WATCHGUARD THREATSYNC®

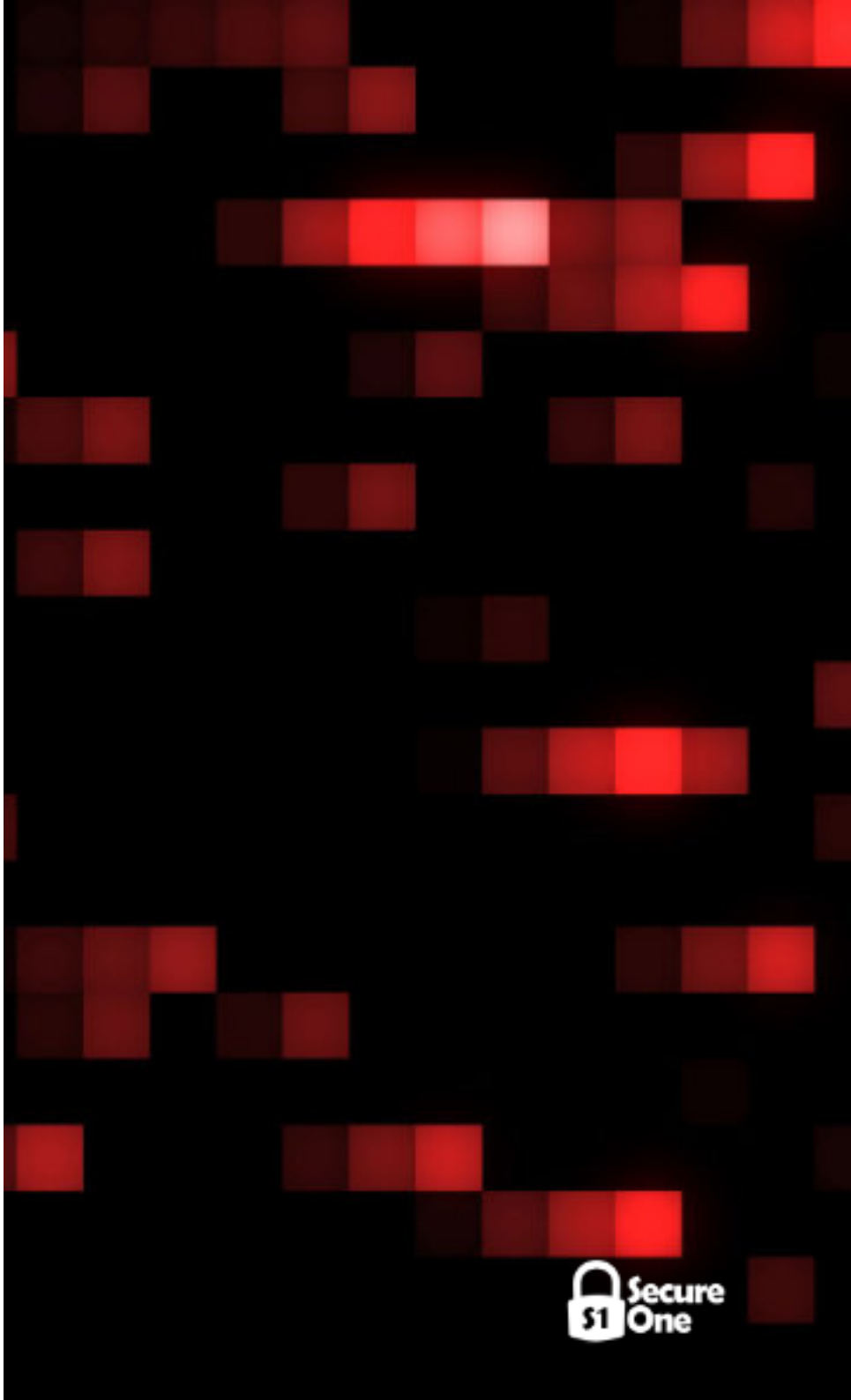
Acessando o Mundo do XDR

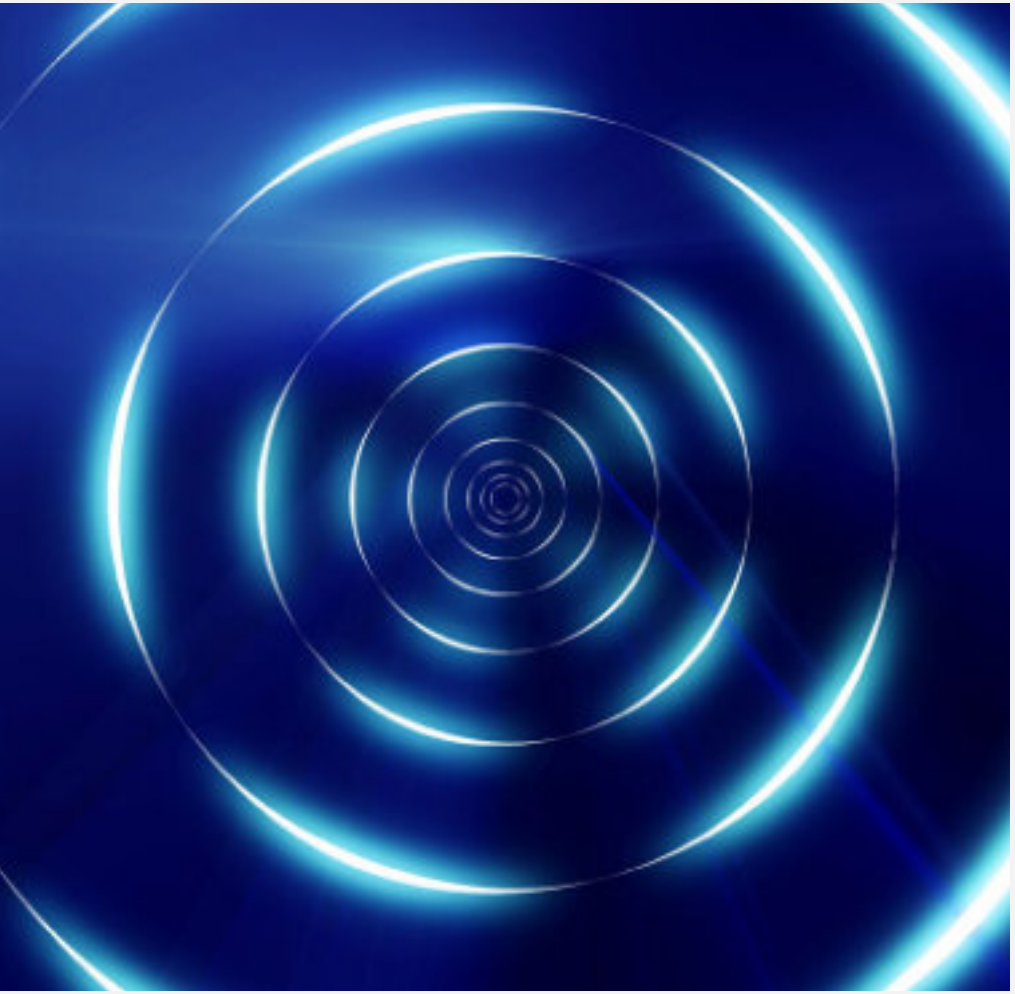
Um guia para liberar a segurança moderna

WatchGuard

SUMÁRIO

WatchGuard

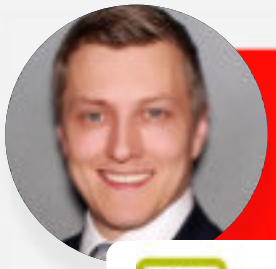




01 Principais Desafios Atuais de Cibersegurança

Organizações de todos os portes enfrentam dificuldades para acompanhar o cenário cada vez mais complexo e traiçoeiro da cibersegurança. Os agentes de ameaças não estão apenas atrás de grandes corporações, eles estão atacando agressivamente empresas de pequeno e médio porte – e seus parceiros de negócios – com ciberataques sofisticados.

As empresas não podem se dar ao luxo de ignorar a realidade e manter o status quo de segurança. Os agentes de ameaças e suas técnicas evoluem rapidamente, por isso, você deve responder na mesma medida para proteger seus ambientes, dispositivos, usuários e dados. Portanto, você deve adotar soluções de segurança que possam se adaptar e expandir no ritmo da sua empresa e da crescente superfície de ameaças de hoje.



F12.net

"A cibersegurança não é um destino, é uma jornada – simplesmente porque está sempre evoluindo."

Calvin Engen
Diretor de Tecnologia da F12.net

Quais são os Principais Desafios Atuais de Cibersegurança?

Segurança Isolada

As equipes de segurança são encarregadas de gerenciar e proteger um número cada vez maior de vetores de ameaças nas redes, endpoints e identidades corporativas. Com tantas vulnerabilidades diferentes em jogo e uma ampla gama de possíveis ciberataques para detectar e mitigar, faz sentido estabelecer uma grande variedade de soluções de segurança. No entanto, um amplo arsenal de ferramentas pode ser uma faca de dois gumes se cada solução operar independentemente do resto. Mais produtos de segurança não significam segurança mais forte.[1]

Um amplo arsenal de ferramentas pode ser uma faca de dois gumes se cada solução operar independentemente do resto.

19%

O número de ferramentas de segurança usadas pelas empresas aumentou 19% nos últimos dois anos

36%

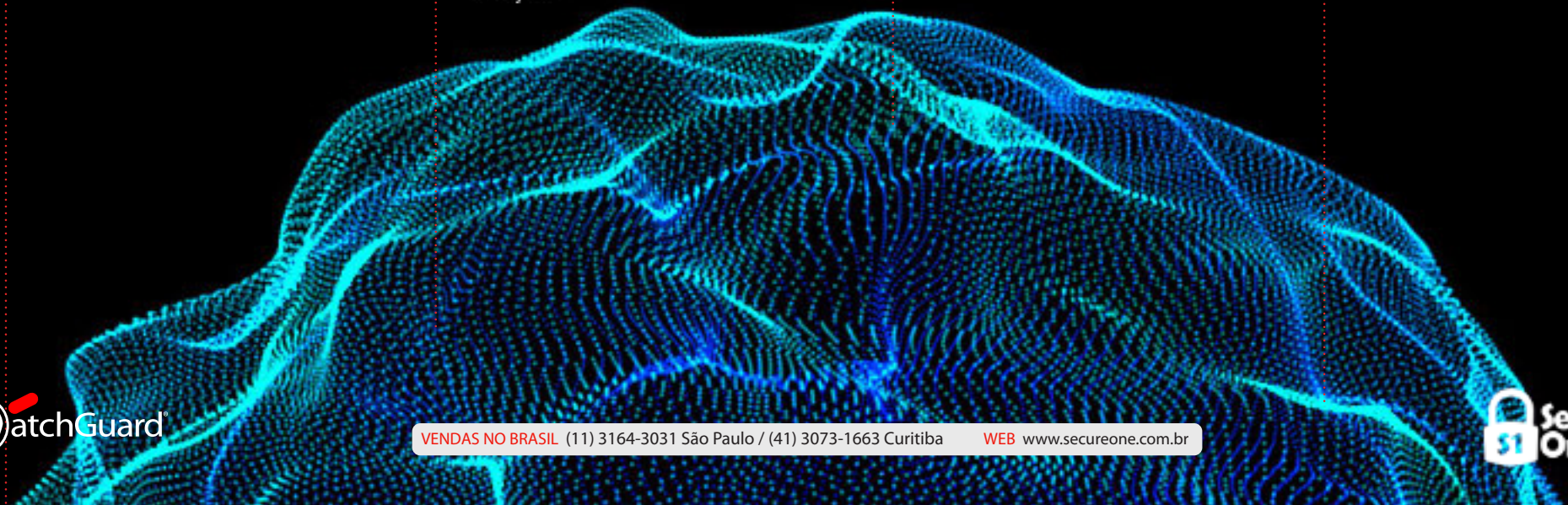
Apenas 36% das empresas dizem que estão "muito confiantes" quando se trata de garantir que os controles estejam funcionando como desejado

64 para 76

O número de ferramentas de segurança usadas pelas grandes empresas aumentou de 64 para 76 aplicativos em média

82%

Além disso, 82% dizem que foram surpreendidas por incidentes de segurança que burlaram as ferramentas existentes



Lacunas de visibilidade

Todas essas ferramentas isoladas também dificultam uma compreensão abrangente de sua postura de segurança. Cada ferramenta fornece apenas uma visão limitada de sua própria área de especialidade. Em conjunto, o resultado é um grupo de peças de quebra-cabeça que você tem de classificar manualmente e tentar juntar para formar uma imagem completa.

Pior ainda, o processo de encaixar essas peças do quebra-cabeça desperdiça um tempo que é crucial no caso de um ciberataque ativo. Se seus administradores de segurança tiverem de fazer login em vários consoles e alternar entre meia dúzia de ferramentas diferentes apenas para determinar o que pode estar acontecendo, os agentes de ameaças já terão uma vantagem considerável ao executar o ataque.

> Os administradores de segurança devem dividir esses silos de segurança para recuperar esse tempo perdido e ter a chance de acompanhar o ritmo dos rápidos ciberataques.

No entanto, a menos que essas ferramentas sejam implementadas pelo mesmo fornecedor, as soluções focadas em diferentes áreas de segurança raramente fornecerão a interoperabilidade necessária para uma proteção eficaz.

Dificuldades de correlação e dados contextuais

Todos os produtos de segurança, como soluções de rede, firewalls, segurança de endpoint ou ferramentas de identidade, têm maneiras diferentes de apresentar registros, telemetria e alertas; cada um tem um formato e uma frequência exclusivos.

Ao mesmo tempo, o vasto volume de dados de segurança coletados desses produtos pode ser difícil de entender e gerenciar manualmente, além de ser complexo de combinar e analisar. É fácil perder indicadores importantes de ameaças ou ficar preso em falsos positivos se você está mergulhado em dados gerados por vários produtos diferentes. Isso acaba levando a ameaças ignoradas que colocam toda a organização em risco.

A integração de vários produtos de segurança de diferentes fornecedores pode ser complicada e demorada, além de exigir conhecimento especializado e experiência. Gerenciar esses produtos ainda pode ser um desafio, mesmo quando integrados com sucesso, principalmente quando se lida com ambientes de TI complexos e diversificados.

Falta de automação de segurança

Seus usuários confiam em você para proteger seus dados valiosos e proteger os ativos corporativos. Sem automação, detectar e responder a incidentes de segurança pode ser lento e ineficaz, aumentando o risco de as redes, os endpoints e os usuários ficarem comprometidos, além de custos e danos à reputação decorrentes de violações de dados.

1. **Tempos de detecção lentos e estendidos**
   Sem a detecção automatizada, as equipes de segurança devem contar com processos manuais que afetam significativamente o tempo médio de detecção (MTTD), causam dificuldades para perceber ameaças, acionam falsos positivos e atrasam os tempos de resposta a incidentes. Esse atraso na detecção de ameaças de segurança pode fazer com que os administradores de segurança percam ameaças críticas e conduzam investigações desnecessárias de alertas de baixo nível, levando ao aumento de custos e deixando a porta aberta a possíveis violações.

2. **Falta de clareza sobre as ações de resposta apropriadas**
   Como os administradores de segurança sabem qual ação de resposta devem adotar primeiro? Quando você passa por um incidente de segurança, a velocidade e a precisão da resposta podem fazer toda a diferença quando se trata do impacto e do escopo do ataque. No entanto, sem recursos de resposta automatizados, pode ser difícil saber qual ação de resposta resolverá a ameaça e reduzirá o tempo médio de resposta (MTTR).

Tempo é dinheiro; tempos de detecção lentos e ações de resposta imprecisas podem facilitar aos agentes de ameaças propagar o ataque em toda a empresa e, muitas vezes, resultar em tempo de inatividade prolongado e perda de dados. A automação de segurança permite serviços de segurança consistentes e eficazes em escala.

A automação de segurança pode ajudar você a fornecer serviços de segurança consistentes e eficazes a vários clientes, além de manter um nível padrão de segurança para todos eles.

Complexidade de segurança e equipes de segurança de TI sobrecarregadas

À medida que a tecnologia avança, os ambientes de TI se tornam mais complexos, com inúmeros sistemas, aplicativos e dispositivos que exigem monitoramento e manutenção constantes para garantir a segurança. Além disso, ameaças sofisticadas continuam a emergir rapidamente, aumentando a pressão para acompanhar o ritmo.

As empresas que procuram novos níveis de agregação, correlação e análise de telemetria de segurança aumentam ainda mais as cargas de trabalho, que já são enormes, de seu pessoal de segurança. Os administradores devem lidar com uma enxurrada constante e crescente de alertas e proteger uma superfície de ataque cada vez mais diversificada, na qual as ameaças se tornaram mais complexas de detectar.

1 **Escassez de profissionais qualificados em cibersegurança**
O recrutamento e a retenção de pessoal qualificado e experiente está se tornando cada vez mais difícil devido à crescente demanda por profissionais qualificados altamente escassos no campo. À luz desse cenário, você pode enfrentar dificuldades para gerenciar uma ampla gama de soluções de segurança especializadas ao mesmo tempo que precisa se dedicar a identificar e mitigar ameaças.

2 **Sobrecarga de alertas**
Em média, a maioria das organizações lida com milhares de alertas de malware por semana, dos quais apenas 19% são considerados confiáveis e somente 4% são investigados. Além disso, algumas soluções de segurança tradicionais, longe de resolver casos de uso específicos, criam maior estresse e aumentam as cargas de trabalho, delegando a responsabilidade pelo gerenciamento de alertas e forçando você a classificar as ameaças manualmente.

O recrutamento e a retenção de pessoal qualificado e experiente está se tornando cada vez mais difícil devido à crescente demanda por profissionais qualificados altamente escassos no campo.

Um olhar mais atento às armadilhas das abordagens de segurança de produtos pontuais

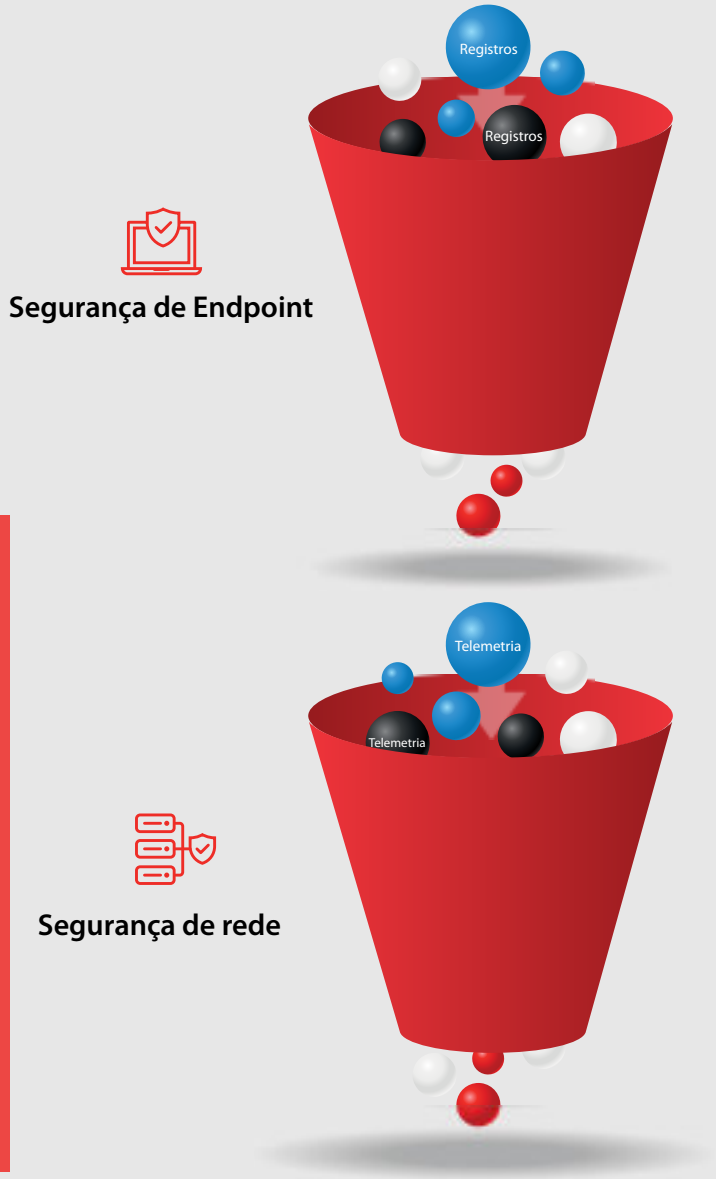
Soluções de Detecção e Resposta de Endpoints (EDR) e de segurança de rede são dois componentes cruciais de uma estratégia moderna de cibersegurança. Essas ferramentas ajudam a identificar, detectar e responder a ameaças avançadas contra domínios críticos.

Embora as soluções corretas de segurança de rede e EDR sejam altamente eficazes quando se trata de detectar e responder a ameaças sofisticadas, elas fornecem visibilidade de áreas específicas da infraestrutura de TI. As ferramentas de segurança de rede, como firewalls e sistemas de detecção de intrusão, operam em um modelo centrado no perímetro da rede e simplesmente não fornecem visibilidade suficiente dos endpoints. O foco delas é proteger os pontos de entrada e saída da rede e monitorar o tráfego na borda. No entanto, com o surgimento de um modelo de trabalho híbrido, o perímetro da rede tornou-se cada vez mais permeável, tornando mais difícil manter a segurança efetiva.

Da mesma forma, as soluções de EDR tornaram-se ferramentas essenciais na batalha para detectar e responder a ameaças de endpoint. Mas, sozinhas, elas não podem proporcionar visibilidade das ameaças que ocorrem nos ambientes de rede dos clientes.

Como resultado, muitas empresas frequentemente são obrigadas a usar uma combinação fragmentada de produtos de segurança para detectar ameaças em várias camadas. Essa abordagem fragmentada cria pontos cegos porque suas soluções de segurança operam de maneira independente uma da outra. Ela limita a visibilidade, os resultados contextuais e a eficácia da detecção e resposta, tornando quase impossível oferecer proteção abrangente e completa aos clientes.

Provavelmente, você já está bem familiarizado com esses desafios. Os administradores de segurança vêm lidando com eles há muito tempo. A verdade é que a maioria desses obstáculos é simplesmente o subproduto de abordagens desatualizadas de segurança. Superá-los requer o compromisso de alterar seu curso e embarcar em uma nova jornada de segurança.



02 XDR: Sua porta de acesso para a segurança moderna

Para superar esses desafios, você precisa de uma abordagem integrada que ofereça contexto e correlação de dados de telemetria entre várias camadas de segurança e domínios de TI.

> Com soluções de segurança mais integradas, você obterá uma visão abrangente do seu status de segurança.

Ao adotar uma abordagem integrada à cibersegurança que inclui recursos de detecção e resposta estendida (XDR) com tecnologias de automação e IA, você pode melhorar drasticamente a eficácia da segurança contra ameaças avançadas enquanto simplifica as operações de segurança.

Como o XDR funciona?

Vivemos em uma realidade onde os ciberataques são mais a regra do que a exceção, e nada pode causar mais estragos do que a materialização dessas ameaças. Com especialistas lidando com ataques persistentes e em evolução, além de vários sistemas e ferramentas para cuidar, agora é o momento certo para uma solução abrangente de detecção e resposta a ameaças que leve os MSPs a um novo mundo de oportunidades. O XDR é essa solução.

O XDR oferece grandes vantagens em relação às ferramentas de segurança desconectadas. Com o XDR, você tem o contexto e a visibilidade necessários para identificar e corrigir ciberataques com um maior grau de velocidade e eficácia. O XDR oferece uma abordagem de segurança abrangente que aproveita as tecnologias de automação e IA para detectar e responder a ameaças em firewalls, servidores, estações de trabalho e dispositivos.

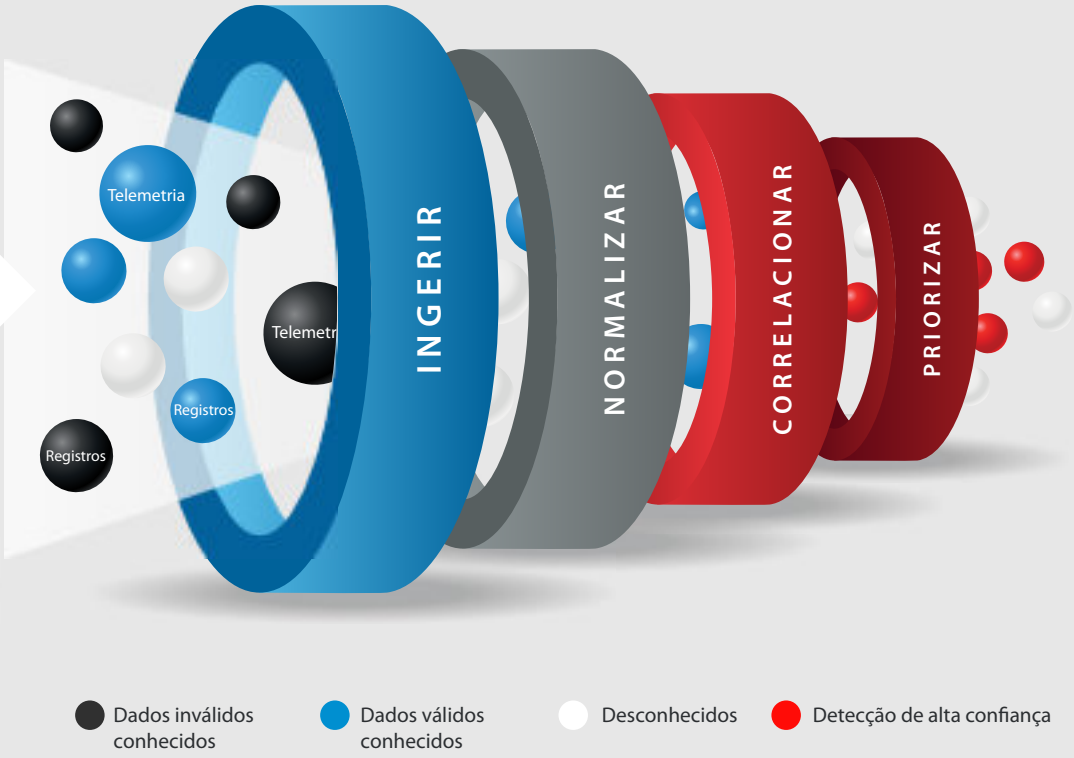
> Uma solução XDR integrada pode simplificar as operações de segurança, reduzir o atrito e os custos operacionais e ajudar você a alcançar uma postura de segurança mais forte em geral.

Segurança de Endpoint

XDR

Segurança de rede

WATCHGUARD THREATSYNC®



03 Acesse o Mundo do XDR e Libere a Segurança Unificada

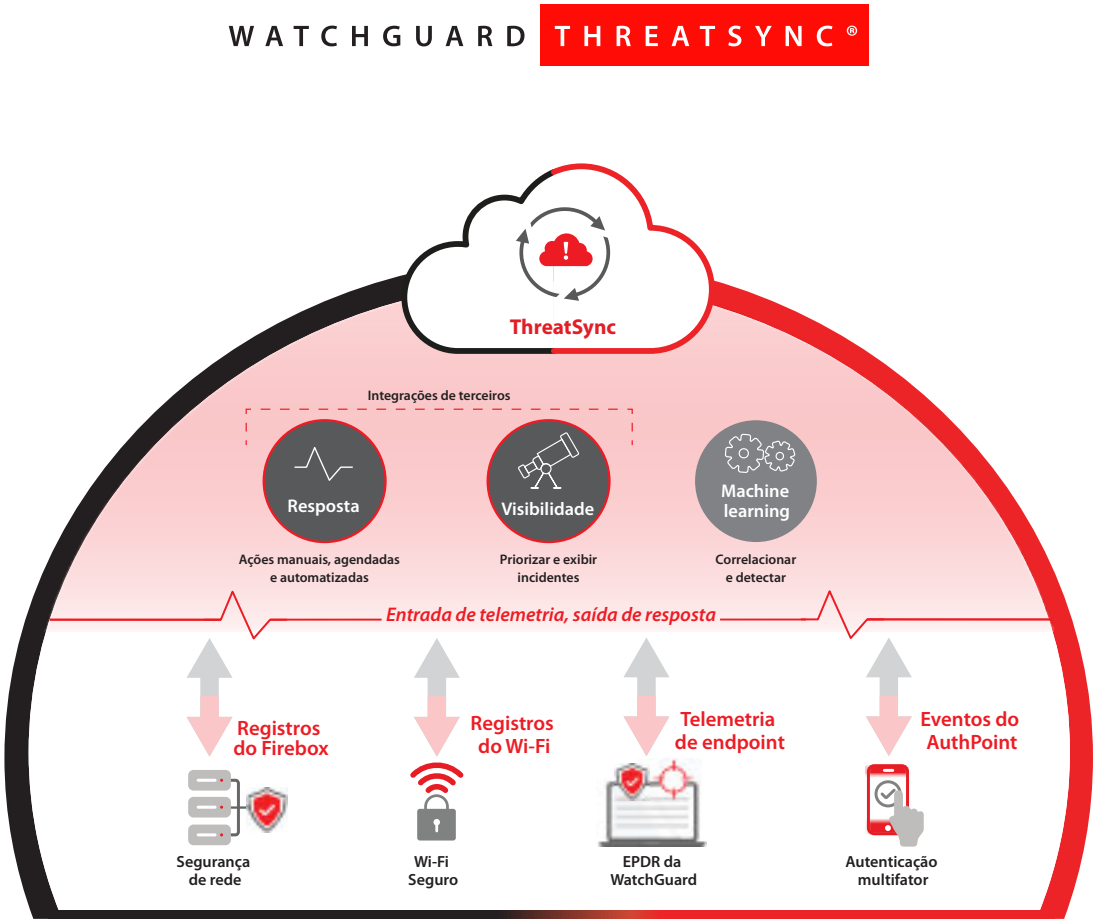
Oferecemos uma solução XDR abrangente e fácil de usar com o ThreatSync, uma camada central da arquitetura Unified Security Platform® da WatchGuard. Isso permite detecções entre produtos unificadas e correções de ameaças com mais rapidez a partir de uma só interface.

Estender, Detectar e Responder com o ThreatSync

1 Estender
Implementamos o XDR com integrações rígidas e telemetria de dados entre domínios com as tecnologias de última geração da WatchGuard. Ao ampliar a gama de feeds de dados para incluir rede, endpoint e inteligência de ameaças do usuário, ampliamos a visibilidade e a proteção.

2 Detectar
Diga adeus às abordagens de segurança isoladas que diminuem os tempos de detecção e deixam passar ataques. Com os recursos de IA e machine learning do ThreatSync, identificamos possíveis ameaças em tempo real em diferentes domínios para reduzir os prazos de detecção e a contenção rápida.

3 Responder
o XDR acelera os tempos de resposta e eleva a segurança da sua empresa. Usamos o ThreatSync para orquestrar ações de resposta automatizadas para neutralizar ameaças contra sua empresa de forma simples, rápida e precisa.



O Poderoso XDR de Maneira Simples

Detecção de Ameaças entre Plataformas

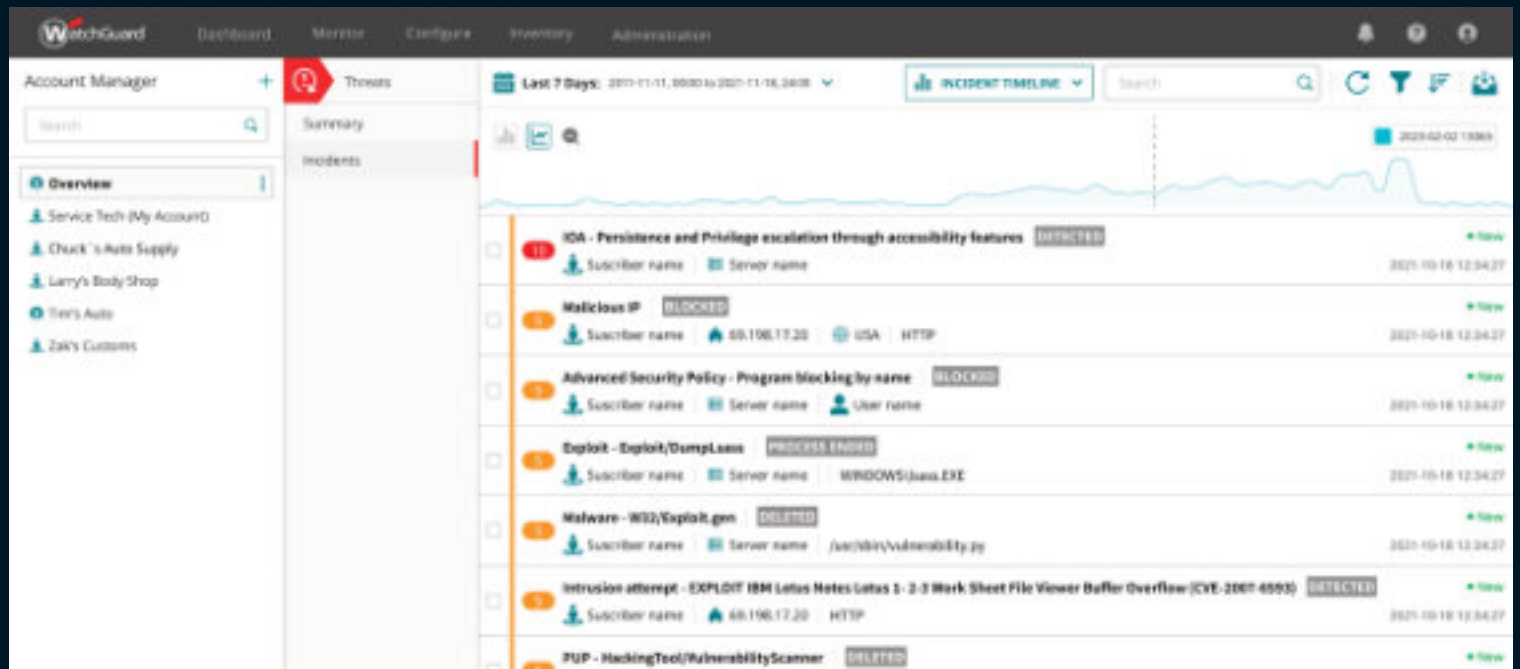
O ThreatSync fornece recursos de detecção estendidos ao consumir e correlacionar indicadores de comprometimento (IoCs) de todos os produtos de segurança da WatchGuard. Esse contexto e a correlação entre domínios permitem que a solução detecte e classifique atividades potencialmente maliciosas relacionadas a ambientes, usuários e dispositivos específicos para reduzir o MTTD, melhorar a precisão e, em última análise, permitir a correção mais rápida.

Unificada e Resposta a Ameaças

O XDR oferece uma visão holística de sua superfície de ameaças, facilitando a identificação de problemas, sua triagem e resposta com velocidade e confiança. O ThreatSync permite trabalhar de forma mais eficiente e eficaz com pontuação inteligente de alertas, políticas de correção automatizada e opções para intervenção manual, conforme necessário. Esse nível de orquestração de resposta a ameaças aprimora a escala e a precisão das equipes de segurança.

Fácil de Implantar e Administrar

Com recursos intuitivos de gerenciamento e automação baseados em nuvem, o WatchGuard ThreatSync facilita a adoção de uma abordagem XDR. Como a robusta camada de XDR na arquitetura da Plataforma de Segurança Unificada® da WatchGuard, o ThreatSync integra inteligência entre produtos para reduzir os custos e o trabalho envolvido ao administrar a implantação de soluções de vários pontos para detecção e resposta a ameaças.

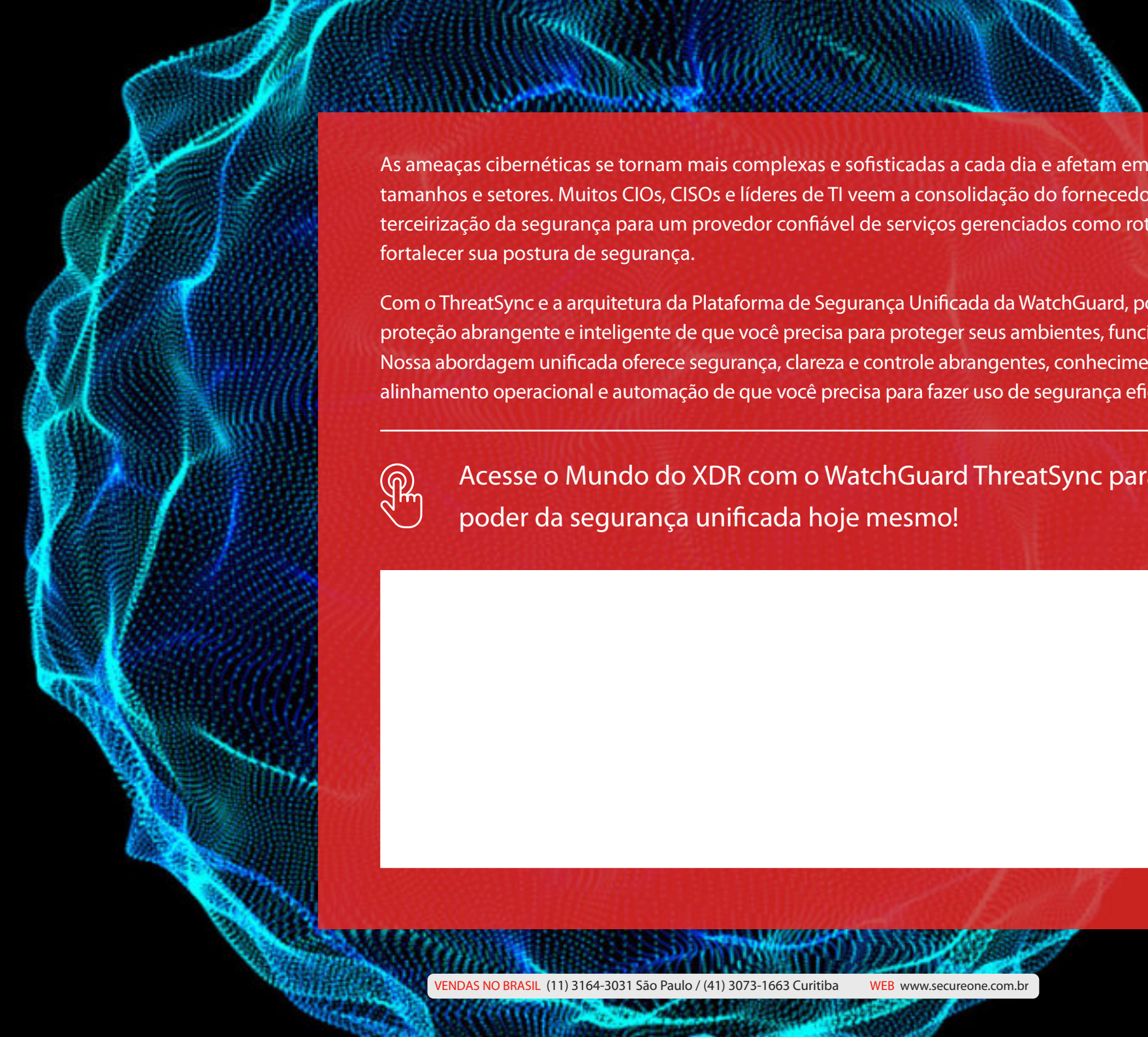


Maior visibilidade da atividade de rede e endpoint, ajudando a identificar ameaças que, de outra forma, não seriam detectadas

Segurança abrangente ao unificar dados e alertas em uma plataforma única, na qual as soluções podem trabalhar juntas para priorizar e responder às ameaças

Redução na sobrecarga da equipe de segurança por meio da automatização do processo de detecção e resposta a ameaças, bem como da liberação de tempo e recursos para outras tarefas de alto valor

Simplificação do processo de resposta fornecendo respostas coordenadas e automatizadas às ameaças detectadas



As ameaças cibernéticas se tornam mais complexas e sofisticadas a cada dia e afetam empresas de todos os tamanhos e setores. Muitos CIOs, CISOs e líderes de TI veem a consolidação do fornecedor de segurança e a terceirização da segurança para um provedor confiável de serviços gerenciados como rotas econômicas para fortalecer sua postura de segurança.

Com o ThreatSync e a arquitetura da Plataforma de Segurança Unificada da WatchGuard, podemos oferecer a proteção abrangente e inteligente de que você precisa para proteger seus ambientes, funcionários e dispositivos. Nossa abordagem unificada oferece segurança, clareza e controle abrangentes, conhecimento compartilhado, alinhamento operacional e automação de que você precisa para fazer uso de segurança eficaz em escala.

Acesse o Mundo do XDR com o WatchGuard ThreatSync para liberar o poder da segurança unificada hoje mesmo!

Portfólio da WatchGuard

Segurança de Rede

As soluções de segurança de rede da WatchGuard foram projetadas desde o início para oferecer implantação, uso e gerenciamento simplificados – com o maior nível de segurança possível. O foco da nossa abordagem exclusiva à segurança de rede é oferecer a melhor segurança da categoria, de nível corporativo, para qualquer organização, independentemente do tamanho ou do conhecimento técnico.

Wi-Fi Seguro

As soluções de Wi-Fi Seguro da WatchGuard são verdadeiras revoluções no mercado atual. Elas foram criadas para oferecer um espaço aéreo seguro e protegido para ambientes de Wi-Fi, ao mesmo tempo em que eliminam problemas administrativos e reduzem muito o custo. Com ferramentas de envolvimento expansivas e visibilidade da análise do negócio, a tecnologia oferece a vantagem competitiva necessária para que as empresas tenham sucesso.

Autenticação Multifator

O WatchGuard AuthPoint® é a solução certa para preencher a lacuna da segurança baseada em senhas por meio da autenticação multifator em uma plataforma na nuvem fácil de usar. A abordagem exclusiva da WatchGuard acrescenta o "DNA do telefone celular" como um fator de identificação para assegurar que somente a pessoa correta tenha acesso a redes confidenciais e a aplicativos em nuvem.

Segurança de Endpoint

A Segurança de Endpoint da WatchGuard é um portfólio de segurança de endpoint avançado e nativo em nuvem. Ela protege empresas de todos os tipos contra ciberataques atuais e futuros. A principal solução, o WatchGuard EPDR tem tecnologia de inteligência artificial e melhora imediatamente a postura de segurança das organizações. O produto combina recursos de Proteção de Endpoints (EPP) e Detecção e Resposta (EDR) com Serviços Zero Trust de Aplicação e Threat Hunting.

A WatchGuard® Technologies, Inc. é líder global em cibersegurança unificada. Nossa abordagem de Plataforma de Segurança Unificada® foi criada exclusivamente para que os provedores de serviços gerenciados forneçam segurança de ponta que aumenta a escala e a velocidade dos negócios, além de melhorar a eficiência operacional. Adotados em todo o mundo por mais de 17 mil parceiros de segurança e prestadores de serviços para proteger mais de 250 mil clientes, os premiados produtos e serviços da empresa incluem segurança e inteligência de rede, proteção avançada de endpoint, autenticação multifator e Wi-Fi seguro. Juntos, eles oferecem uma plataforma de segurança com cinco elementos indispensáveis: segurança abrangente, conhecimento compartilhado, clareza e controle, alinhamento operacional e automação. A WatchGuard tem sua sede em Seattle, no estado de Washington, nos EUA, e escritórios na América do Norte, Europa, Ásia-Pacífico e América Latina. Para saber mais, acesse WatchGuard.com/br.

WatchGuard®

VENDAS NO BRASIL (11) 3164-3031 São Paulo / (41) 3073-1663 Curitiba WEB www.secureone.com.br

Secure One