NOZOMI NETWORKS

E-BOOK

Resolvendo a questão da segurança cibernética para sistemas de gerenciamento de edifícios

Edifícios inteligentes:

Mitigando os riscos e os custos cibernéticos

Os proprietários de edifícios inteligentes estão adicionando sistemas e sensores de IoT aos seus sistemas de gerenciamento de edifícios que se tornam mais antigos à medida que procuram formas de reduzir os custos operacionais e o consumo de energia.

No entanto, os dispositivos de IoT conectados aumentam a superfície de ataque cibernético—no momento em que os edifícios inteligentes são um alvo sedutor para os invasores. Eles oferecem diversas oportunidades para violações em razão de uma série de sistemas implementados, falta de uma segurança inerente e baixo foco no gerenciamento dos ataques cibernéticos. Os sistemas expostos incluem muitos que não são cobertos pela TI como, por exemplo, HVAC, elevador, IoT, iluminação e estacionamento.

Como enfrentar essa exposição e manter a continuidade das operações vitais ao mesmo tempo em que se mantém os moradores seguros e confortáveis? Para garantir a resiliência cibernética e operacional, você precisa ter visibilidade e segurança cibernética para todos os seus dispositivos e sistemas de gerenciamento de edifícios da IoT — usando uma solução e um fornecedor com profundo conhecimento em edifícios.

O desafio:
Reduzir o risco cibernético e manter a resiliência operacional

Os edifícios inteligentes têm uma série de sistemas como, por exemplo, energia, controle de acesso, CCTV, gerenciamento de energia, HVAC e controle de iluminação. Adicionar sensores de IoT a essa combinação torna os edifícios mais vulneráveis a ameaças e rupturas cibernéticas. Tendo em vista que a segurança cibernética, de modo geral, não tem um proprietário, as empresas precisam de uma solução que reduz o risco e melhora a resiliência—de forma eficiente e em escala.

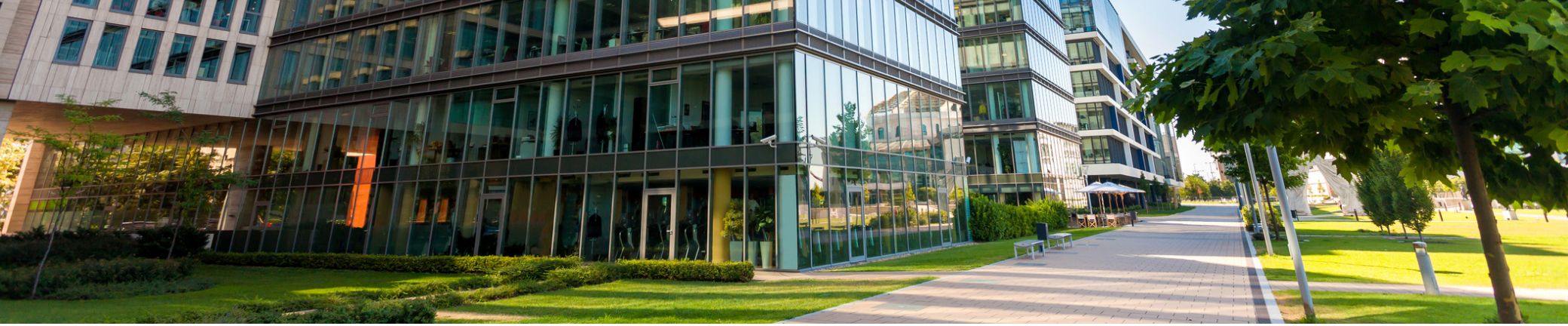
Os edifícios inteligentes enfrentam três principais desafios de segurança:

Falta de visibilidade

Aumento no risco cibernético

Limitação dos recursos de segurança cibernética

> Há uma área da segurança cibernética que os departamento e as empresas de TI não puderam dominar: a vulnerabilidade, a fragmentação e a inconsistência dos sistemas de edifícios e contratados.
>
> ***Edifícios inteligentes***



Falta de visibilidade

Aumento no risco cibernético

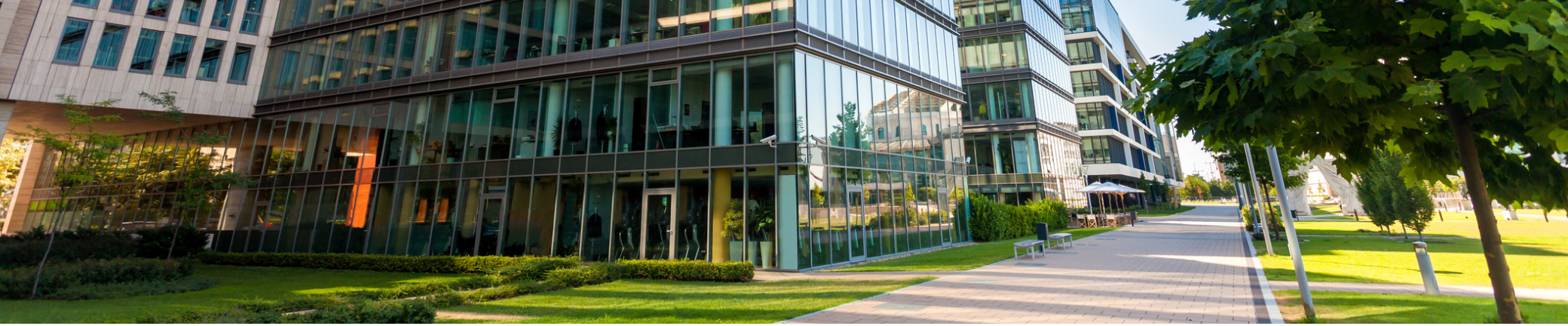
Limitação dos recursos de segurança cibernética

Proteger os edifícios inteligentes contra ameaças cibernéticas é difícil em razão de um número significativo de **pontos cegos** e **lacunas de segurança** nos sistemas de TO e IoT.

Os riscos cibernéticos crescem à medida que você agrega dispositivos de IoT e TO à sua infraestrutura. Mas você não pode proteger o que não consegue ver. Os especialistas em TI e os gerentes de instalações precisam da visibilidade completa de todos os dispositivos e sistemas de todos os fornecedores para ter uma melhor segurança cibernética. A visibilidade possibilita a detecção precisa das vulnerabilidades e anomalias para que você possa mitigar os riscos cibernéticos e minimizar as rupturas.

À medida que os ataques aos edifícios inteligentes tornam-se mais frequentes, os vetores de ameaça penetram por meio da TO do edifício e dos dispositivos de IoT como, por exemplo, acesso ao edifício, câmeras, elevadores, HVAC e iluminação. Devido a uma grande variedade, é difícil obter uma visão holística de todos os sistemas e uma avaliação priorizada dos riscos.

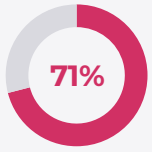
Os gerentes das instalações e os gerentes de TI precisam de uma visão automatizada e consolidada de todos os seus ativos, redes e sistemas para avaliar, de modo adequado, o risco e tomar ações eficientes para manter a resiliência operacional.



Falta de visibilidade

Aumento no risco cibernético

Limitação dos recursos de segurança cibernética



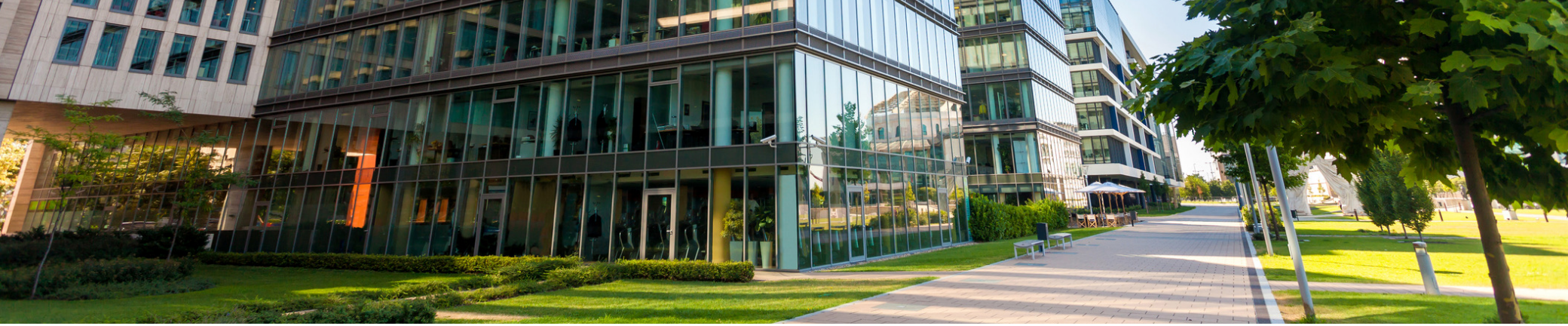
dos gerentes das instalações consideram a segurança cibernética **uma “preocupação” ou uma “inquietação.”***

*Fonte: Honeywell, "Protegendo a tecnologia operacional nas instalações contra ameaças cibernéticas", 2021

Os ataques cibernéticos estão aumentando e são intensificados pelas tensões geopolíticas no mundo todo. Um ataque a um edifício ameaça não apenas a segurança e o conforto dos moradores, mas também a reputação da marca e a situação financeira dos proprietários e gerentes do edifício.

No entanto, proteger os edifícios inteligentes não é tão simples quanto parece. As soluções de segurança cibernética de TI não são adequadas para cobrir os dispositivos de IoT e TO, e os diversos fornecedores que gerenciam sistemas de gerenciamento de edifícios têm, de modo geral, conhecimento e foco limitados em segurança cibernética.

O aumento na sofisticação dos ataques cibernéticos torna a identificação e priorização das vulnerabilidades algo crítico para os dispositivos existentes e novos. Os departamentos de TI precisam de um monitoramento abrangente e de informações de risco atualizadas constantemente e em escala para proteger os edifícios inteligentes.



Falta de visibilidade

Sistemas fragmentados

Limitação dos recursos de segurança cibernética

Os sistemas herdados não foram criados para resistir **às ameaças cibernéticas sofisticadas de hoje em dia.**

A segurança cibernética dos sistemas de gerenciamento de edifícios sofre, de modo geral, com a falta de um responsável claro e provimento inadequado de recursos.

Os programas de segurança cibernética executados pelos departamentos de TI, de modo geral, não abrangem riscos provenientes dos sistemas de TO e IoT da automação de edifícios.

Os gerentes das instalações também têm um foco limitado no risco da segurança cibernética e não priorizam a busca por uma solução. Eles são motivados pela necessidade de manter as instalações em operação e os moradores dos edifícios confortáveis e em segurança.

A falta de ferramentas compartilhadas de monitoramento dificulta o trabalho dos departamentos de TI e dos gerentes das instalações de detectar o risco cibernético e mitigá-lo de forma eficiente.

Quando se trata de proteger edifícios inteligentes, o alinhamento limitado entre silos e a falta de recursos e conhecimento especializado constituem um obstáculo significativo.

A oportunidade:
Antecipar, diagnosticar, responder

Os edifícios inteligentes têm uma ampla superfície de ataque e são cada vez mais o alvo de malfeitores sofisticados. Os sistemas diversos e as redes em várias instalações exigem monitoramento unificado. As empresas precisam de soluções que possam ser dimensionadas facilmente para controlar os custos e acompanhar o ritmo da inovação.

A única forma de aumentar a conscientização sobre a questão e corrigir os problemas antes de gerarem uma ruptura é através de visibilidade e segurança precisas e profundas de TI, TO e IoT.

Para ficar à frente das ameaças de ataque e garantir a resiliência operacional, você deve:

Antecipar

vulnerabilidades de segurança e requisitos de manutenção pra otimizar os processos operacionais

Diagnosticar

as ameaças de segurança emergentes e processar os problemas com análise baseada em IA para reduzir o risco do negócio

Responder

às prioridades mais altas com insights práticos e esforços de remediação orientados para obter a eficiência máxima

Antecipar

Diagnosticar

Responder

Visibilidade abrangente e em tempo real, alerta antecipado de ameaças cibernéticas e avarias de equipamento

A antecipação de problemas começa com a visibilidade. Você sabe quais e quantos dispositivos existem, de fato, na sua rede? Quais, de fato, apresentam comunicação ativa? Como tomar medidas antes de um ataque cibernético causar dano?

Para identificar e resolver problemas de incidentes cibernéticos ou de rede que ameaçam a confiabilidade, você precisa ter visibilidade em tempo real dos seus ativos, conexões, comunicações, bem como alerta antecipado do risco.

Ao automatizar o inventário do gerenciamento de edifícios, você elimina os pontos cegos e revela ativos que podem ter sido ignorados anteriormente. Você economiza tempo e dinheiro, usando uma solução que sempre cria um inventário atualizado em vez de depender de instantâneos de dados.

É necessário ter um fornecedor que forneça um panorama geral do seu ecossistema de TO, IoT e TI e alerte você das vulnerabilidades de segurança e requisitos de manutenção para que possa estar sempre à frente de qualquer ruptura.

"Bom produto para detectar anomalias e fornecer visibilidade
Este produto me fornece maior visibilidade ao meu ambiente de TO. Muito bom e fácil de usar. O suporte também é bom, rápido e eficiente. A interface para gerenciar o dispositivo é muito fácil e fornece muitas informações."

~ Avaliações dos clientes

Antecipar

Diagnosticar

Responder

Detecção avançada de ameaças e anomalias

A crescente sofisticação dos invasores de ameaças cibernéticas está aumentando a dificuldade para os gerentes das instalações e especialistas de TI encarregados de proteger os edifícios inteligentes.

Em que medida a sua análise de segurança é precisa? Ao avaliar o risco, você leva em consideração os dados operacionais de todos os seus sistemas e subsistemas?

A eficiência dos recursos é fundamental ao coletar e analisar as informações provenientes de todo o gerenciamento complexo das suas instalações e dos ambientes de IoT.

Os edifícios inteligentes precisam de informações de risco atualizadas que forneçam confiança no estado da sua segurança e resiliência das suas operações.

Além disso, para analisar possíveis alterações de rede problemáticas ao longo do tempo ou para dar uma resposta rápida a incidentes, são necessárias uma análise de linha de tempo forense forte e ferramentas de consulta.

"Ela fornece ótima segurança para a nossa rede.
A Nozomi é uma ótima avaliadora de rede. Ela protege a nossa rede contra qualquer ameaça. Ela mostra todos os dispositivos vulneráveis em tempo real. Não há alarmes falsos. Principais motivos para a compra: gerenciamento de custos, melhora na agilidade e nos resultados dos processos do negócio."

~ Avaliações dos clientes

Antecipar

Diagnosticar

Responder

Guias de procedimentos que economizam tempo

Ainda que seja muito importante, a percepção situacional não é suficiente. Você precisa saber como tratar os alertas que sinalizam um risco cibernético ou comportamento anormal.

Um sistema que resume e prioriza riscos, com inteligência prática e guias de procedimentos para remediação, ajuda você a tornar as suas instalações mais seguras de forma eficiente e sistemática.

Você precisa de instruções detalhadas para cada tipo de problema que tentar resolver e informações de ameaças para priorizar a redução do risco. Com as informações e as ferramentas certas, você pode focar os seus esforços e reduzir o tempo médio de resposta (MTTR).

"Essencial para um CISO em um ambiente de TO
A Nozomi Networks é líder nessa área. Não se trata apenas de tecnologia de segurança. Trata-se de um olho bem vigilante na escuridão do mundo da Tecnologia da Operação. Para mim, como gerente de segurança, é algo essencial!!"

~ Avaliações dos clientes

Tomar ações

Os gerentes dos edifícios e os especialistas de TI que entendem esses desafios e que reconhecem que a solução certa pode ajudar a mitigar o risco estarão na frente.

Aqui temos algumas estratégias que você pode adotar agora:

Consolidar o monitoramento

Expandir a sua estratégia de segurança cibernética

Dimensionar

Aprenda mais sobre os nossos produtos

Guardian™

O que é? Sensores que analisam e visualizam os dados das redes de edifícios inteligentes.

Saiba mais

CMC™

O que é? Dispositivos que reúnem dados dos sensores Guardian para monitoramento com um único console e no local.

Saiba mais

Vantage™

O que é? SaaS que escala o monitoramento de segurança e visibilidade para diversas instalações conectadas e ambientes complexos de gerenciamento de edifícios.

Saiba mais

Eficiente em todos os sistemas de IoT e operacionais em edifícios inteligentes, incluindo iluminação, elevadores, CCTV, emergência, sistemas de incêndio, HVAC, endereços públicos e segurança.

Consolidar o monitoramento

Expandir a sua estratégia de segurança cibernética

Dimensionar

Os invasores sabem como explorar as lacunas de defesa de TI/TO. Grandes quantidades de IoT de edifícios e sistemas de gerenciamento de edifícios conectados em diversas instalações geram risco cibernético em lugares difíceis de detectar. Para reduzir o risco, é fundamental consolidar o monitoramento dos ativos de TO e IoT em uma única visualização.

Os edifícios inteligentes precisam de uma solução que forneça visibilidade abrangente e monitoramento de todos os diferentes sistemas e ativos.

A TI precisa poder ver todos esses ativos e redes e detectar rapidamente o uso e as atividades ilegítimas. Uma solução que consolida informações de todos os sistemas e subsistemas, prioriza vulnerabilidades e ameaças e dá resposta com inteligência prática é a ideal.

Leia o nosso infográfico sobre sistemas de gerenciamento de edifícios para ver como a Nozomi Networks fornece segurança cibernética inteligente para os edifícios.

Download

Consolidar
o monitoramento

Expandir a sua estratégia de segurança cibernética

Dimensionar

Os dispositivos de IoT abrem a porta para violações cibernéticas em razão de sua falta de recursos de segurança e conexão com sistemas externos. Os edifícios inteligentes podem usar ferramentas de segurança cibernética de TI,
mas se os dispositivos de IoT e TO existentes e recentemente adicionados
não forem cobertos de forma adequada, eles estarão expostos ao risco cibernético.

Os fornecedores raramente consertam ou atualizam os dispositivos de IoT e é difícil consertar os dispositivos de TO por motivos operacionais, o que faz com que as operações do edifício tenham risco.

Para limitar a exposição a ameaças cibernéticas e garantir a confiabilidade financeira, os operadores dos edifícios inteligentes precisam de uma estratégia de segurança cibernética inclusiva que abrange não apenas os sistemas de TI, mas também a infraestrutura de IoT e TO em expansão.

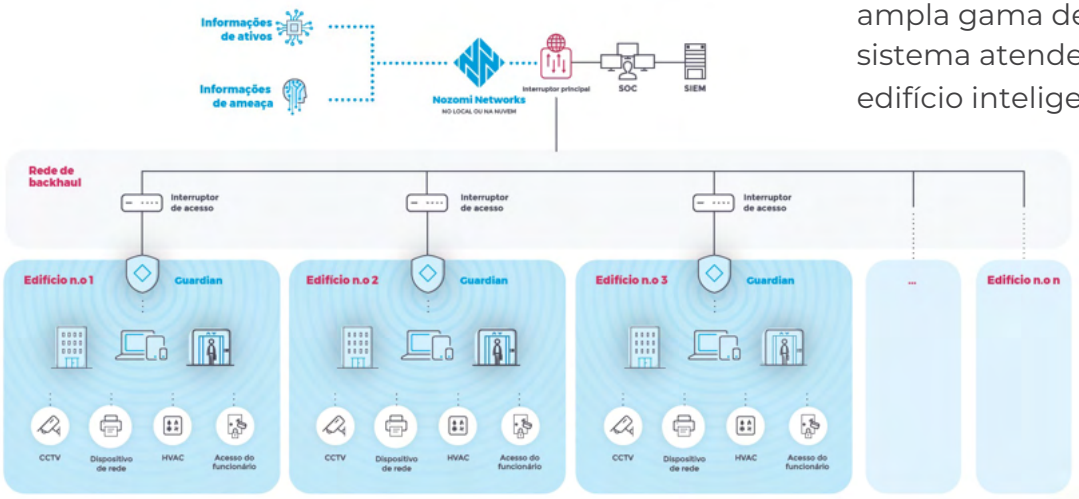
Com uma abordagem abrangente de segurança cibernética, você pode desfrutar, de modo seguro, dos benefícios da transformação digital, incluindo, por exemplo, a economia de energia. E as soluções de IoT/TO certas ajudam a preparar os seus edifícios para o futuro com informações contínuas sobre ameaças para combater o malware e a escalabilidade de amanhã a fim de administrar novas tecnologias e propriedades.

Consolidar
o monitoramento

Expandir a sua
estratégia de segurança
cibernética

Dimensionar

Edifícios dispersos e em rápido desenvolvimento
Os sistemas de IoT exigem monitoramento em escala.
É fundamental implementar uma solução que possa proteger qualquer número de ativos de TO, IoT, TI, edge e nuvem.



Você precisa de um sistema de fácil implementação e econômico que seja dimensionado de forma elegante. Um aplicativo alimentado por SaaS fornece um único painel de riscos acumulados e priorizados em todas as instalações. Ele é dimensionado rapidamente e reduz a complexidade e o custo. Aliado a uma ampla gama de sensores no local, esse sistema atende às necessidades de qualquer edifício inteligente.

Como seria
o sucesso para você?

Estudos de caso:

- Proprietário de um dos 5 principais centros comerciais
- Proprietário de um dos 5 principais hotéis

Proprietário de um dos 5 principais centros comerciais

O desafio:

O proprietário de um dos 5 principais centros comerciais globais queria:

Obter visibilidade de um ambiente com um grande número de dispositivos de IoT e TO gerenciados por diversos fornecedores

O resultado:

Ao implementar a solução da Nozomi Networks, a empresa pode:

Obter a visibilidade dos principais sistemas de gerenciamento de edifícios, incluindo aqueles controlados por fornecedores terceirizados

Reduzir o tempo de visibilidade ao automatizar o inventário de todos os ativos, incluindo dispositivos de IoT

Consolidar o monitoramento

Proprietário de um dos 5 principais hotéis

O desafio:

Proprietário dos 5 principais hotéis globais queria:

Minimizar o risco cibernético

Proteger a marca das consequências negativas de um ataque cibernético

O resultado:

Ao implementar a solução da Nozomi Networks, a empresa pode:

Determinar se algum dispositivo de IoT, TO ou TI está exposto a ameaças cibernéticas

Obter um entendimento claro dos riscos cibernéticos

Usar insights práticos para implementar mitigações e acelerar o tempo de resposta

Avaliações dos clientes Gartner Peer Insights

Gartner peerinsights™

★★★★★

CARGO: ANALISTA SÊNIOR DE SEGURANÇA CIBERNÉTICA
SETOR: OUTRO
PORTE DA EMPRESA: < US$ 500 milhões a US$ 1 bilhão

Com a Nozomi, temos uma visão aprofundada da rede de TO e profissionais extremamente qualificados

A sua adoção nos permitiu ter uma visibilidade mais ampla da rede industrial de forma mais aprofundada, o que nos deu a base para melhorar em vários aspectos. Aspectos que vão além da análise e anomalias que são o principal foco, e também nos ajudam a entender as redes herdadas.

★★★★★

CARGO: INFRAESTRUTURA E OPERAÇÕES
SETOR: SAÚDE
PORTE DA EMPRESA: Mais de US$ 30 bilhões

A Nozomi fornece soluções excelentes para monitorar as redes de TO

O trabalho em parceria com a Nozomi foi excelente. A ferramenta deles fornece a visibilidade que precisamos para proteger os nossos ambientes de TO... Fácil de implementar

★★★★★

CARGO: GERENTE CORPORATIVO DE SEGURANÇA CIBERNÉTICA
SETOR: SAÚDE
PORTE DA EMPRESA: US$ 250 milhões a US$ 500 milhões

Essencial para um CISO em ambientes de TO

A Nozomi Networks é líder nessa área. Não se trata apenas de tecnologia de segurança. Trata-se de um olho bem vigilante na escuridão do mundo da Tecnologia da Operação. Para mim, como gerente de segurança, é algo essencial!!

Mais análises dos clientes da Nozomi Networks

NOZOMI NETWORKS

Próximas etapas

Descubra como a Nozomi Networks pode ajudar você a melhorar a resiliência cibernética, visibilidade e segurança nos seus edifícios inteligentes:

Página de automação de edifícios

Solicite uma demonstração

Quer
saber mais?

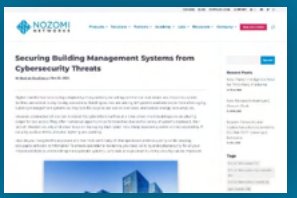
Sobre a Nozomi Networks e os edifícios inteligentes

A Nozomi Network é a sua parceira na área de segurança e visibilidade para edifícios inteligentes e sistemas de automação de edifícios. A nossa solução escalável e flexível fecha pontos cegos de TO e IoT e preenche lacunas, fornecendo visibilidade e monitoramento excepcionais dos ativos e redes. Isso resulta em detecção precisa de ameaças, riscos e anomalias, bem como na melhora da mitigação do risco corporativo e da resiliência operacional.

Recursos adicionais:

[Infográfico de soluções]

[Visibilidade do espectro total e detecção de ameaças para redes de IoT]



[Blogue: Protegendo o BMS contra ameaças de segurança]

[Protegendo a TO e IoT no BMS]

[Melhorando a segurança cibernética de IoMT]

[Melhorando a segurança cibernética do setor de varejo]

NOZOMI NETWORKS

Obrigado!

A Nozomi Networks acelera a transformação digital protegendo a infraestrutura crítica mundial e as organizações industriais e governamentais contra ameaças cibernéticas. Nossa solução proporciona visibilidade excepcional da rede e dos ativos, detecção de ameaças e informações para ambientes de TO e IoT. Os clientes confiam em nós para minimizar o risco e a complexidade e, ao mesmo tempo, maximizar a resiliência operacional.

nozominetworks.com

EBOOK-BMS-Solving-Cybersecurity-PT-A4-001