Kaspersky OT Cybersecurity

Oferta para o setor de operadores de redes elétricas, usinas e serviços públicos no setor de energia



kaspersky

Resumo do mercado

O setor de fornecimento de energia é fundamental para a sociedade, desempenhando um papel central no crescimento econômico, na melhoria da qualidade de vida e no apoio aos avanços tecnológicos. A eletricidade é um recurso essencial, que impulsiona diversas áreas estratégicas da sociedade, incluindo:

- Uso residencial e cidades inteligentes (iluminação pública, HVCA etc.)
- Transporte (EV, carga)
- Fabricação

O setor desempenha um papel importante no atingimento de emissões Net Zero, alinhado com os objetivos do Acordo de Paris (ONU). O setor apoia o fornecimento de energia para todos os outros setores e impulsiona a transição para o uso de energias renováveis.

A tendência do setor voltada para a energia limpa aponta a demanda por redes elétricas robustas e eficientes.

~x2

investimento mundial em energia limpa em comparação com combustíveis fósseis [1]

(1) World Energy Investment 2024, relatório da IEA

Objetivos de digitalização

A digitalização é um fator capacitador das metas de sustentabilidade no setor, com soluções digitais que apoiam os objetivos estratégicos de empresas do setor:

- Aprimoramento da segurança e eficiência de ativos
- Condução da energização e descarbonização global
- Aceleramento da implementação da infraestrutura de energia renovável
- Garantia de condições de trabalho seguras

Principais casos de uso de solução digital no setor

- **Dispositivos de Internet de Energia (IoE)**
  Capacita a automação para toda a área para o monitoramento e controle em tempo real das operações de redes de energia
- **Cloud Energy**
  Análise em tempo real, infraestrutura escalável, gerenciamento e integração remotos das novas tecnologias
- **Réplicas digitais para o setor de energia**
  Simulação de modo de rede de energia, insights preditivos, monitoramento e diagnóstico de equipamentos em tempo real
- **Rede de energia inteligente orientada por ML e IA**
  Otimização da manutenção preditiva e o monitoramento de condição
- **Robotização**
  Inspeções áereas e robóticas de usinas, gerenciamento de vegetação

Conforme a digitalização transforma o setor, as operações vão inevitavelmente enfrentar problemas de segurança.

Sistemas energéticos precisarão expandir os recursos de comunicação e automação que sejam seguros, confiáveis e eficazes.

2.3 p.p.

Redução da quantidade de computadores ICS no setor de energia com objetos maliciosos bloqueados no primeiro trimestre de 2025 (em comparação com o mesmo período em 2024)[2]

(2) Relatório sobre o cenário de ameaças para os sistemas de automação industrial gerado pelo ICS CERT

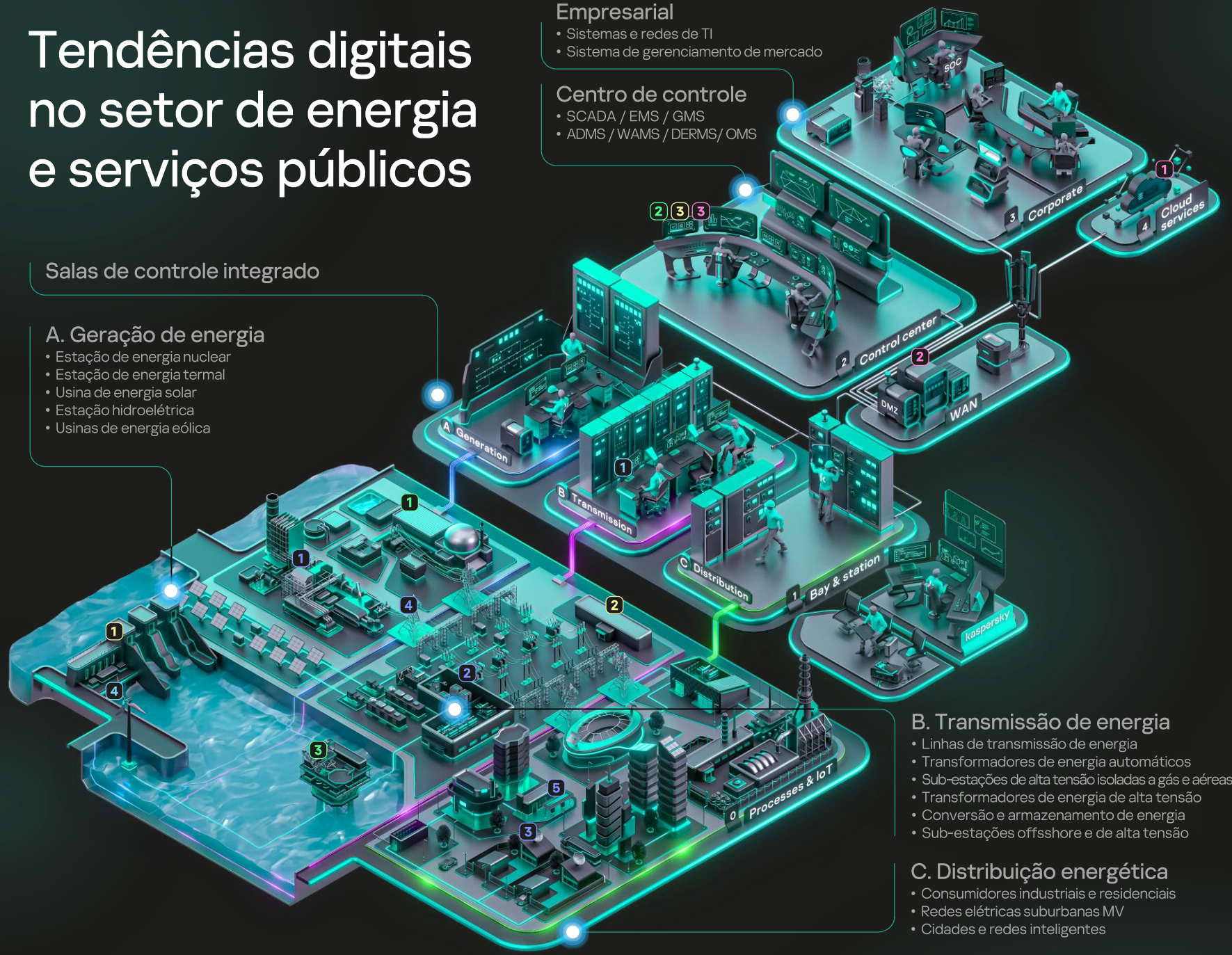
Tendências digitais no setor de energia e serviços públicos

Empresarial
- Sistemas e redes de TI
- Sistema de gerenciamento de mercado

Centro de controle
- SCADA / EMS / GMS
- ADMS / WAMS / DERMS/ OMS

Salas de controle integrado

A. Geração de energia
- Estação de energia nuclear
- Estação de energia termal
- Usina de energia solar
- Estação hidroelétrica
- Usinas de energia eólica



B. Transmissão de energia
- Linhas de transmissão de energia
- Transformadores de energia automáticos
- Sub-estações de alta tensão isoladas a gás e aéreas
- Transformadores de energia de alta tensão
- Conversão e armazenamento de energia
- Sub-estações offsshore e de alta tensão

C. Distribuição energética
- Consumidores industriais e residenciais
- Redes elétricas suburbanas MV
- Cidades e redes inteligentes

IoE
1. Medição inteligente de fornecimento energético e climático
2. Monitoramento de condições de equipamentos primários
3. Gerenciamento de recursos de energia distribuídos (DEI)
4. Monitoramento de condições de linhas de transmissão e distribuição (T&D)
5. Monitoramento de estações de carga e veículos conectados

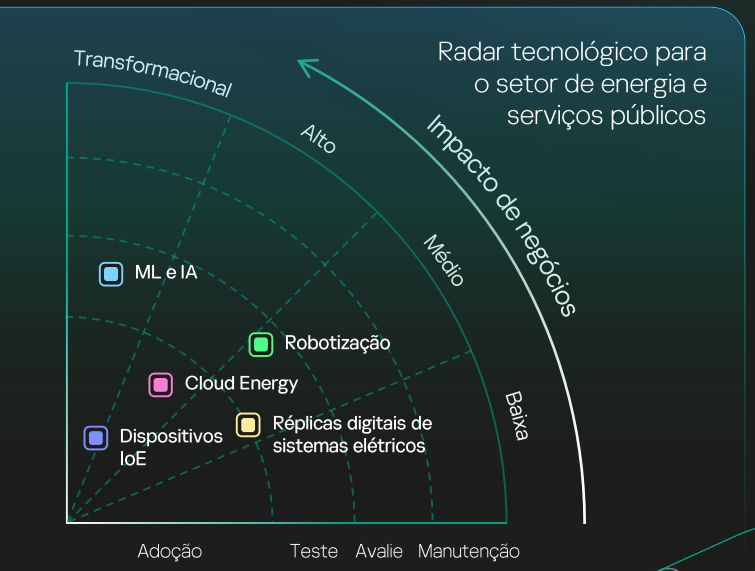
Cloud Energy
1. Análise preditiva do fornecimento usando previsões meteorológicas e outros dados
2. WANs que possibilitam a comunicação em tempo real entre sistemas OT, sensore e centros de controle de rede elétrica
3. Sistemas de Informação de Rede (NIS) fornecendo aos operadores de redes elétricas rotas e topologia de rede

Réplicas digitais de sistemas elétricos
1. Gerenciamento de desempenho de ativos com monitoramento de equipamentos e análise de causa raíz
2. Mapeamento de clusters de risco para visualizar áreas com riscos concentrados e prevenção de desencadeamento de falhas
3. Simulação de armazenamento de energia para otimização de planos de fornecimento e análise de picos de carga

ML e IA
1. Balanceamento de rede através de ajuste de fluxos de energia, minimizando perdas e prevenindo sobrecarga
2. Otimização de energia reativa e controle de tensão para evitar blecautes
3. Análise de dados de infraestrutura de medição inteligente para uma melhor comercialização e regulação da demanda de pico
4. Previsão de padrões meteorológicos para ajustar o posicionamento de pás eólicas

Robotização
1. Drones integrados com sensores para supervisão aérea
2. Automatização de atividades de inspeção para identificar problemas potenciais (ex.: hot spots, vazamentos, linhas de distribuição etc.)
3. Inspeção submarina de parques eólicos offshore

Desafios de cibersegurança no setor energético



A transformação digital no setor apresenta diversos desafios de cibersegurança

1. Relés numéricos e automação defasados
2. Aumento na quantidade de nodes como comprometimento
3. Acesso remoto e sincronização de tempo comprometidos
4. Falhas de segmentação de rede TI e OT
5. Regulamentações CIP

Relés numéricos e automação defasados

Cloud Energy | ML e IA



Cloud Energy

Controle de acesso e dados de clientes

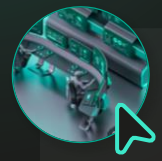
Controle de unidade multi SCADA

Simulador de usina energética

Controle de micro-rede elétrica

Otimizador de despachos

Exemplo de geração de energia



Camada externa

HMI central

Rede central

Servidores centrais

Infovia de aplicativos

Servidor de segurança

Servidor de aplicativos

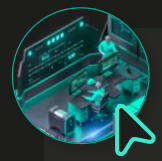


WAN

Servidores de terminais

Roteador

Roteador



Camada de aplicativos

Infovia de aplicativos

Servidor de aplicativos

Servidor de segurança

Nível de automação



Camada de automação

Infovia de automação

Controle de turbinas

Controle de tração de pit

Controle de boiler

Parte elétrica

Sistemas de terceiros

A integração de sistemas defasados com tecnologias modernas como ML, IA e nuvem representa diversos desafios críticos.
Problemas de compatibilidade podem ocorrer quando sistemas antigos enfrentam dificuldades para se comunicarem com tecnologias mais recentes. Interoperabilidade limitada pode interromper as operações e reduzir os ganhos de eficiência proporcionados pelas soluções modernas. Em particular, os sistemas legados geralmente não são capazes de se comunicar eficazmente com plataformas de nuvem ou ferramentas de automação orientada por IA.

Hardware legado geralmente é responsável por

>1/3

do consumo energético total das organizações [1]

(1) Estudo da Daisy Corporate Services

Características da solução



Como a Kaspersky pode ajudar

Kaspersky Industrial CyberSecurity

- Monitoramento contínuo de redes industriais para prevenir vulnerabilidades
- Detecção e resposta de endpoint
- Auditorias de segurança periódicas

Kaspersky Machine Learning for Anomaly Detection

- Previne falhas em sistemas de relé antigos usando a aprendizagem de máquina
- Detecta ciberameaças que visam relés defasados

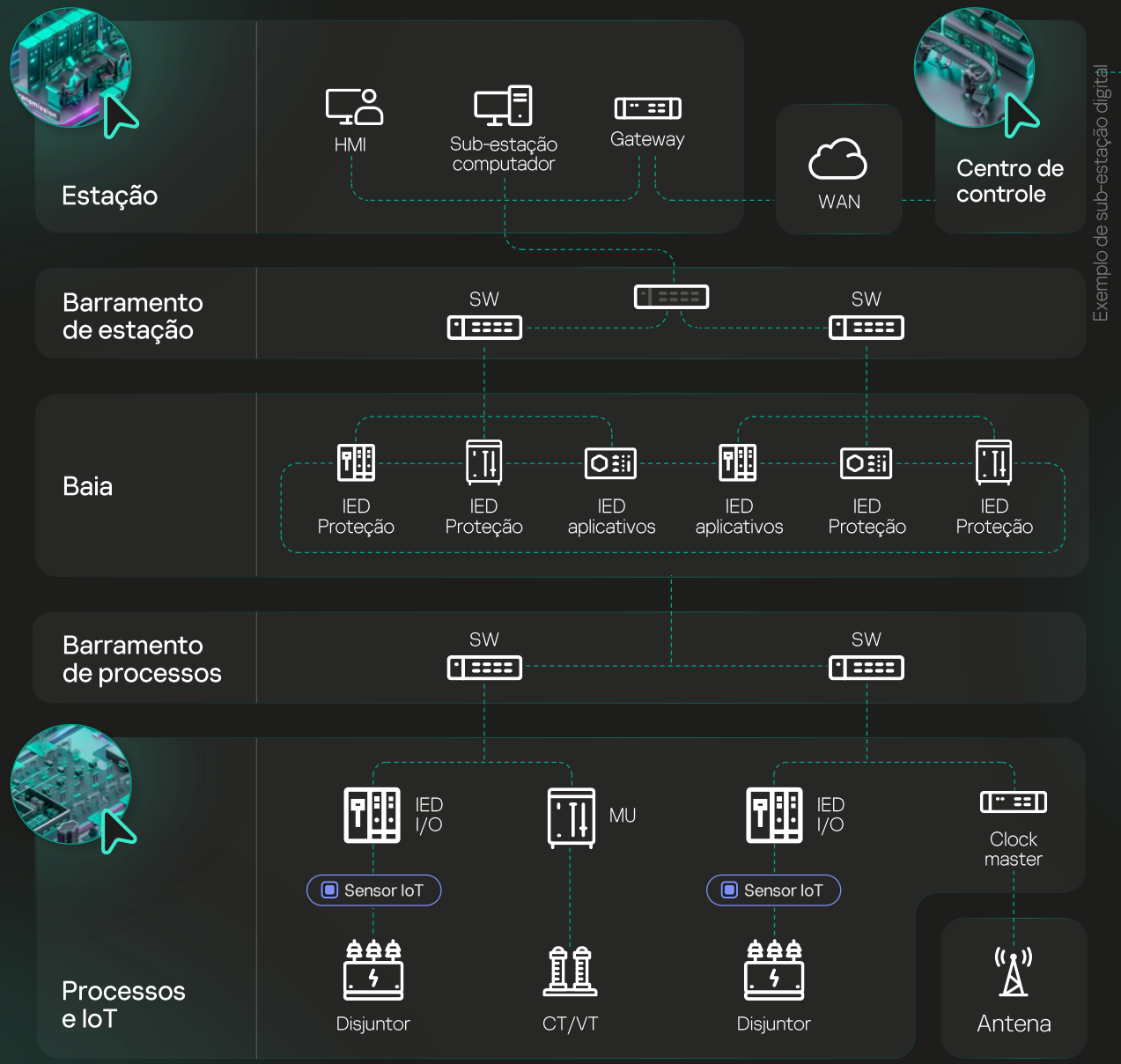
Ecossistema de serviços de suporte

Kaspersky ICS Threat Intelligence

- Análise completa para identificar e avaliar a exposição ao risco e os níveis de segurança de infraestruturas de redes industriais

Maior número de nodes comprometidos

IoE



Integração de componentes robóticos e IoT em sub-estações cria mais pontos de entrada para ciberataques conforme cada dispositivo desprotegido é um alvo em potencial.

Gerenciamento e aplicação de patches de diversos dispositivos conectados é um desafio, e uma única violação pode ter um efeito cascata por sistemas, com o perigo de paralisação generalizada.

Características da solução



Como a Kaspersky pode ajudar

Kaspersky Industrial CyberSecurity

- Visibilidade da rede e detecção de anomalias da rede
- DPI de comunicações industriais com recursos de aprendizagem de máquina
- Auditoria detalhada do sistema

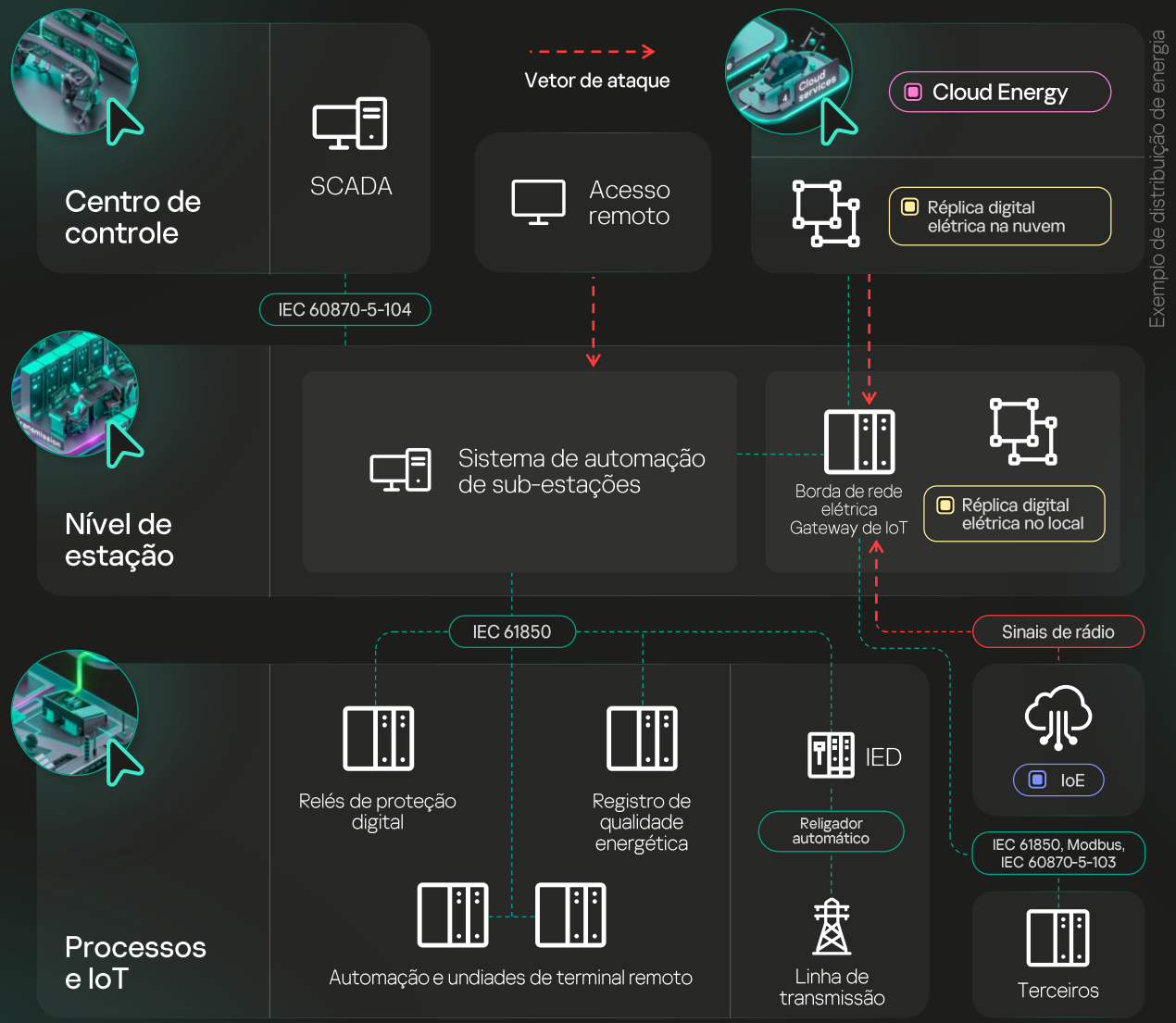
Ecossistema de serviços de suporte

Kaspersky Managed Detection and Response

- Busca de ameaças e investigação de incidentes
- Monitoramento de segurança

Comprometimento das conexões e da sincronização

IoE | Cloud Energy | Réplicas digitais de sistemas elétricos



Integração de tecnologias como IoE, réplicas digitais e serviços na nuvem em sub-estações aumentam o risco de ciberataques causados por conexões comprometidas, o que pode acarretar em acesso não autorizado para sistemas SCADA e redes de controle. Além disso, manter uma sincronização de tempo precisa para relés de proteção e unidades de medição de fase é crítico, conforme erros podem resultar em falhas de operação de dispositivos na rede elétrica

Características da solução



Como a Kaspersky pode ajudar

Kaspersky Next XDR Expert

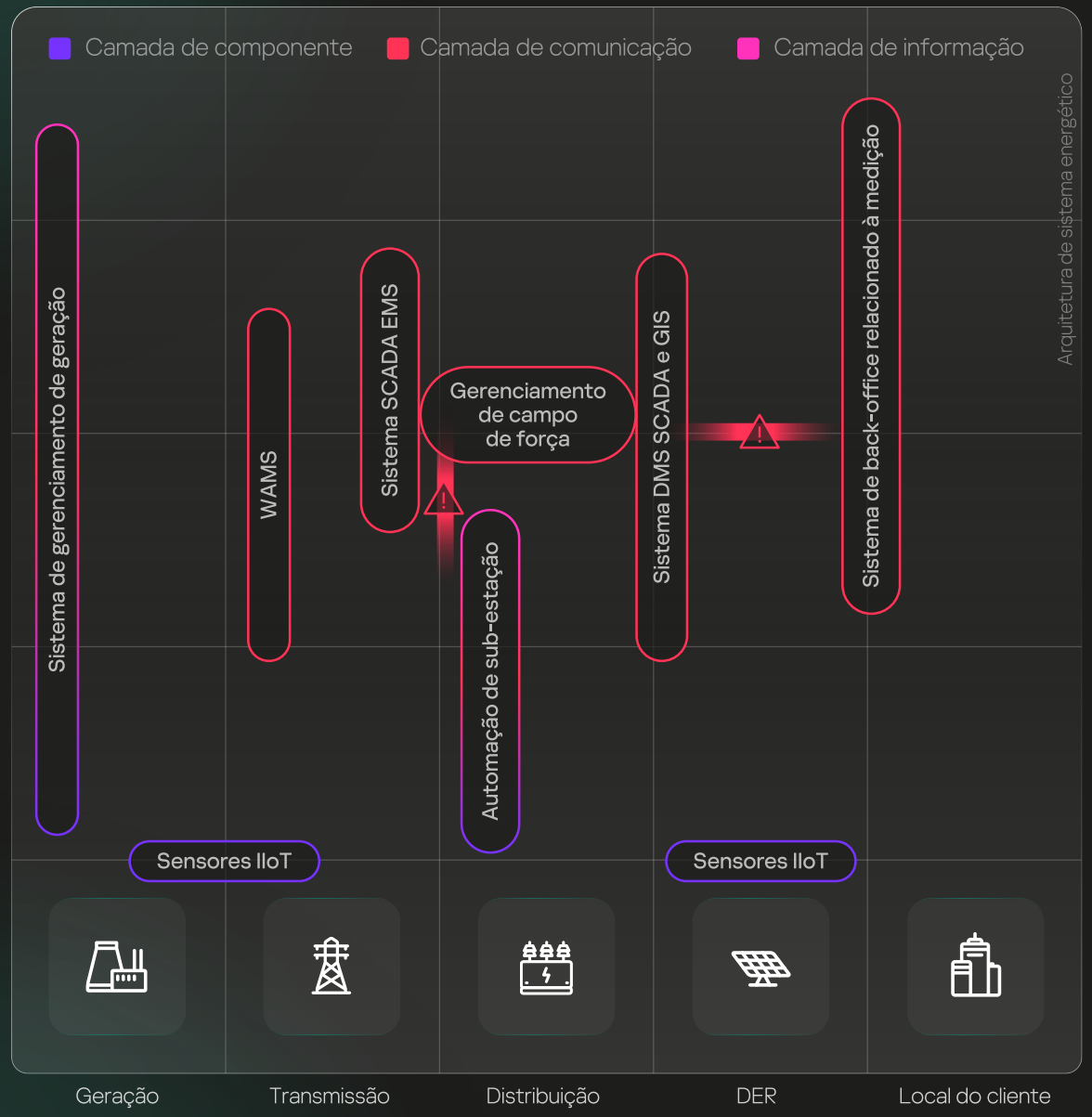
- Proteção robusta de endpoints físicos e virtuais
- Cobertura ponta a ponta em todas as infraestruturas complexas

Kaspersky Thin Client

- Conexão remota e engenharia executada pela equipe e terceirizados
- Monitoramento e gerenciamento centralizado de todos os eventos de infraestrutura de dispositivos

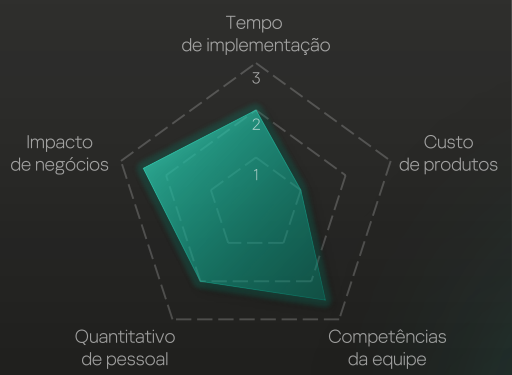
Falhas de segmentação de rede TI e OT

IoE



Segmentação de rede inadequada em redes elétricas, especialmente com a integração de réplicas digitais, pode levar a vulnerabilidades de segurança substanciais. Quando essas redes não são segmentadas corretamente, o caráter interconectado das réplicas digitais pode aumentar o rsico de ciberataques, propagando-os de sistemas de TI para a infraestrutura de OT crítica. Isso pode interromper a distribuição de energia e causar blecautes de ampla proporção

Características da solução



Como a Kaspersky pode ajudar

Kaspersky Industrial CyberSecurity

- Análise de tráfego de rede para identificar anomalias e ameaças
- Proteção, detecção e resposta para endpoints
- Segmentação de rede e conformidade de uso

Kaspersky SD-WAN

- Monitoramento de rede distribuída em tempo real.
- Visibilidade de rede
- Segurança e gerenciamento de rede unificados

Ecossistema de serviços de suporte

Kaspersky ICS Security Assessment

- Identifica falhas de segurança na arquitetura da rede
- Fornece recomendações acionáveis para remediação
- Teste de penetração externa

Regulamentações CIP

As regulamentações de cibersegurança para o setor energético e de serviços públicos varia globalmente, mas têm em geral um objetivo comum: aumentar a resiliência, proteger a infraestrutura crítica e garantira continuidade do serviço. Muitos países implementaram regulamentações para garantir que provedores de energia elétrica e operadores de redes elétricas adotem práticas de cibersegurança, conduzindo avaliações periódicas de vulnerabilidade e garantam a conformidade com protocolos de resposta a incidentes padronizada.

Global

- ISA/IEC 62443
- IEC 62351 (IEC 61850 TR)
- ISO/IEC 27019
- IEEE 1547.3-2023, C37.240, 1686
- Série de Segurança Nuclear IAEA No. 17-T

Indonésia

- PR 47/2023 Gestão de Crise Cibernética e Estratégia de Cibersegurança Nacional
- BSSN Reg. 1/2024 Gestão de Incidentes Cibernéticos
- BSSN Reg. 2/2024 Gestão de Incidentes Cibernéticos

Egito

- Diretrizes Técnicas ENRRA para Cibersegurança em Usinas Nucleares

Emirados Árabes Unidos

- Estratégia de Cibersegurança Nacional
- Estrutura de Proteção de Infraestrutura de Informações Críticas DESC (CII)
- Política CIIP NESA

Turquia

- Plano de Cibersegurança NDK para Usinas Nucleares
- Regulamentação BTK CIPR
- Lei de Cibersegurança No. 7545

Tailândia

- NCSA B.E. 2566
- NCSA B.E. 2562
- NCSA B.E. 2564

Arábia Saudita

- Controles de Cibersegurança OT OTCC-1:2022
- Controles de Cibersegurança Essenciais ECC-1:2018

Brasil

- Estratégia de Cibersegurança Nacional (E-Ciber)
- Resolução ANEEL No. 964/2021
- PRODIST - Módulo 8 ANEEL

África do Sul

- Ato de Proteção da Infraestrutura Crítica
- Orientação NNR RG-0014
- Estrutura de Política de Cibersegurança Nacional

Índia

- Diretrizes e Regulamentações de Cibersegurança CEA
- Diretrizes NCIIPC
- Diretivas CERT-In
- Diretrizes e Códigos de Segurança AERB

China

- GB/T 44462.1-2024
- GB/T 36572-2018
- GB 42250-2022
- GB/T 36627-2018

Malásia

- Regulamentações NACSA CNII
- Diretrizes de Cibersegurança da Malásia (MyVAC)
- Regras de Cibersegurança Suruhanjaya Tenaga

Europa

- Diretiva NIS2
- Diretiva CER
- Diretrizes ENISA
- Código de Rede sobre a Cibersegurança de Fluxos Elétricos Transfronteiriços

EUA

- NERC CIP
- NIST CSF
- Guia Regulatório NRC

França

- Estratégia de Cibersegurança Nacional
- Estrutura de Cibersegurança ANSSI para ICS
- Lei de Proteção de Infraestrutura de Informação Crítica

Alemanha

- IT-Sicherheitsgesetz 2.0
- Energiewirtschaftsgesetz
- BSI KritisV / BDEW- B3S

Holanda

- Estratégia de Cibersegurança da Holanda (NLCS)
- Ato de Segurança de Sistemas e Redes de Informação (WBNI)
- Guia NSCS para Medidas de Cibersegurança

Espanha

- Estrutura de segurança nacional
- Decreto Real CNPI 704/2011
- Guias de Segurança CCN-STIC

Reino Unido

- Regulamentações de Segurança da Indústria Nuclear (NISR)
- NCSC CAF
- Orientação OT NCSC
- Cibersegurança para IACS (OG86)

Como a Kaspersky pode ajudar

Kaspersky Industrial CyberSecurity

Soluções Kaspersky protegem usinas elétricas, sub-estações, redes elétricas e outros elementos de sistemas energéticos para manter a continuidade de operações industriais e de serviços públicos críticos com uma abordagem baseada na 'defesa aprofundada'.

Soluções para redes elétricas em conformidade com **ISA/IEC 62443, NIS2, SOC 2 Type2, ISO/IEC 27001, GB 42250-2022**

Compatibilidade testada:

Schneider Electric, GE, CHINT, Valmet, SIEMENS, ProSoft Systems, EKRA, Mitsubishi

Mais de 150

sistemas de mais de 50 fornecedores

Kaspersky Security Awareness e Treinamento Especializado

Capacite os funcionários com habilidades de cibersegurança essenciais em conformidade com os requisitos da Diretiva NIS2

Leia mais sobre a Diretiva NIS2 e a conformidade dos nossos produtos

Resiliência cibernética com o ecossistema OT Kaspersky

Inventário e avaliação

Experiência

Descoberta de Ativos de Rede

- Identifique todos os ativos de software e hardware na infraestrutura de OT
- Crie um inventário detalhado para planejar sua estratégia de cibersegurança

Inventário de endpoints

- Catalogue componentes de hardware e software
- Mantenha um inventário atualizado para identificar ativos críticos e vulnerabilidades

Desenvolvimento de políticas

- Desenvolva políticas e procedimentos abrangentes.
- Use análises de impacto e perigo para estabelecer níveis de cibersegurança e identificar os controles necessários.

Segurança essencial

Tecnologia

Reforço de sistema operacional

- Configure sistemas com segurança e aplique patches e atualizações regularmente
- Implemente controles adicionais
- Prevenção de exploits e verificação de dispositivos removíveis

Controle de Aplicativos

- Restrinja aplicativos não autorizados para manter a integridade do sistema

Proteção de endpoint

- Implemente soluções anti-malware para proteger dispositivos em ambientes ICS e OT.

Recursos avançados de detecção de ameaças, auditoria e conformidade

Conhecimento+Tecnologia+Expertise

Visibilidade da rede

- Monitore o tráfego de rede para detectar anomalias e compreender padrões de ataque.

Detecção de ameaça e anomalia

- Use aprendizagem de máquina e DPI para identificar intrusões e anomalias na rede
- Use tecnologia EDR para monitorar telemetria de hosts OT

Auditorias de segurança

- Conduza verificações de vulnerabilidade e auditorias de conformidade regularmente.

Controle de configuração

- Mantenha as auditorias de sistema e configurações de controle detalhados

Gestão da conformidade

- Garanta a conformidade com os requisitos regulatórios e normas da indústria.

Segmentação de rede

Conhecimento+Tecnologia+Expertise

Prevenção contra intrusos

- Aprimore a detecção de ameaças avançadas e conte com recursos de prevenção para integrar equipamentos de rede existentes.

Fluxo de dados restrito

- Use SD-WAN e VLANs para otimizar a segmentação e fluxo de dados
- Aplique controles de segurança, mesmo em locais remotos e altamente reduzidos

Controles IoT

- Implemente a visibilidade de controles de segurança avançada garantida por gateways e protocolos projetados para dispositivos IoT

Acesso remoto

- Use dispositivos e gateways de segurança para obter acesso remoto controlado

Operações de segurança altamente especializadas

Conhecimento+Tecnologia+Expertise

Inteligência contra ameaças SOC industrial

- Use inteligência contra ameaças em tempo real contra malware, phishing, vulnerabilidades e exploits

Consultoria em SOC

- Envolva especialistas para aprimorar sua capacidade de SOC para tratar ameaças sofisticadas.

Resposta e detecção em ambientes de convergência IT/OT

- Integre a segurança de TI e OT para uma detecção e resposta a ameaças unificadas

Proteção gerenciada

- Use serviços de resposta e detecção gerenciadas para o monitoramento contínuo e o tratamento especializado de incidentes

Tolerância a falhas e prontidão

Tecnologia

Treinamento de especialistas

- Forneça treinamento de cibersegurança especializado para o pessoal, capacitando-os a tratar e combater falhas eficazmente

Treinamento de conscientização

- Realize sessões de treinamento periódicos para aumentar a tolerância geral a falhas e a prontidão dos funcionários

Análise de desempenho de ativos

- Utilize ferramentas e metodologias para analisar o desempenho de ativos garantindo a confiabilidade e identificar as falhas potenciais

Saiba mais sobre a abordagem completa da Kaspersky para a cibersegurança em todos os níveis

Registro comprovado de sucesso da Kaspersky com empresas do setor de energia

Mais de 10
anos
de experiência ativa no setor

Mais de 80
projetos
concluídos no setor de energia nuclear, termal, hidráulica e outras áreas, incluindo de energia renovável

Mais de 40
Empresas de energia e serviços públicos
já protegidas pela Kaspesky

Mais de 60,000
licenças
Emitidos a clientes

O Kaspersky OT CyberSecurity fornece uma proteção completa para infraestruturas industriais de empresas do setor energético em todos os níveis

Por que empresas de energia e serviços públicos preferem a Kaspersky

Apoia o cumprimento de conformidade e compatibilidade

- Soluções testadas para garantir a compatibilidade com os produtos líderes de mercado
- Fornece medidas de cibersegurança robustas que estão em conformidade com diversas normas regulatórias

Construindo uma arquitetura escalável

- Aprimora a transparência em todo o ICS, considerando a necessidades específicas de empresas de energia elétrica
- Apoia sistemas antigos e modernos, garantindo que todos os componentes do ICS sejam protegidos

Integra-se a um ecossistema robusto

- Solução de fornecedor único que oferece proteção completa através de um ecossistema unificado
- Integra setores industriais e corporativos em uma infraestrutura protegida e unificada com uma segurança de ponta a ponta

Case studies de sucesso no setor de energia elétrica e serviços públicos

Somente na última década, a Kaspersky:

Forneceu soluções de cibersegurança para **a quarta maior empresa provedora de energia** entre os 5 maiores complexos hidrelétricos por capacidade instalada

Implementou soluções de proteção no maior fornecedor nacional de energia elétrica, responsável pela geração de **17% do volume energético do país**

Executou projetos de proteção de infraestrutura industrial para **um das 5 maiores fornecedores de energia renovável** com mais de 600 unidades de geração de energia

EMC

Maior operador de energia da Sérbia

Optou pelas soluções da Kaspersky após uma avaliação minuciosa das ofertas da concorrência. Fatores decisivos para seleção incluíram a presença de parceiro local e a compatibilidade total com a infraestrutura atual de TI.

Implementou o KICS for Nodes e o KICS for Networks, planejando a implementação da nossa plataforma KUMA SIEM.

€500 milhões
volume de negócios

34
sub-estações planejadas para a implementação do KICS

Saiba mais

PacificLight

Gerador e revendedor de energia elétrica

Avaliação de vulnerabilidade de redes industriais para identificar pontos fracos e áreas vulneráveis para uma segurança aprimorada.

Vetores de ataque simulados específicos do setor para revelar vulnerabilidades, atividades e anomalias maliciosas.

1 milhão
residências atendidas

10%
da geração de energia total de Singapura

Saiba mais

Grid Company

Grande empresa de transmissão de energia

Mais de 150 servidores e estações de trabalho no loop de processo do Grupo Empresarial da Rede são protegidos pelo KICS for Nodes, enquanto 10 servidores KICS for Networks monitoram segmentos estratégicos da rede industrial.

19239 MVA
Capacidade instalada

388
Sub-estações

Saiba mais

ROSATOM

A maior usina nuclear da Rússia por capacidade instalada

Implementou o Kaspersky Industrial CyberSecurity para proteger a infraestrutura de todos os níveis, dos servidores SCADA e estações de trabalho de operador a controladores lógicos programáveis (PLCs) e equipamentos de rede.

4337 MW
saída

7 milhões
consumidores

Solicitação Estudo de caso

www.kaspersky.com.br

© 2025 AO Kaspersky Lab.
As marcas registradas e de serviço pertencem aos seus respectivos proprietários.

Gerencie sua segurança com a Kaspersky e torne-se um parceiro

Fale conosco e participe da nossa conferência global para clientes

Saiba mais

#kaspersky
#bringonthefuture