Segurança escalável, flexível e automatizada para implantação de IoT

Proteja dados, ativos e infraestrutura crítica com visibilidade, detecção e correção de ameaças em tempo real

Desafio

O volume e a variedade dos dispositivos de IoT tornam a segurança um desafio significativo. A maioria dos endpoints de IoT tem uma base limitada para a execução de funções de segurança, o pessoal de segurança é escasso e as vulnerabilidades de dia zero estão aumentando bastante. As soluções tradicionais de segurança baseada em perímetro não são suficientes.

Solução

A Software-Defined Secure Network da Juniper permite que você tenha toda a sua rede como uma plataforma de segurança cibernética unificada que utiliza análises, aprendizado de máquina e automação para melhorar a sua postura de segurança contra o aumento explosivo dos riscos de IoT.

Benefícios

- Visibilidade total de dispositivos de IoT, redes e aplicações
- Detecção inteligente de ameaças conhecidas ou não, com análise de comportamento e aprendizado de máquina
- Correção e controle em tempo real por meio da aplicação automatizada de políticas
- Cumprimento de requisitos de conformidade regulatória, como NERC CIP, HIPPA e GDPR
- Proteção escalável, flexível e automatizada em qualquer lugar

Em 2018, a Internet das Coisas (IoT) passará por um importante ponto de inflexão, quando muitas empresas levarem sua implantação de IoT da experimentação inicial para a escala comercial[1].

Esse é um marco crítico, marcando a entrada da IoT no circuito convencional. O Gartner prevê que, até 2020, 20,4 bilhões de coisas conectadas estarão em uso no mundo todo[2]. Da mesma forma, o IHS Markit prevê que o número de dispositivos de IoT conectados crescerá até 125 bilhões até 2030[3].

Conforme aumenta a escala de endpoints de IoT, a área de ataque aumenta também, oferecendo amplas oportunidades de ataque, com inovação dos mesmos pelos criminosos cibernéticos. Não surpreende que a segurança seja a preocupação número um das empresas que pensam em adotar a IoT.

O desafio

Nos primórdios da IoT, a segurança era algo secundário. Hoje, os usuários estão pagando o preço dessa negligência. A AT&T relatou um aumento de 3.198% no número de invasores que buscam vulnerabilidades em dispositivos de IoT nos últimos três anos[4]. Em 2016, cerca de 100.000 dispositivos de IoT foram infectados pelo malware Mirai e transformados em botnets que iniciaram ataques DDoS de 1,2 Tbps contra o provedor de serviços DNS Dyn. Esses ataques causaram uma paralisação que durou mais de duas horas e afetou grandes provedores de serviços, como Twitter, Spotify e Github.

Estima-se que, para empresas com receita anual de US$ 2 bilhões ou mais, o custo potencial de uma violação de IoT seja de mais de US$ 20 milhões[5]. Além da perda financeira, as violações de IoT também podem causar danos físicos e até mesmo ameaçar a segurança das pessoas. Em 2015, a Chrysler fez o recall de 1,4 milhão de veículos depois que hackers demonstraram que poderiam sequestrar remotamente os sistemas digitais de um Jeep. Nesse mesmo ano, um malware de IoT russo atacou a rede elétrica da Ucrânia, cortando a energia de 230.000 pessoas[6].

[1] https://go.forrester.com/blogs/predictions-2018-iot-will-move-from-experimentation-to-business-scale/
[2] https://www.gartner.com/newsroom/id/3598917
[3] https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
[4] https://www.business.att.com/cybersecurity/archives/v4/emerging-vulnerabilities/
[5] https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security
[6] https://www.forbes.com/sites/thomasbrewster/2015/07/24/chrysler-recall-exploit/

Figura 1: A Internet das Coisas

Desafios de segurança da IoT

Em comparação a dispositivos conectados tradicionais, como laptops, celulares e tablets, os dispositivos conectados da IoT têm seus próprios desafios de segurança. Por exemplo:

- Muitos dispositivos de IoT são pequenos, de baixa potência e baratos, com memória e computação limitadas demais para acomodar funções de segurança. É por isso que a própria rede é tão importante para atenuar as ameaças de IoT.
- As equipes de operações de segurança são desafiadas a acompanhar o ritmo do crescimento exponencial dos dispositivos de IoT. Assim, a automação da segurança é essencial para a implantação em ampla escala da IoT.
- A diversificação de dispositivos de IoT (tipos, sistemas operacionais, fabricantes, etc.) significa também que muitas vulnerabilidades de dia zero podem ser exploradas pelos hackers. As organizações precisam utilizar a análise de segurança e o aprendizado de máquina para detectar ameaças desconhecidas e se defender desses ataques à IoT.
- A segurança de perímetro tradicional desconfia de tudo o que está além do firewall e pressupõe que tudo o que está dentro de seus limites é seguro. Essa abordagem não considera cenários de IoT em que dispositivos internos sejam comprometidos. É preciso ter uma nova perspectiva.

A solução de segurança de IoT da Juniper Networks

A solução de segurança de IoT da Juniper inclui os seguintes componentes.

- **Os Gateways de Serviços da Série SRX da Juniper Networks e suas versões virtuais de container vSRX/cSRX:** os gateways de serviços físicos SRX e virtuais vSRX fornecem proteção de firewall de próxima geração (NGFW) com reconhecimento de aplicações integradas, prevenção de invasões e controles de usuário baseados em funções, além do melhor gerenciamento unificado de ameaças (UTM) da categoria para proteger ativos de negócios.

  Os firewalls da Série SRX e vSRX podem ser gerenciados centralmente com a aplicação de gerenciamento Junos Space® Security Director da Juniper Networks.

  O cSRX Container Firewall é executado sem que o sistema operacional sobrecarregue a plataforma de execução, requer recursos menores e é mais fácil de migrar ou baixar. Ele usa menos memória e seu tempo de ativação é medido em frações de segundos, o que proporciona maior densidade a um custo menor, algo perfeito para vários casos de uso da IoT.

  Para saber mais sobre os firewalls de nova geração da Série SRX, visite www.juniper.net/us/en/products-services/security/srx-series/.

- **Junos Space Security Director:** a aplicação de gerenciamento escalável e intuitivo Security Director da Juniper permite que os usuários empresariais tomem decisões precisas e obtenham visibilidade total de aplicações, usuários e ameaças por meio de seus firewalls SRX físicos e virtuais. Com uma visão global, um conjunto avançado de recursos de segurança e a inteligência prática e fácil de usar proporcionada pelo Juniper Sky™ Advanced Threat Prevention e pelo Juniper Sky ATP Appliance (veja abaixo), o Security Director deixa você criar políticas de segurança para tomar ações corretivas e bloquear aplicações e ameaças de alto risco. Oferecendo gerenciamento com um único painel de visualização, um assistente de criação de regras de segurança fácil de usar e um recurso de inserção de regras automáticas, o Security Director permite criar políticas de segurança menos complexas com mais mais rapidez.

  O Policy Enforcer, um componente do Security Director, é um módulo de inteligência central que se comunica com produtos de segurança e elementos de rede de vários fornecedores para consolidar informações de ameaças de várias fontes da rede, fornecer análises e aplicar políticas de segurança globalmente, desde a borda até a nuvem.

  Para saber mais sobre o Security Director, visite www.juniper.net/us/en/products-services/security/security-director.

- **Juniper Sky Advanced Threat Prevention:** um serviço baseado na nuvem, integrado com firewalls do Junos Space Security Director e firewalls da Série SRX que fornecem recursos de inspeção avançados, bloqueio inline e alertas úteis, adaptando-se constantemente a um panorama de ameaças sempre em evolução por meio de informações em tempo real obtidas na nuvem. A tecnologia de identificação do Juniper Sky ATP utiliza diversas técnicas sofisticadas para detectar e impedir ataques cibernéticos rapidamente. Elas incluem:
  - Algoritmos avançados de aprendizado de máquina
  - Análise dinâmica com técnicas para forçar o malware a se ativar e se identificar
  - Buscas rápidas no cache para acelerar a identificação prévia de malware
  - Mecanismo antivírus baseado em assinatura para identificar arquivos conhecidos

  - Análise estática de código de software para identificar possíveis fragmentos perigosos

  Para saber mais sobre o Juniper Sky ATP, visite www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/.

- **Juniper Advanced Threat Prevention Appliance:** o Juniper ATP Appliance fornece proteção local abrangente contra um sofisticado panorama de ameaças sempre em evolução.

  Com ferramentas de segurança tradicionais baseadas em assinatura, ataques de dia zero costumam passar despercebidos. Utilizando análise comportamental e aprendizado de máquina avançado, o Juniper ATP Appliance identifica ameaças avançadas existentes e desconhecidas em tempo quase real, por meio de detecção contínua em vários estágios e análise de tráfego da Web, de e-mail e de propagação lateral.

  O Juniper ATP Appliance recebe feeds de vários dispositivos de segurança, aplica análises para identificar ataques avançados e agrega os eventos em uma única linha de tempo abrangente que mostra todas as ameaças da rede. As equipes de segurança podem determinar rapidamente como o ataque ocorreu e priorizar alertas críticos.

  Para saber mais sobre o Juniper ATP Appliance, visite www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/.

- **Juniper Secure Analytics:** os Appliances da Série JSA Secure Analytics combinam, analisam e gerenciam um conjunto sem precedentes de dados de vigilância (comportamento de rede, eventos de segurança, perfis de vulnerabilidade e informações de ameaças), capacitando as empresas a automatizarem a análise de grandes conjuntos de dados e gerenciarem com eficiência as operações de negócios usando um console único. Um componente essencial da plataforma SDSN, o JSA Series Secure Analytics também está integrado ao software de gerenciamento centralizado Security Director, fornecendo inteligência em tempo real para a correção rápida de ameaças e a aplicação direta de políticas em toda a rede.

  Para saber mais sobre o portfólio da Série JSA Secure Analytics, visite www.juniper.net/us/en/products-services/security/secure-analytics/.

Recursos e benefícios

A solução de segurança de IoT da Juniper permite que você transforme a sua rede em um único domínio de aplicação amplo, utilizando análise, aprendizado de máquina e automação para visibilidade, detecção e correção de ameaças em tempo real.

- **Visibilidade total de dispositivos de IoT, redes e aplicações:** se você não pode ver, não pode se defender. É por isso que a visibilidade é tão crítica.
- **Visibilidade de dispositivos de IoT:** quando um endpoint de IoT se conecta à rede, os switches de acesso da Juniper utilizam o AAA (RADIUS/DHCP/AD/LDAP) baseado em padrões existente, além da integração com parceiros de controle de acesso à rede (NAC) e tecnologia de segurança, como ForeScout, Aruba ClearPass e Impulse Point, a fim de fornecer integração e perfis de dispositivos. Com isso, os clientes conseguem uma flexibilidade considerável na implantação, escolhendo entre com/sem fio, com/sem agente e com/sem suporte para 802.1X. Você tem visibilidade completa dos dispositivos de IoT e do tráfego de rede, e pode aplicar políticas de segurança e implementar a segmentação de rede da IoT.
- **Visibilidade da rede de IoT:** como uma das principais soluções de Security Information and Event Management (SIEM), o JSA Series Secure Analytics coleta, agrega, armazena e analisa dados de eventos de dispositivos de rede da Juniper e de terceiros continuamente, fornecendo uma imagem completa de como a infraestrutura da rede se comporta em tempo real para identificar comportamentos anormais. Conforme cresce o número de objetos da rede, e também as métricas que eles geram, o modelo pull tradicional usado por SNMP e CLI — que requer processamento adicional para realizar sondagens regularmente — limita a escalabilidade. A Junos Telemetry Interface (JTI), um recurso do sistema operacional do Junos da Juniper Networks, supera esses limites adotando um modelo push para fornecer dados assincronamente, eliminando a necessidade da sondagem. Uma estação de gerenciamento envia uma solicitação de dados uma única vez para transmitir atualizações periódicas. Como resultado, a JTI é altamente escalável e pode monitorar milhares de objetos de rede.
- **Visibilidade das aplicações de IoT:** o Juniper Networks AppSecure, um recurso essencial dos NGFWs da Série SRX, fornece um mecanismo poderoso para reconhecer novas aplicações instantaneamente, usando técnicas que identificam todas as aplicações que passam pela rede, independentemente de porta, protocolo ou método de criptografia. Oferecendo ampla visibilidade e controle das aplicações, o AppSecure fornece o contexto que vincula o uso das aplicações a um usuário, em qualquer local ou dispositivo. Projetado para entender o comportamento das aplicações e identificar vulnerabilidades, o AppSecure bloqueia as ameaças de segurança trazidas pelas aplicações antes que possam causar danos. Além disso, o Junos Space Security Director fornece uma maneira fácil e intuitiva de identificar as aplicações que usam mais largura de banda, têm o maior número de sessões ou estão sob mais riscos.
- **Detecção inteligente de ameaças conhecidas ou não, com análise de comportamento e aprendizado de máquina:** o volume elevado de dispositivos de IoT e de trocas de dados pode transformar a detecção de ameaças em um grande desafio.

  Os dispositivos SRX Series incluem um sistema de prevenção de invasões (IPS) que fornece proteção completa contra uma grande variedade de ataques de segurança conhecidos em aplicações, bancos de dados e sistemas operacionais. Os gateways de serviços da Série SRX estão sempre em busca de novos ataques de vulnerabilidades recém-descobertos, garantindo que a proteção da rede esteja atualizada em relação aos métodos de ataques mais recentes.

Para ameaças desconhecidas, como ataques de dia zero, as soluções de prevenção de ameaças avançada da Juniper (o Juniper Sky ATP baseado na nuvem e o Juniper ATP Appliance para implantações no local) fornecem detecção avançada por meio de aprendizado de máquina e análise de comportamento. Os clientes obtêm uma linha de base do comportamento normal dos dispositivos de IoT para detectar anomalias e se defender de ataques, além de impedir paralisações amplas causadas por ameaças de IoT, transformando ameaças "desconhecidas" em ataques conhecidos.

- **Correção e controle em tempo real por meio da aplicação automatizada de políticas:** se examinarmos incidentes de segurança anteriores, veremos que a maioria dos sistemas detectava o ataque e enviava alertas. Entretanto, normalmente a reação era manual e levava horas ou, em alguns casos, dias; nesse ponto, os danos já tinham ocorrido. Com a IoT em grande escala, a automação da segurança é necessária para que as equipes de operação acompanhem tal crescimento. E cenários diferentes exigem tratamentos diferentes; por exemplo, se uma câmera de vigilância for infectada, basta desconectá-la da rede. Por outro lado, um ataque contra uma linha de manufatura automotiva requer uma paralisação não planejada que custa à empresa US$ 22.000 por minuto, ou US$ 1,3 milhão por hora[7].

[7] www.businessinsider.com/what-1-minute-of-unplanned-downtime-costs-major-industries-2016-9

A solução SDSN da Juniper permite definir políticas flexíveis e abrangentes para acomodar diferentes cenários de IoT e homogeneizar as decisões de aplicação automatizada de políticas para qualquer fornecedor e nuvem, em qualquer lugar, simplificando as operações de segurança gerais. Por exemplo, quando um dispositivo IoT é infectado por malware e tenta iniciar uma comunicação com um servidor Command and Control (C&C), o Juniper Sky ATP ou o Juniper ATP Appliance detecta este comportamento anormal e o relata imediatamente ao Security Director Policy Enforcer. O Policy Enforcer aplica automaticamente uma resposta predefinida para colocar o dispositivo infectado em quarentena, impedindo o malware de se disseminar e corrigindo a ameaça em tempo real.

O fluxo de correção ocorre como descrito a seguir e mostrado na Figura 2:

- Um dispositivo de IoT infectado conectado à rede tenta baixar um arquivo restrito ou inicia um ataque em infraestrutura crítica.
- A tentativa de download não autorizada é registrada pelo JSA e o ATP Appliance, sendo relatada ao Junos Space Security Director Policy Enforcer.
- O Policy Enforcer aplica uma regra de lista de controle de acesso/controle de acesso de rede à porta de switch ou ponto de acesso Wi-Fi afetado a fim de colocar o host em quarentena, corrigindo rapidamente a ameaça.

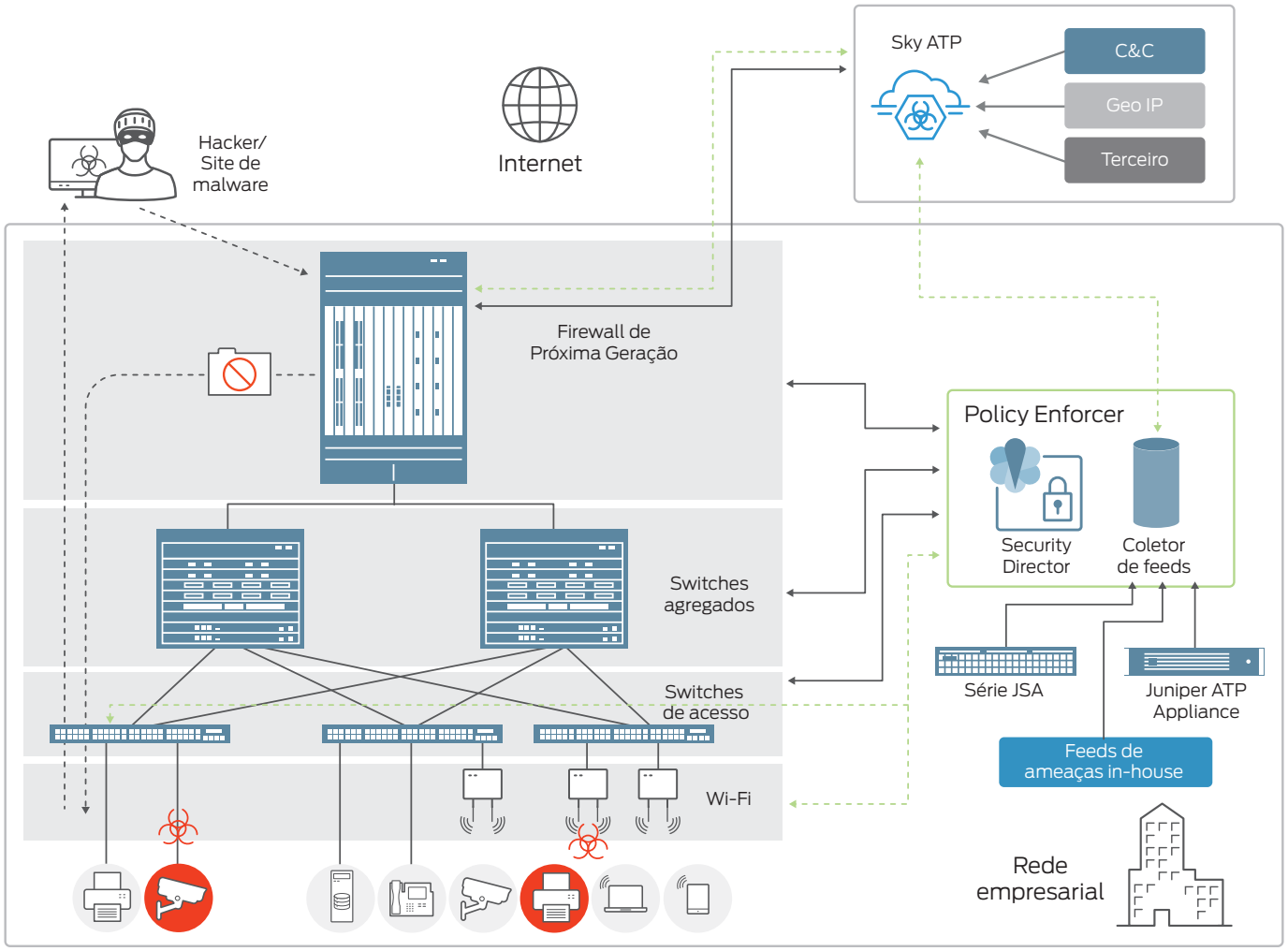

Figura 2: Arquitetura da solução de segurança de IoT da Juniper

- **Cumprimento de requisitos de conformidade regulatória, como NERC CIP, HIPPA e GDPR:** com mais dispositivos conectados à rede empresarial, cada qual gerando mais e mais dados, a necessidade de conformidade com os requisitos regulatórios é cada vez mais importante.

  Além do IP tradicional e protocolos legados como MODBUS para sistemas industriais Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), alguns novos protocolos específicos da IoT, como Message Queue Telemetry Transport (MQTT) e Constrained Application Protocol (CoAP), também estão sendo adotados no circuito convencional. Para atender a requisitos de conformidade, as organizações precisam identificar fontes de comunicação e controlar tráfego com base nos protocolos de IoT usados. O IPS da Juniper, disponível nos Gateways de Serviços da Série SRX, dá suporte à maioria das assinaturas de aplicações de IoT, além de permitir que os usuários finais criem assinaturas personalizadas para suas necessidades específicas. O Security Director facilita a identificação das aplicações sendo usadas e permite modificar assinaturas de aplicações.

  Os dispositivos da Série JSA tornam a conformidade regulatória fácil e automática por meio de ferramentas avançadas de coleta, correlação e relatório. São realizadas verificações de rede regulares, e trilhas de auditoria detalhadas são registradas para facilitar a conformidade com regulamentações federais ou setoriais. O JSA Series tem suporte para várias melhores práticas de regulamentação e segurança, e inclui mais de 500 modelos de relatório de conformidade prontos para uso que atendem às necessidades específicas de relatório e auditoria de conformidade.

- **Proteção escalável, flexível e automatizada em qualquer lugar:** embora muitos cenários de IoT enfrentem vulnerabilidades de segurança semelhantes aos ambientes de TI tradicionais, o número total de dispositivos de IoT aumenta drasticamente os requisitos de escalabilidade. Sensores de IoT podem criar literalmente milhões de sessões breves para trocar informações com aplicações de IoT. Além disso, um grande número de dispositivos de IoT fica em locais remotos; alguns podem até estar sempre mudando de lugar. O conceito tradicional de "perímetro" não se aplica mais ao contexto da IoT. As ameaças continuarão vindo de todos os lugares, e a proteção de segurança precisa ser onipresente.

  Os Gateways de Serviços SRX4000 e SRX5000, já implantados em infraestrutura crítica como aquela que protege as grandes redes elétricas da América do Norte, fornecem o alto número de conexões por segundo e a capacidade de sessão necessários para dar suporte a essas sessões em implantações de IoT de grande escala. Os flexíveis fatores de forma físicos, virtuais e conteinerizados dos SRX, de todos os tamanhos, significam que podem ser colocados onde você quiser, desde a borda da IoT (como um servidor de computação móvel na borda (MEC) ou um gateway de IoT) até o interior de um carro ou em qualquer nuvem, seja pública, privada, híbrida ou multicloud. O Policy Enforcer permite aplicar políticas de segurança automatizadas de maneira consistente, não só em equipamentos da Juniper mas também de terceiros, oferecendo proteção realmente holística.

Resumo — A segurança para IoT em grande escala requer uma mudança de paradigma

Conforme você adota tecnologias de IoT para sua organização com a implantação em grande escala como um próximo passo, a segurança precisa ser abordada de forma completa. Violações da IoT causam grande perda financeira e danos à reputação, além de representarem uma ameaça à segurança das pessoas.

Quando você expande a implantação, o volume total e a variedade dos dispositivos de IoT e a troca de dados relacionada tornam a segurança um desafio significativo. A maioria dos endpoints de IoT tem recursos limitados para executar funções de segurança, tornando o papel da rede como atenuadora de riscos ainda mais crítico. Para a maioria das organizações, o pessoal de segurança é um recurso escasso; com implantações de IoT em grande escala, manter os sistemas seguros será um imenso desafio operacional para as empresas. Os criminosos cibernéticos também continuarão a desenvolver novos ataques, em especial ameaças de dia zero explosivas e desconhecidas, tornando as soluções de segurança baseadas em perímetro insuficientes.

A IoT em grande escala requer uma mudança de paradigma da segurança. Ao contrário de produtos pontuais focados em ações únicas, a solução de segurança para IoT da Juniper, a Software-Defined Secure Network, capacita você a transformar toda a sua rede em uma plataforma unificada de segurança cibernética que utiliza análises, aprendizado de máquina e automação para você melhorar a sua postura de segurança e se defender da expansão dos riscos da IoT. A SDSN da Juniper é escalável, flexível e automatizada, protegendo seus dados, ativos e infraestrutura crítica de IoT em qualquer lugar.

Próximos passos

Para obter mais informações sobre as soluções de segurança da Juniper, visite-nos em www.juniper.net/us/en/products-services/security ou entre em contato com um representante da Juniper Networks.

Sobre a Juniper Networks

A Juniper Networks simplifica as redes com produtos, soluções e serviços que conectam o mundo. Por meio da inovação da engenharia, eliminamos as restrições e as complexidades das redes na era da nuvem para solucionar os maiores desafios que nossos clientes e parceiros enfrentam hoje. Na Juniper Networks, acreditamos que a rede é um recurso de compartilhamento de conhecimentos e avanço humano que desafia o mundo. Estamos comprometidos a imaginar maneiras revolucionárias de fornecer redes automatizadas, escaláveis e seguras que avançam no ritmo dos negócios.

Sede corporativa e de vendas
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Telefone: 888.JUNIPER (888.586.4737)
ou +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

Sede APAC e EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Telefone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510636-002-PT-BR Apr 2018