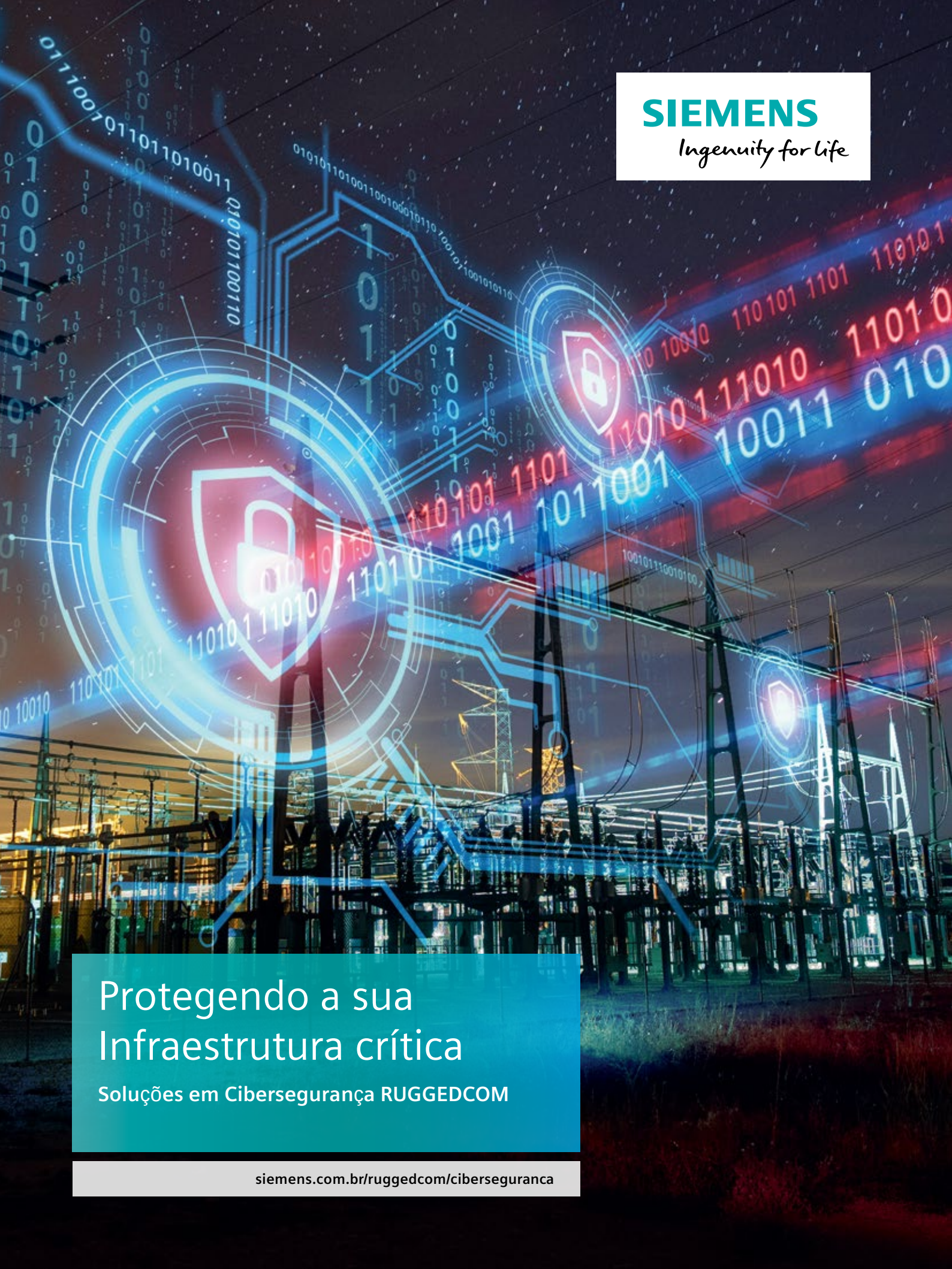


SIEMENS

Ingenuity for life

Protegendo a sua Infraestrutura crítica

Soluções em Cibersegurança RUGGEDCOM

siemens.com.br/ruggedcom/ciberseguranca

Cibersegurança de dentro para fora

A cada minuto que a sua planta fica parada, são gerados custos devido a:

- Interrupções críticas na infraestrutura de rede enquanto os técnicos resolvem os problemas de comunicação
- Brechas de seguranças que podem causar impactos devastadores
- Alto custo de reparos em equipamentos e sistemas
- Necessidade de técnicos especializados para reconfiguração de redes
- Espionagem industrial ou roubo de propriedade intelectual, afetando a integridade das operações

Crítico para o seu sucesso

Mais do que apenas um porto seguro, a segurança cibernética deve ser uma abordagem holística para proteger todos os seus sistemas contra ataques e/ou acessos não autorizados. Com bilhões de dispositivos conectados na Internet das Coisas (IoT) em todo o mundo, a cibersegurança é crucial para o sucesso da economia digital.

Ataques e ameaças cibernéticas aumentaram e se tornaram mais sofisticados com a convergência da Tecnologia da Informação (TI) e Tecnologia Operacional (TO).

A automação e a operação orientadas a dados exigem um forte sistema de segurança cibernética para proteger seus ativos, equipamentos e propriedade intelectual, reduzindo o tempo de inatividade da sua planta industrial.

Defense in Depth

Os benefícios das operações interconectadas também trazem ameaças potenciais de hackers, que podem causar paradas não planejadas. Ameaças de malware, ataques externos ou pontos de vulnerabilidade em uma rede podem paralisar as operações.

Órgãos regulatórios geralmente exigem a divulgação de relatórios de violação de segurança para garantir que as partes interessadas fiquem cientes quando informações pessoais e confidenciais do setor forem comprometidas.

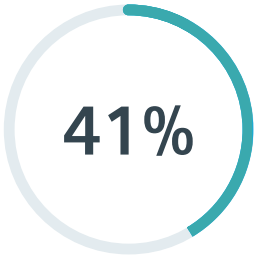
Conheça o Defense in Depth, uma abordagem para operações digitalizadas baseado no padrão IEC 62443 que leva em consideração as oportunidades de invasão e um design exclusivo de rede para uma solução unificada que protege contra ameças atuais e futuras.

dizem estar confiantes com suas habilidades em manter a segurança de dispositivos e sistemas IIoT

Fonte: Pesquisa de segurança de IoT industrial SANS 2018: Shaping IIoT Security Concerns, julho de 2018

é a estimativa atual que o cibercrime custou ao mundo no ano passado, ou 0,8% do PIB global.

Fonte: McAfee, Economic Impact of Cybercrime - No Slow Down, fevereiro de 2018



dos Sistemas de Controle Industrial (ICS) foram atacados ao menos uma vez no primeiro semestre de 2018, contra 36,6% em 2017

Fonte: Kaspersky Lab, cenário de ameaças para sistemas de automação industrial, Setembro de 2018

O líder global em cibersegurança

Como membro fundador da "Charter of Trust", a Siemens é líder no desenvolvimento da segurança cibernética global. Assinado em Munique com parceiros em todo o mundo, a Carta exige regras e padrões para construir confiança na segurança cibernética e avançar na digitalização..

Com um portfólio completo de produtos, sistemas e serviços de última geração que protegem os dados e equipamentos dos clientes, a Siemens é um parceiro confiável e preferido para empresas que buscam os mais altos padrões de segurança cibernética.

Por meio de um know-how único e multifacetado com as soluções de tecnologia para a cibersegurança, a Siemens é o lar de especialistas em redes industriais com mais de uma década de experiência em avaliação e projetos de redes OT.

Avaliação

A avaliação da rede é a primeira etapa e a chave para uma implantação bem-sucedida de soluções de segurança cibernética.

Nesta fase, os especialistas da Siemens analisam o número de ativos que o cliente tem. Esta avaliação também fornece insights sobre as vulnerabilidades de segurança da rede do cliente.

Implementação

Depois de trabalhar para entender as necessidades e riscos de segurança, a Siemens implementa um novo método, muito mais do que apenas um sistema de segurança.

Antes de adotar um novo sistema, a Siemens auxilia na concepção e implantação de um solução de segurança para garantir uma boa transição. Isso inclui serviços de pré-configuração e teste, bem como treinamento para que a equipe possa começar a trabalhar e desempenhar sua parte nas operações seguras.

Gestão

Gerenciar a segurança de uma rede significa estar prevenido: monitorar ameaças, manter as soluções de segurança atualizadas e garantir tempos de reação rápidos para identificar falhas.

Manter a rede segura não invalida a implementação de soluções de cibersegurança. Nesta fase, o cliente gerencia a solução de segurança cibernética implementada, mantendo o software e suas assinaturas atualizadas.

RUGGEDCOM
Soluções em segurança cibernética

Soluções de segurança cibernética na plataforma de hardware RUGGEDCOM detectam ataques em potencial, reduzem os custos e garantem a conformidade em um ambiente de regulamentações cada vez maior.

A Siemens oferece soluções de segurança cibernética embarcadas na família de produtos RUGGEDCOM - Multi-Service Platform, de switches e roteadores, em camada 2 e 3, projetados para ambientes de substação de energia. Pode ser combinado com serviços de consultoria de rede, suporte no local, avaliações de segurança, integração, implantação e treinamento.

A Siemens colaborou com as principais mentes em segurança cibernética industrial para trazer soluções agrupadas com aplicativos certificados de parceiros oficiais.

Os aplicativos de terceiros das principais empresas de segurança cibernética disponíveis em dispositivos RUGGEDCOM oferecem mais opções para lidar com vários desafios de segurança.

Levando em consideração as preferências específicas de cada região para segurança cibernética, a Siemens ajuda a criar um ecossistema de soluções abrangentes e confiáveis para as necessidades dos clientes, de forma personalizada. Sem necessidade de manutenção programada e com disponibilidade 24 horas por dia, 7 dias por semana. Os produtos RUGGEDCOM fornecem acesso à infraestrutura crítica, tranquilidade e segurança.

Usando as soluções de segurança cibernética RUGGEDCOM, os clientes da Siemens podem estabelecer um perímetro de segurança eletrônica em torno de sua infraestrutura crítica para evitar a interrupção de aplicações por atos acidentais ou maliciosos.

Stateful Inspection Firewall

Firewall de inspeção inteligente para controlar o tráfego entre diferentes zonas em uma rede. Inclui Network Address Translation (NAT) para evitar que atividades não autorizadas ou maliciosas, iniciadas por hosts externos, cheguem à rede local (LAN) interna.

Virtual Private Networking (VPN)

Fornece links de comunicação segura em redes. Garante a confidencialidade, autenticação do remetente, integridade da mensagem e usa IPSec (Segurança IP) para criptografar e autenticação de todos os pacotes IP na camada de rede.

Criptografia forte

Utiliza algoritmos de criptografia para autorização, autenticação e privacidade. Os exemplos incluem TLS e SSH em níveis de protocolo superiores, RSA e ECC para criptografia de chave pública e 3DES e AES para criptografia de fluxo.

RUGGEDCOM Multi-Service Platform

A família de produtos Multi-Service Platform de switches e roteadores, em camada 2 e 3, desenvolvida especificamente para fornecer várias camadas de defesa eletrônica para a proteção de ativos cibernéticos críticos. A RUGGEDCOM Multi-Service Platform é o principal ponto de entrada entre a rede local (chão de fábrica ou subestação) e o mundo exterior. A plataforma combina um roteador de camada 3, um firewall e uma VPN em um dispositivo.

RUGGEDCOM Application Processing Engine (APE)

RUGGEDCOM RX1500

RUGGEDCOM RX1500

A série RX1500 da RUGGEDCOM é uma família de switches e roteadores, em camada 2 e 3, para ambiente de subestação de energia. A plataforma modular e substituível em campo do RX1500 permite que os clientes selecionem entre Wide Area Network (WAN), serial e opções de Ethernet, tornando-o adequado para serviços públicos, pisos de plantas industriais e sistemas de controle de tráfego e trilhos.

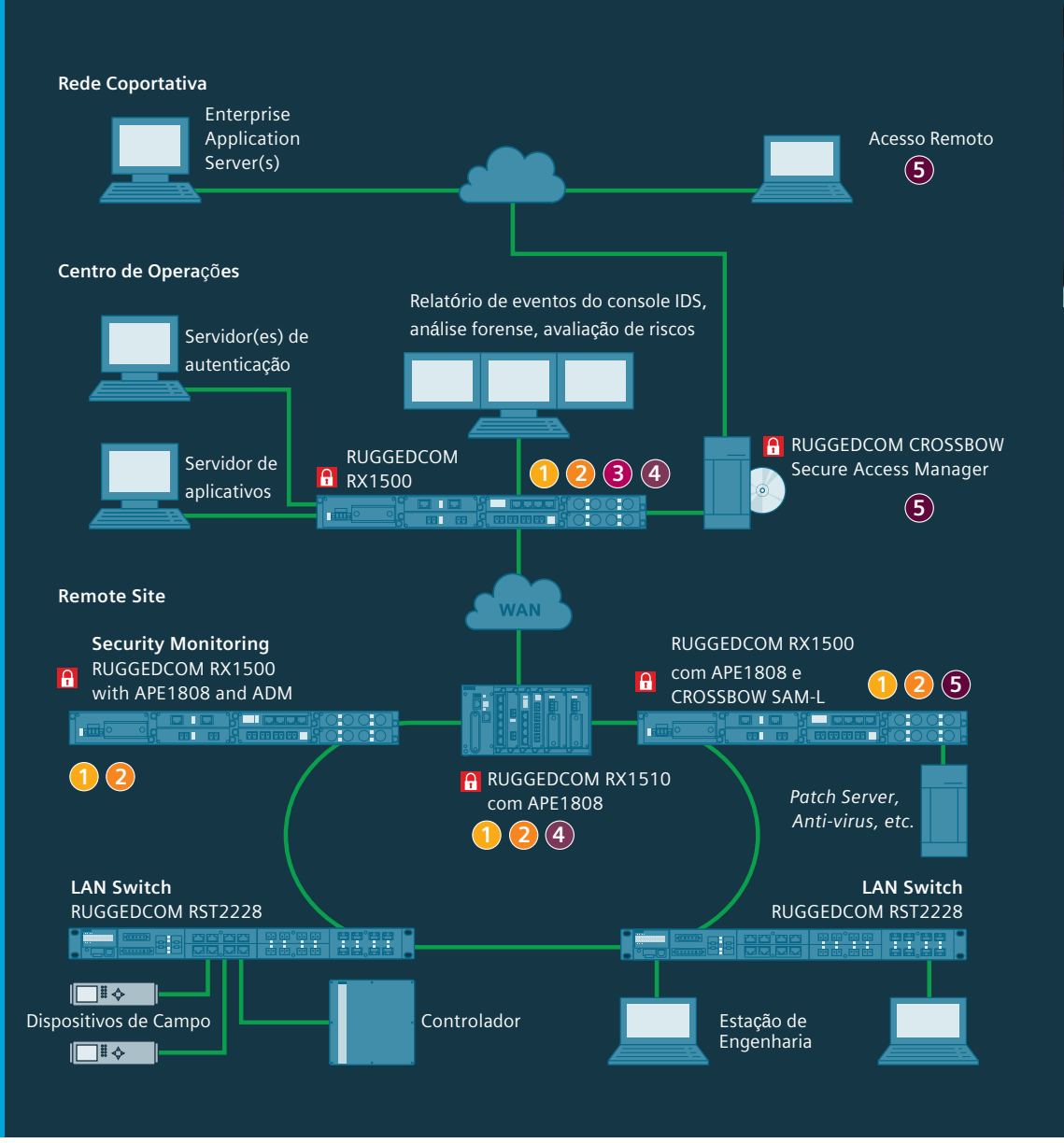
Esses dispositivos foram combinados com aplicativos de segurança cibernética para oferecer soluções personalizadas em vários níveis de segurança. Módulos substituíveis em campo garantem flexibilidade e fácil manutenção para aplicações críticas e são certificados para uso em ambientes hostis de energia elétrica, transporte e indústrias de petróleo e gás.

RUGGEDCOM Application Processing Engine (APE)

A nova versão da plataforma de hospedagem de aplicativos industriais RUGGEDCOM APE1808 é ideal para executar com segurança aplicativos de software de terceiros em ambientes hostis.

O módulo se conecta diretamente a qualquer membro da família RUGGEDCOM RX1500, exceto para o RX1512, sem a necessidade de instalar um PC industrial externo. O RUGGEDCOM APE1808 se destaca na hospedagem de uma variedade de aplicativos, como firewalls de última geração, log de rede e processadores de carga e sensores de intrusão. Baseado na arquitetura Intel quadcore e x86_64 com suporte para Linux e Windows 10, o RUGGEDCOM APE1808 fornece uma plataforma que permite integração com softwares líderes do setor na detecção e prevenção de ameaças cibernéticas.

Soluções de segurança cibernética RUGGEDCOM instaladas com o pacote Multi-Service Platform, desenvolvido para ambientes agressivos e aplicações críticas de uma planta industrial.



- Ethernet Industrial
- 1 Sistema de detecção de intrusão baseado em anomalias (IDS)
- 2 Deep Packet Inspection (DPI)
- 3 Sistema de prevenção de intrusão (IPS)
- 4 Next Generation Firewall (NGFW)
- 5 RUGGEDCOM CROSSBOW – Secure Access Control

RUGGEDCOM CROSSBOW – Secure Access Control

RUGGEDCOM CROSSBOW é uma solução de gerenciamento de acesso seguro projetada para fornecer assistência com conformidade de segurança cibernética, incluindo NERC CIP (proteção de infraestrutura crítica da North American Electric Reliability Corporation) e acesso IEC 62443-1 a Dispositivos Eletrônicos Inteligentes (IEDs). A solução CROSSBOW se concentra em fornecer ganhos de produtividade para administradores e usuários, ao mesmo tempo em que auxilia na conformidade de segurança cibernética na gestão, proteção e geração de relatórios sobre acesso remoto.

O sistema RUGGEDCOM CROSSBOW consiste em um servidor central junto com uma série de clientes que se conectam de forma segura com TLS 1.2 - em computadores desktop ou laptops. O servidor contém o banco de dados do sistema, baseado no Microsoft SQL Server, e gerencia todas as conexões dos clientes aos IEDs remotos. O servidor central oferece suporte a uma configuração de cluster de alta disponibilidade para maior confiabilidade.

Com acesso baseado em função (RBA) definido pelo administrador, CROSSBOW fornece registro de atividades e privacidade de dados conforme os usuários se conectam a dispositivos eletrônicos inteligentes (IEDs) remotos. Os operadores têm uma conexão segura garantida aos dispositivos de campo sem acessar o local ou logar em uma aplicação, permitindo-lhes acessar os dispositivos no conforto e segurança da sala de controle. A autenticação forte de dois fatores por meio de RSA SecurID, Active Directory e RADIUS garante a mais alta segurança de processo.

Além do acesso seguro, a solução RUGGEDCOM CROSSBOW fornece funcionalidade automatizada para gerenciamento de senha de dispositivo, configuração e versão de firmware monitoramento, verificação de conectividade remota e recuperação de arquivos de dados.

Sistema de detecção de intrusão baseado em anomalias

O software Intrusion Detection System (IDS) não intrusivo e baseado em anomalias para redes operacionais de missão crítica, operando em hardware RUGGEDCOM, fornece notificação de alerta precoce e alerta sobre vulnerabilidades e ameaças cibernéticas sofisticadas que podem ser indetectáveis por ferramentas de segurança de TI convencionais.

Deep Packet Inspection

Deep Packet Inspection (DPI) no RUGGEDCOM RX1500 com o APE1808 examina pacotes de dados utilizando uma metodologia não intrusiva para redes críticas com foco em protocolos OT (como Modbus e DNP3) procurando por tráfego potencial de não conformidade, vírus, spam, intrusões ou critérios definidos pelo usuário para determinar se o pacote pode passar ou se precisa ser roteado para um destino diferente para análise e mitigação de segurança cibernética, ajudando a proteger a comunicação para centros de controle e redes de TI.

Next Generation Firewall

Utilizando uma combinação de plataforma de comutação e roteamento RUGGEDCOM, com a funcionalidade de Firewalls de última geração (NGFW) em um único dispositivo integrado, fornece funcionalidades de DPI / IPS integradas adicionais, oferecendo segurança ao conectar redes de TI não críticas a redes operacionais críticas.

Sistema de prevenção de intrusão

Intrusion Prevention System (IPS) é um recurso disponível no hardware RUGGEDCOM e equipado com uma solução NGFW. O IPS está localizado entre a WAN e a LAN para negar o tráfego que representa uma ameaça conhecida com base em um perfil de segurança.

Serviços profissionais da Siemens

Da avaliação, pré-configuração até serviços de teste para implementação e treinamento, a Siemens tem tudo sob controle.

Os serviços profissionais da Siemens oferecem:

- Descoberta e análise dos ativos existentes e da arquitetura de rede
- Avaliação de vulnerabilidade da rede pelo acesso existente de segurança e fornecendo um relatório de avaliação com recomendações sobre como melhorar a segurança
- Projeto e implantação de soluções de segurança e treinamentos para toda a equipe envolvida

Publicado por
Siemens AG

Digital Industries
Process Automation
Avenida Mutinga, 3800
02675-031 São Paulo, Brasil

Artigo.: DIPA-B10050-00-7600
Dispo 06366
WS 08192.0
Traduzido no Brasil

siemens.com.br/ruggedcom/ciberseguranca

Informação de Segurança

Siemens fornece produtos e soluções com segurança industrial funções que suportam a operação segura de plantas, sistemas, máquinas e redes.
Para proteger plantas, sistemas, máquinas e redes contra ameaças cibernéticas, é necessário implementar e manter continuamente um conceito de segurança industrial de última geração holístico. Siemens ' produtos e soluções constituem apenas um elemento de tal conceito. O cliente é responsável por impedir o acesso não autorizado a suas fábricas, sistemas, máquinas e redes. Sistemas, máquinas e componentes só devem ser conectados à rede corporativa ou à Internet se e na medida necessária e com medidas de segurança adequadas (por exemplo, uso de firewalls e segmentação de rede) no local. Além disso, a orientação da Siemens sobre medidas de segurança adequadas deve ser levada em consideração. Para obter mais informações sobre segurança industrial, visite

siemens.com/industrialsecurity

Os produtos e soluções da Siemens passam por desenvolvimento contínuo para torná-los mais seguros. A Siemens recomenda fortemente aplique as atualizações do produto assim que disponíveis e sempre use versões mais recentes do produto. O uso de versões de produto que não são mais suportadas e a não aplicação das atualizações mais recentes podem aumentar a exposição do cliente a ameaças cibernéticas. Para se manter informado sobre as atualizações do produto, assine o Siemens Feed RSS de Segurança Industrial em

siemens.com/industrialsecurity