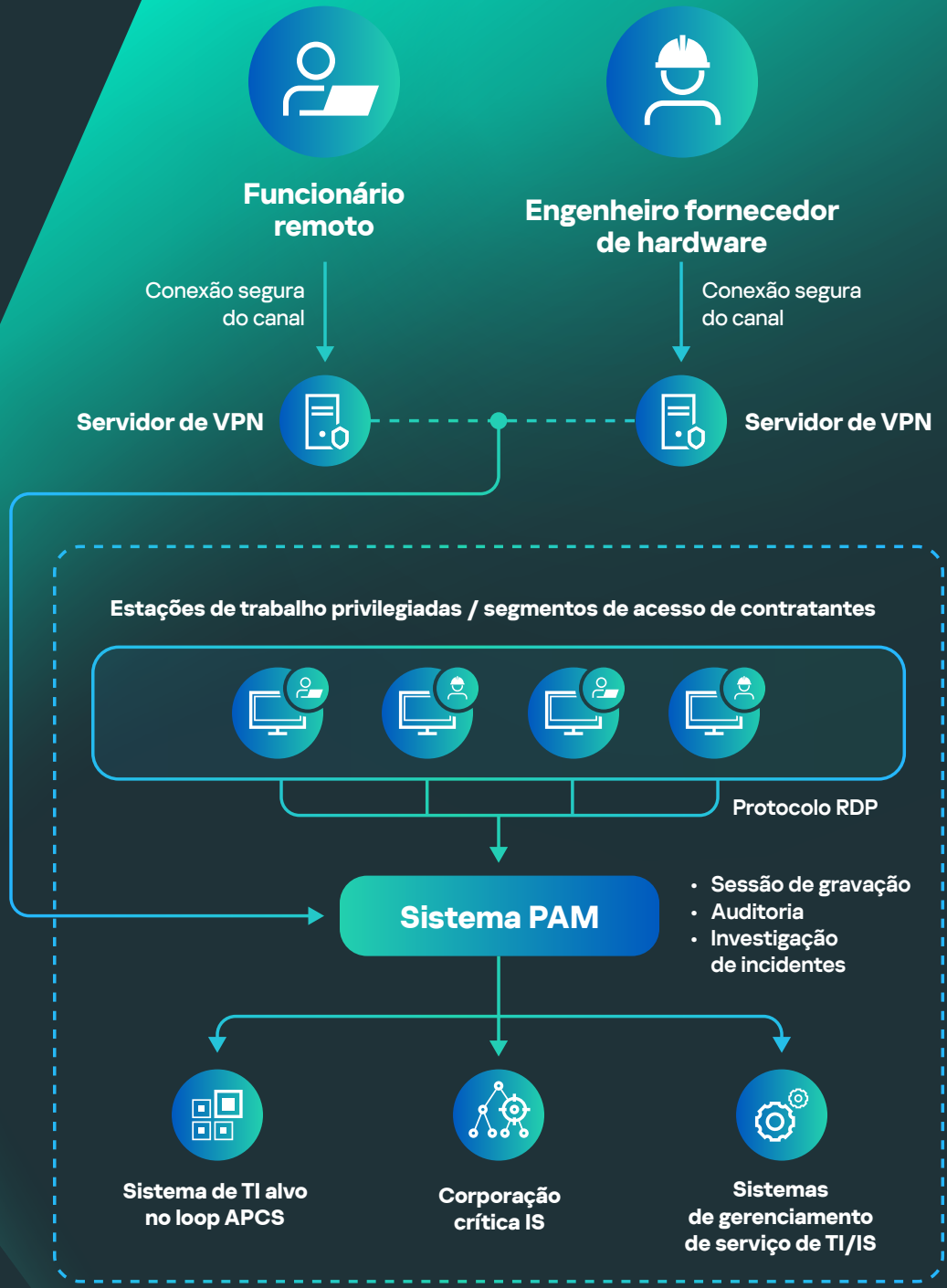
As estações de trabalho dos usuários estão entre os alvos mais comuns de ciberataques.

Solução

Kaspersky Secure Remote Workspace (KSRW) é uma solução para construir uma infraestrutura gerenciada e funcional de "clientes leves" baseada no próprio microkernel KasperskyOS do sistema operacional Kaspersky Security.

Infraestrutura Cyber Immune Thin Client

Cyber Immune Thin Clients, como parte do Kaspersky Secure Remote Workspace, fornecem uma conexão segura para desktops virtuais, incluindo uma zona confiável para conectar usuários à infraestrutura industrial.

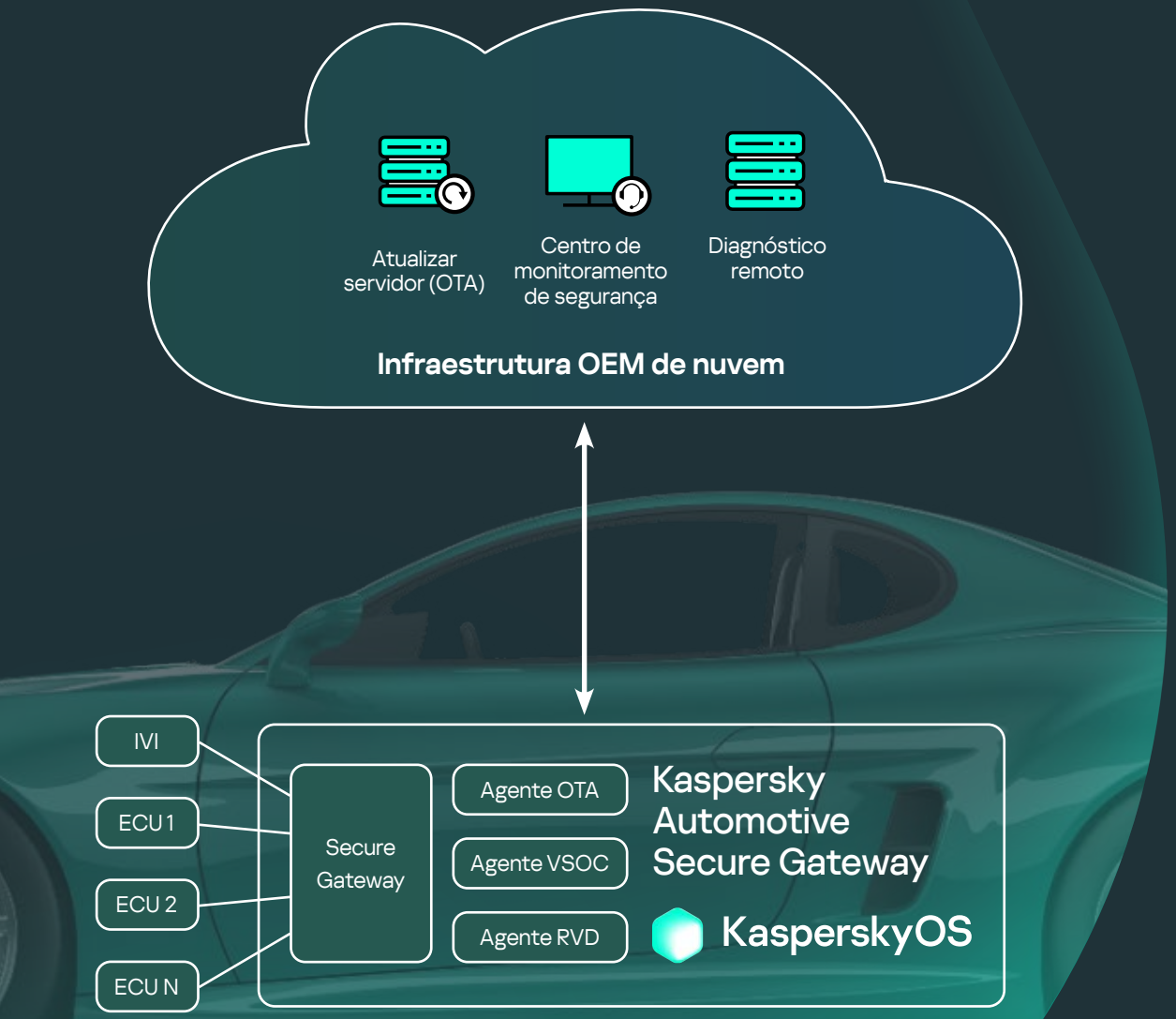


Visão geral da solução Solicite uma demo Folheto

Visitar site

Kaspersky Automotive Secure Gateway

SAFE MONEY



Proteção de veículos

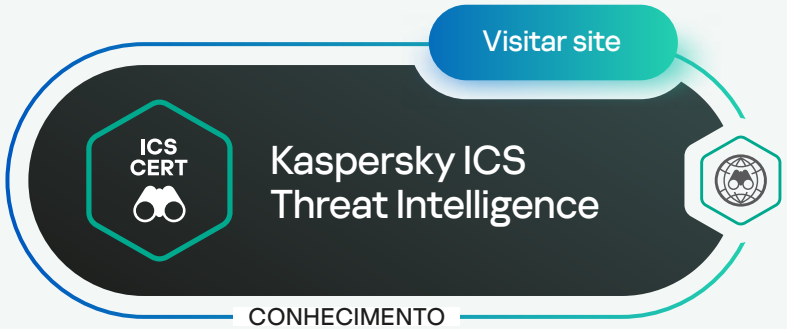
- Acesso não autorizado
- Ataques visados a ECU
- Ataques por meio de sistemas de infoentretenimento de veículos (IVI)
- Diagnósticos maliciosos
- Comprometimento do sistema de atualização
- Conexões não controladas de fluxo de dados, interrupção de comunicação

Principais benefícios

- Solução segura desde a concepção
- Ajuda a cumprir as regulamentações de cibersegurança
- 4 em 1: gateway conectado, gateway de segurança, OTA-master e agente VSOC
- Conformidade com ISO21434, ISO26262, AUTOSAR Adaptive, Uptane

AUTOSAR

Fale conosco Folheto



Grande compreensão de ameaças e vulnerabilidades de cibersegurança industrial para avaliação eficiente de riscos, detecção bem-sucedida de ataques, investigação de incidentes e resposta.

Apoiado por um arsenal de conhecimento e experiência do Kaspersky ICS CERT, o primeiro CERT privado em cibersegurança industrial.

Principais recursos

- Detecção rápida de ameaças e recursos analíticos abrangentes
- Aumenta a eficácia das investigações e pesquisas de ameaças ativas
- Informações detalhadas sobre ameaças e vulnerabilidades para uma tomada de decisões mais precisa

Esteja um passo à frente dos seus adversários com visibilidade detalhada das ciberameaças direcionadas à sua organização

Kaspersky ICS Threat Data Feeds

Um conjunto de feeds de dados de inteligência de ameaças regularmente atualizados, adaptados às necessidades específicas da cibersegurança industrial

Inteligência de ameaças

Fluxos de dados automáticos

Relatórios do Kaspersky ICS Threat Intelligence

Fornece inteligência aprofundada e maior conscientização sobre campanhas maliciosas que visam organizações industriais, bem como informações sobre vulnerabilidades encontradas nos mais populares sistemas de controle industrial.

Kaspersky Ask the Analyst

Um serviço para clientes solicitarem orientação e insights de especialistas sobre ameaças específicas que estão enfrentando ou têm interesse.

Solicite uma demo Visão geral da solução Fale conosco

O serviço Kaspersky Threat Data Feed fornece informações de inteligência de ameaças em tempo real, ajudando organizações industriais a proteger suas redes e sistemas contra ciberameaças. Os feeds de dados incluem informações sobre malware conhecidos, sites de phishing, vulnerabilidades e exploits mais recentes, e outros tipos de ciberameaças. Fornecidos com contexto, os dados podem ser usados diretamente para revelar o "plano geral" e responder perguntas do tipo "quem, o quê, onde, quando" para identificar seus adversários e a tomar decisões rápidas para agir.

O que você recebe:

Feed de dados de hash do Kaspersky ICS

Inteligência de ameaças para ICS atuais e outros sistemas usados em TO para simplificar e automatizar a detecção e a investigação imediata de ataques

#prevenção

#detecção

#investigação

Kaspersky ICS Vulnerability Data Feed

Dados verificados e refinados sobre vulnerabilidades descobertas em software e hardware de sistemas ICS e outros sistemas utilizados em ambientes industriais, fornecidos em um formato legível por máquina

#prevenção

#detecção

#investigação

ICS Vulnerability Data Feed em formato OVAL

Feed atualizado regularmente contendo definições OVAL para detecção automatizada de vulnerabilidades conhecidas em sistemas SCADA e outros softwares industriais

#detecção

Fale conosco Mais sobre o serviço

Visitar site

Relatórios do Kaspersky ICS Threat Intelligence

CONHECIMENTO

O Kaspersky ICS Threat Intelligence Reporting fornece inteligência aprofundada e uma maior conscientização sobre as diversas campanhas maliciosas que têm como alvo organizações industriais, bem como informações sobre vulnerabilidades encontradas nos mais populares sistemas de controle industrial e tecnologias subjacentes. Informações detalhadas adaptadas para organizações industriais ajudam os clientes a proteger ativos críticos, incluindo componentes de software e hardware, e garantir a segurança e continuidade do processo tecnológico.

Os relatórios são entregues via **Kaspersky Threat Intelligence Portal** ou podem ser acessados pela API.

O que você recebe:

Relatórios de APTs
Relatórios sobre novas APT e campanhas de ataque de alto volume que visam organizações industriais e atualizações sobre ameaças ativas

O cenário de ameaças
Relatórios sobre mudanças significativas no cenário de ameaças para sistemas de controle industriais, fatores críticos recém-descobertos que afetam os níveis de segurança de ICS e a exposição de ICS a ameaças, incluindo informações específicas por região, país e setor.

Vulnerabilidades detectadas
Relatórios sobre vulnerabilidades identificadas pela Kaspersky nos mais populares produtos utilizados nos sistemas de controle industrial, a internet das coisas industrial e infraestruturas em várias indústrias.

Análise e mitigação de vulnerabilidades
Nossos consultores fornecem recomendações acionáveis de especialistas da Kaspersky para ajudar a identificar e mitigar ameaças.

Fale conosco Mais sobre o serviço

***Informações adicionais sobre relatórios publicados**

- Informações sobre vulnerabilidades de ICS
- Estatísticas de ameaças e novas tendências em sistemas de controle de processos por região e indústria
- Análise de malwares visando o ICS
- Informações sobre requisitos e padrões regulatórios

O que você recebe:

O Kaspersky Ask The Analyst complementa o portfólio do Kaspersky Threat Intelligence Com este serviço, você pode entrar em contato com especialistas para obter suporte e informações úteis sobre ameaças e vulnerabilidades específicas que você está enfrentando ou nas quais está interessado. Usando esses dados, você pode melhorar suas defesas contra ameaças que têm como alvo a sua empresa ou infraestrutura industrial.

Principais benefícios

Acesso a especialistas líderes em inteligência de ameaças, incluindo especialistas em segurança industrial do Kaspersky ICS CERT

Informações contextuais personalizadas e detalhadas para possibilitar investigações eficazes

Instruções detalhadas de nossos especialistas sobre como responder rapidamente a ameaças e vulnerabilidades

Fale conosco Mais sobre o serviço

Visitar site

Kaspersky Security Awareness

CONHECIMENTO

Aumento de ciberliteratura do funcionário

- Materiais de treinamento que capacitam seus funcionários com o conhecimento necessário sobre os aspectos mais importantes da cibersegurança industrial, aumentando o nível de conscientização em todos os níveis da organização
- Kaspersky Interactive Protection Simulation — treinamento baseado em jogos por meio de simulações de negócios com uma infinidade de cenários em diferentes setores: energia térmica, energia hidrelétrica, petróleo e gás, petroquímica, empresas de petróleo, etc.
- Kaspersky Automated Security Awareness Platform (ASAP) — módulos de aprendizado interativo e ataques simulados de phishing projetados para promover comportamentos cibernéticos seguros

Principais tópicos abordados

- E-mail
- Sites e Internet
- Senhas e contas
- Redes sociais e aplicativos de mensagens
- Cibersegurança para a indústria
- Segurança do PC
- Dispositivos móveis
- Dados confidenciais
- Segurança de cartões bancários e PCI DSS
- GDPR

[Fale conosco](#) [Experimente agora](#) [Catálogo de treinamento](#)

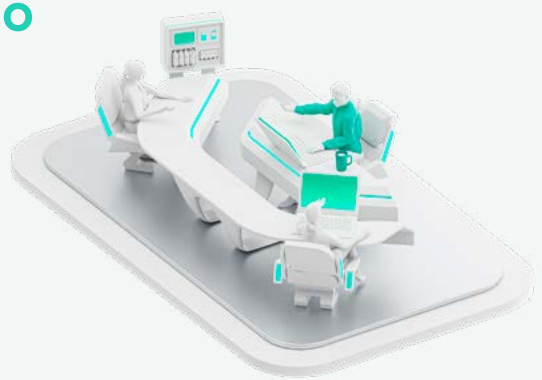
Visitar site

Kaspersky ICS CERT Expert Trainings

CONHECIMENTO

Aprendizado aplicado

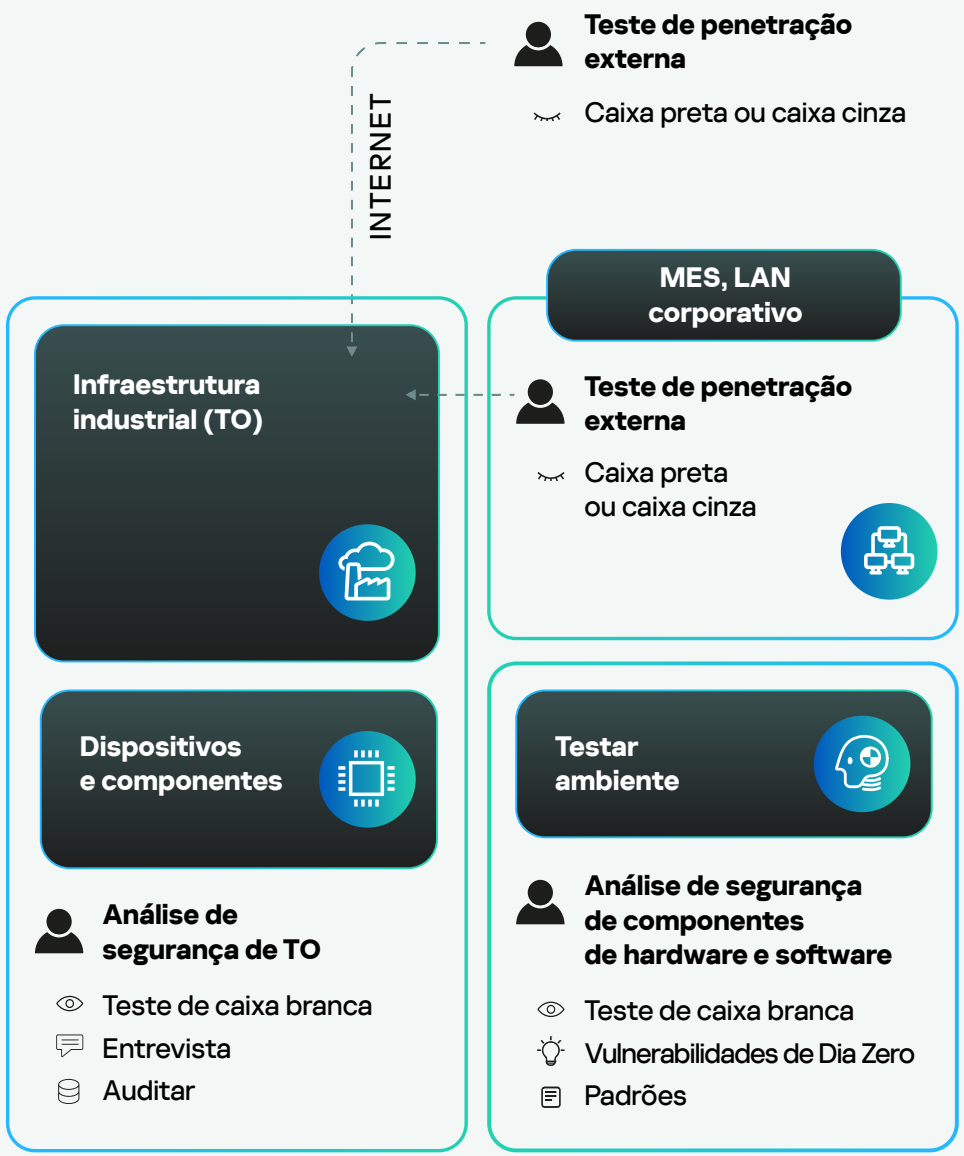
Nosso programa de treinamento ICS foi especialmente projetado para garantir que profissionais de tecnologia da informação (TI), tecnologia operacional (TO) e segurança da informação (SI), bem como gerentes e outros funcionários, possam expandir seu conhecimento em cibersegurança industrial e adquirir habilidades práticas especializadas.



Habilidades práticas de especialistas da Kaspersky

- Perícia digital e resposta a incidentes
- Explorando vulnerabilidades em dispositivos TO/IoT e softwares industriais
- Programas de treinamento interfuncionais para especialistas em TI, TO e SI

[Fale conosco](#) [Catálogo de treinamento](#)



Visitar site

Kaspersky ICS Security Assessment

EXPERIÊNCIA

Análise da segurança da sua infraestrutura industrial

Uma abordagem abrangente para identificar vulnerabilidades e fraquezas de segurança em infraestruturas industriais, incluindo:

- Superfície de ataque
- O nível de segurança da infraestrutura de rede industrial, DCS, e dispositivos industriais
- Riscos de comprometimento de sistemas críticos

Verificação de componentes críticos

- Tráfego de rede, incluindo protocolos industriais
- Componentes de controle de processo: SCADA, PLC, medidores inteligentes, etc.
- Elementos físicos do sistema de controle do processo automatizado
- Arquitetura de rede, incluindo redes ACS

Mais sobre o serviço Fale conosco

Visitar site

Kaspersky Managed Detection and Response

EXPERIÊNCIA

Principais recursos

- Detecção proativa de ameaças: indicadores de ataque patenteados ajudam a rastrear ameaças não detectadas dentro do sistema de controle
- Resposta guiada e automatizada (com investigação forense completa e análise de malware disponível sob demanda)
- Especialidade em cibersegurança de ICS: respaldada por uma das equipes de detecção de ameaças proativas mais bem-sucedidas e experientes do setor

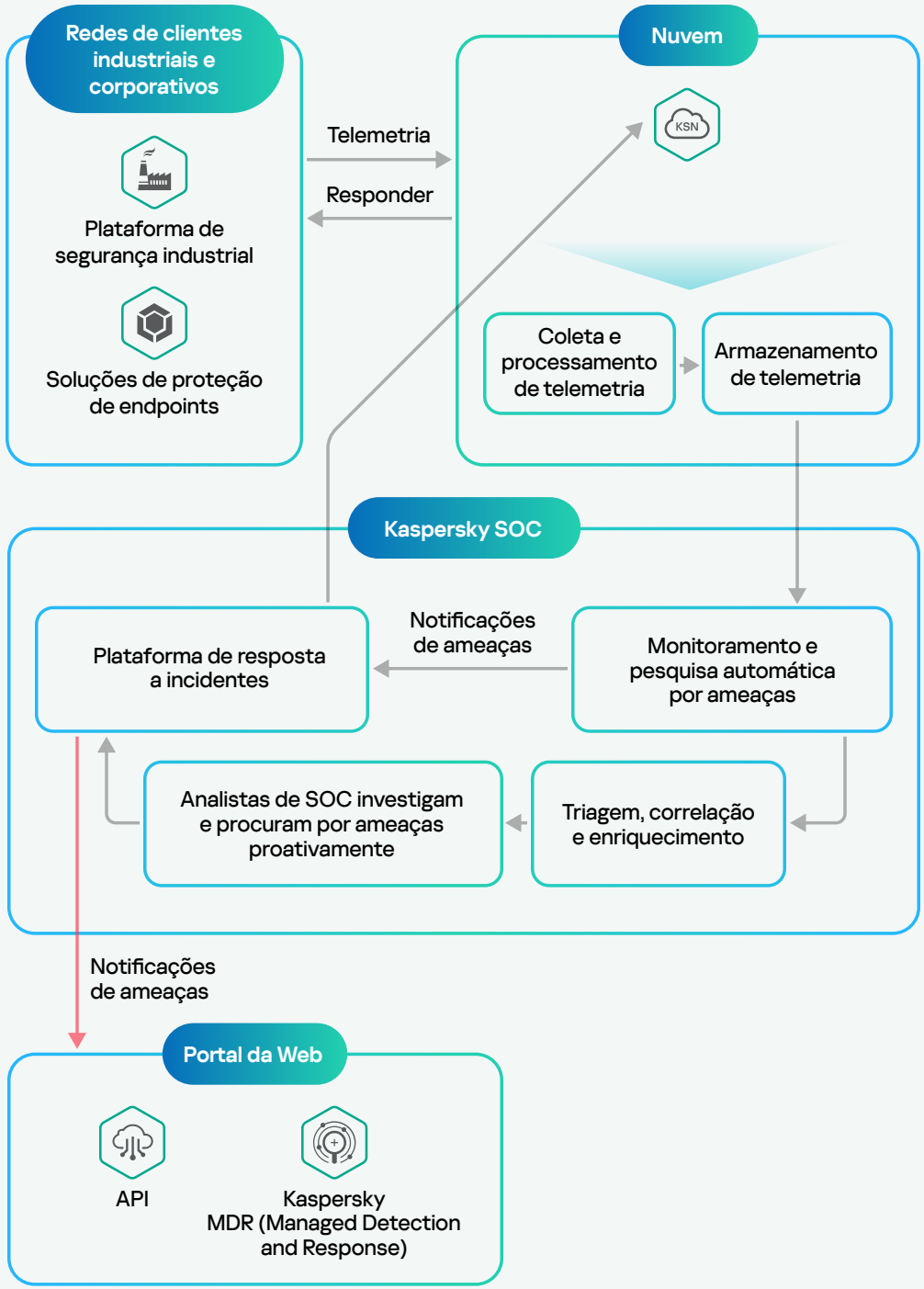
O que você recebe:

- Caça, detecção e eliminação contínuas de ameaças direcionadas à sua empresa industrial
- Redução de custos de segurança ao eliminar a necessidade de contratar novos especialistas em cibersegurança
- Todos os principais benefícios de um SOC sem precisar estabelecer um internamente

25% dos nossos clientes protegidos são do setor industrial

Veja o relatório MDR para saber mais

Fale conosco Mais sobre o serviço



Visitar site

Kaspersky
Incident Response

EXPERIÊNCIA

Reagindo a incidentes

Risco

Uma vulnerabilidade é suficiente para que cibercriminosos ganhem controle de sistemas industriais inteiros

Solução

- Rápida eliminação das consequências de um incidente pelo Kaspersky Global Emergency Response Team
- Análise das causas, fontes e consequências do incidente
- Visão detalhada do malware usado
- Suporte adicional da Kaspersky ICS-CERT

Composição do serviço

Resposta a incidentes: investigação e eliminação de ameaças

Análise forense digital: Análise de evidências digitais

Análise de malware: obtenha uma visão detalhada dos arquivos usados em um ataque

Solicite o manual de IR em Kaspersky ICS-CERT

Saiba mais

Fale conosco

Descubra as tendências de IR com a pesquisa do Kaspersky Global Emergency Response Team (GERT).

Um parceiro no qual você pode confiar

- Vinte e seis anos de experiência de classe mundial e petabytes de dados de ameaça processados
- ICS-CERT - Divisão própria de pesquisa de segurança de IoT / TO internacional
- Experiência comprovada na indústria de segurança de TI/TO com inúmeros prêmios e conquistas
- Mais de 100 certificados de interoperabilidade com soluções de fornecedores de automação
- Eficácia comprovada da tecnologia, conformidade com padrões e requisitos

[Mais sobre o ecossistema de TO]

[Mais sobre o ecossistema de TO]

[Fale conosco]