Symantec
A Division of Broadcom

Resumo do produto

Symantec Endpoint Security

A implementação de uma estratégia coesa de segurança de endpoints é mais importante do que nunca

Introdução

Os endpoints estão entre os principais alvos dos invasores cibernéticos. À medida que as consequências e os danos resultantes de ataques bem-sucedidos aumentam, muitas empresas tentam reforçar sua defesa geral com a adição de vários produtos de proteção de endpoints. Infelizmente, essa abordagem enfraquece a postura de segurança de uma organização.

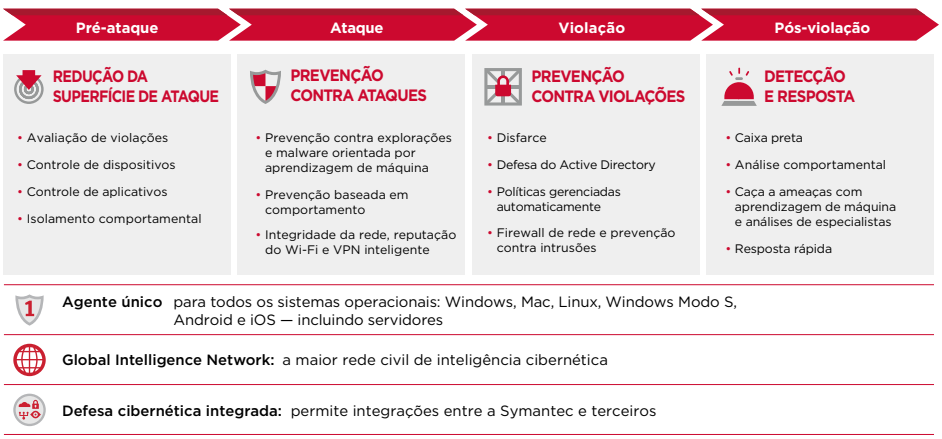
O Ponemon Institute descobriu que as organizações instalam, em média, sete agentes de endpoint diferentes para dar suporte ao gerenciamento e à segurança de TI.[1] Cada agente opera de forma independente, com seu próprio console e conjunto de regras e políticas, e tudo isso precisa ser configurado, distribuído, gerenciado e mantido. Além de criarem mais sobrecarga e custos de TI, os vários produtos introduzem lacunas e erros de defesa, aumentando as chances de que uma ameaça passe despercebida.

A prevenção é essencial, porque as ameaças cibernéticas globais estão mais agressivas do que nunca e podem ter um impacto esmagador sobre uma empresa. Enquanto você lê este resumo do produto, uma empresa inteira pode ser comprometida. Segundo se sabe, o ataque NotPetya devastou uma das maiores empresas de remessas do mundo em apenas sete minutos,[2] juntamente com milhares de outras organizações. É fundamental evitar os ataques o mais cedo possível, porque a janela de detecção e reação a um ataque moderno é muito breve. O investimento na resposta a incidentes também é essencial para criar uma postura de segurança mais rígida a fim de evitar ataques futuros. Com a Symantec, você pode acabar com os comprometimentos. Por que escolher entre a melhor segurança e a maior simplicidade quando se pode ter as duas?

Principais recursos do Symantec Endpoint Security Complete

- Proteção para todos os endpoints: laptops, desktops, tablets, dispositivos móveis e servidores
- Agente único para redução da superfície de ataque, prevenção contra ataques, prevenção contra violações e Endpoint Detection and Response (EDR)
- Console único com visibilidade de ameaças em tempo real
- Flexibilidade de implementação: modelos no local, gerenciados em nuvem e híbridos
- Segurança do Active Directory
- Recursos de isolamento comportamental e controle de aplicativos
- Gerenciamento de segurança orientado por inteligência artificial (IA)
- Análise de ataques direcionados e caça a ameaças
- A Global Intelligence Network (GIN), uma das maiores do mundo, fornece informações sobre ameaças em tempo real, análises de ameaças, classificação de conteúdo e dados abrangentes de bloqueio de ameaças
- Integração a aplicativos de terceiros, incluindo Microsoft Graph, Open C2 e outras soluções da Symantec, por meio do Symantec ICDx

Figura 1: Symantec Endpoint Security Complete



1: The 2017 State of Endpoint Security Risk, Ponemon Institute LLC, novembro de 2017.
2: *You're Just 7 Minutes Away from an Infinite Toxic Loop in Your Network*, Blog da Symantec, abril de 2019.

Principais recursos da versão Enterprise

- Protege laptops, desktops, celulares e tablets
- Agente único para a segurança de endpoints
- Console único com visibilidade de ameaças em tempo real
- Flexibilidade de implementação: modelos no local, gerenciados em nuvem e híbridos
- Gerenciamento de segurança orientado por inteligência artificial (IA)
- A Global Intelligence Network, uma das maiores do mundo, fornece informações sobre ameaças em tempo real
- Integração a aplicativos de terceiros, como Microsoft Graph, Open C2 e outras soluções da Symantec, por meio do Symantec Integrated Cyber Defense Exchange (ICDx)

Visão geral da solução

O Symantec Endpoint Security Complete oferece a plataforma de segurança de endpoints mais abrangente e integrada do planeta. Como uma solução no local, híbrida ou baseada em nuvem, a plataforma de agente único da Symantec protege todos os seus endpoints tradicionais e móveis, fornecendo defesas interligadas no nível de dispositivo, aplicativo e rede, além de usar inteligência artificial (IA) para otimizar decisões de segurança. Um sistema de gerenciamento unificado e baseado em nuvem simplifica a proteção, a detecção e a resposta a todas as ameaças avançadas direcionadas aos seus endpoints.

Segurança de endpoints incomparável para sua empresa
O Symantec Endpoint Security fornece à sua organização a melhor segurança de endpoints para dispositivos tradicionais e móveis em todas as três fases de ataque — pré-ataque, ataque e pós-ataque — com ênfase na prevenção em toda a cadeia de ataque para permitir uma rápida contenção. A redução proativa da superfície de ataque e as tecnologias inovadoras de prevenção fornecem a defesa mais robusta contra as ameaças mais difíceis de detectar e que dependem de métodos dissimulados de malware, roubo de credenciais, ataques sem arquivo e do tipo "living off the land". A Symantec também evita violações completas antes que a exfiltração possa ocorrer. A análise sofisticada de ataques, a análise comportamental, os manuais de investigação automatizados e a primeira metodologia de prevenção de movimentação lateral e roubo de credenciais do setor fornecem detecções precisas de ataques e caça proativa de ameaças para conter o invasor e resolver ameaças persistentes em tempo real.

Redução da superfície de ataque

A Symantec fornece a defesa proativa de endpoints com recursos de redução da superfície de pré-ataque baseados em controles e tecnologias avançadas de políticas que verificam continuamente vulnerabilidades e configurações incorretas em aplicativos, no Active Directory e em dispositivos. Com as defesas de redução da superfície de ataque implementadas, muitas táticas e técnicas de ataque não podem ser utilizadas nos endpoints.

- A **Avaliação de violações** sonda continuamente o Active Directory em busca de configurações incorretas de domínios, vulnerabilidades e persistências utilizando simulações de ataque para identificar riscos, o que permite a mitigação imediata com recomendações prescritivas sobre correção.
- O **Controle de dispositivos** especifica políticas de bloqueio ou permissão em diferentes tipos de dispositivos que se conectam a computadores clientes, como dispositivos USB, infravermelho e FireWire, para reduzir o risco de ameaças e exfiltração.
- O **Controle de aplicativos** avalia o risco de aplicativos e suas vulnerabilidades e permite que apenas aplicativos conhecidamente bons sejam executados.
- O **Isolamento comportamental** limita comportamentos incomuns e arriscados de aplicativos confiáveis com o mínimo de impacto operacional.
- A **Correção de vulnerabilidades**[3] aprimora a postura de segurança, fornecendo visibilidade e inteligência sobre vulnerabilidades e seus riscos associados. As vulnerabilidades detectadas são classificadas por gravidade, com base no CVSS (Common Vulnerability Scoring System), juntamente com a identificação do número de dispositivos afetados, para garantir que as ameaças maiores sejam corrigidas primeiro.

3: Suporte apenas em dispositivos Win 10, Win 10 Modo S, iOS e Android.

Prevenção contra ataques

A prevenção contra ataques multicamada da Symantec protege imediata e efetivamente contra vetores e métodos de ataque com e sem arquivo. A aprendizagem de máquina e a inteligência artificial usam esquemas avançados de detecção baseados em dispositivos e nuvem para identificar ameaças em evolução entre vários tipos de dispositivos, sistemas operacionais e aplicativos. Os ataques são bloqueados em tempo real para manter a integridade dos endpoints e evitar impactos negativos.

- A **Prevenção contra malware** combina detecção e bloqueio pré-execução de ameaças novas e em evolução (aprendizagem de máquina avançada, uso de área restrita para detectar malwares ocultos em empacotadores personalizados e monitoramento e bloqueio comportamentais de arquivos suspeitos) e métodos baseados em assinatura (análise de reputação de arquivos e sites e verificação de malware).
- A **Prevenção contra explorações** bloqueia ameaças de dia zero baseadas em memória de vulnerabilidades em softwares populares.
- A **Proteção intensiva** permite fazer o ajuste fino do nível de detecção e bloqueio separadamente a fim de otimizar a proteção e obter maior visibilidade dos arquivos suspeitos.
- A **Segurança na conexão de rede** identifica redes Wi-Fi invasoras, utiliza a tecnologia de reputação de hotspots e fornece uma VPN orientada por políticas para proteger as conexões de rede e oferecer suporte à conformidade.

Prevenção contra violações

A abordagem de prevenção da Symantec envolve a contenção dos invasores o mais cedo possível — no endpoint — antes que eles tenham qualquer oportunidade de persistir na rede. Várias tecnologias de disfarce e prevenção contra intrusões orientadas por IA trabalham juntas para deter os esforços de persistência na rede antes e imediatamente após o comprometimento dos endpoints — e antes que uma violação completa possa ocorrer.

- A **Prevenção contra intrusões e o firewall** bloqueiam ataques conhecidos de malware baseados em rede e navegador utilizando regras e políticas e impedem a configuração de comandos e controles com o uso de uma lista de bloqueio automatizada de endereços IP de domínios.
- O recurso de **disfarce** usa chamarizes e iscas (arquivos, credenciais, compartilhamentos de rede, entradas de cache, solicitações da Web e endpoints falsos) para expor, determinar a intenção e as táticas do invasor e atrasar os invasores através da visibilidade antecipada.
- A **Segurança do Active Directory** defende a principal superfície de ataque contra movimentações laterais e roubo de credenciais de administrador de domínios ao controlar a percepção do invasor quanto aos recursos do Active Directory de uma organização a partir do endpoint e ao utilizar a ofuscação ilimitada (ou seja, criação de ativos e credenciais falsas). Com a ofuscação, o invasor se entrega enquanto interage com ativos *falsos* ou tenta usar credenciais de administrador de domínio na percepção do Active Directory.
- As **Políticas gerenciadas automaticamente**, baseadas em IA e ML avançadas, combinam com exclusividade indicadores de comprometimento e anomalias históricas para adaptar continuamente os limites ou as regras de políticas de endpoint e mantê-los atualizados e alinhados ao perfil de risco atual de sua organização.

Resposta e correção pós-violação

A Symantec combina as tecnologias de detecção e resposta em endpoints (EDR) e a experiência incomparável de analistas do Centro de operações de segurança (SOC), fornecendo as ferramentas necessárias para impedir rapidamente incidentes em endpoints e minimizar os impactos de ataques. Os recursos integrados de EDR, em uma arquitetura de agente único que abrange endpoints tradicionais e modernos, detectam com precisão ataques avançados, fornecem análises em tempo real e permitem caçar ameaças ativamente e realizar investigações e correções forenses.

- A **Análise comportamental** oferece a capacidade de registrar e analisar o comportamento dos endpoints para identificar técnicas avançadas de ataque que podem estar utilizando aplicativos legítimos para fins maliciosos. Esses dados são enriquecidos com a estrutura MITRE ATT&CK para ajudar a orientar os responsáveis pela resposta a incidentes durante as investigações.
- **Ferramentas avançadas de caça a ameaças** são fornecidas no Symantec EDR, incluindo manuais incorporados que encapsulam as práticas recomendadas de caçadores de ameaças experientes e da detecção de comportamentos anômalos. Os responsáveis por resposta a incidentes podem verificar toda a empresa em busca de IOCs para incluir a consulta direta aos endpoints.
- A **Resposta integrada** age diretamente sobre o endpoint para fazer correções por meio de recuperação e exclusão de arquivos, isolamento de endpoints e inclusão em listas de bloqueio. O Symantec EDR oferece suporte ao envio automático de arquivos suspeitos identificados para a área restrita, para uma análise completa de malware, incluindo a exposição de malwares com consciência de VM.

Resposta e correção pós-violação (cont.)

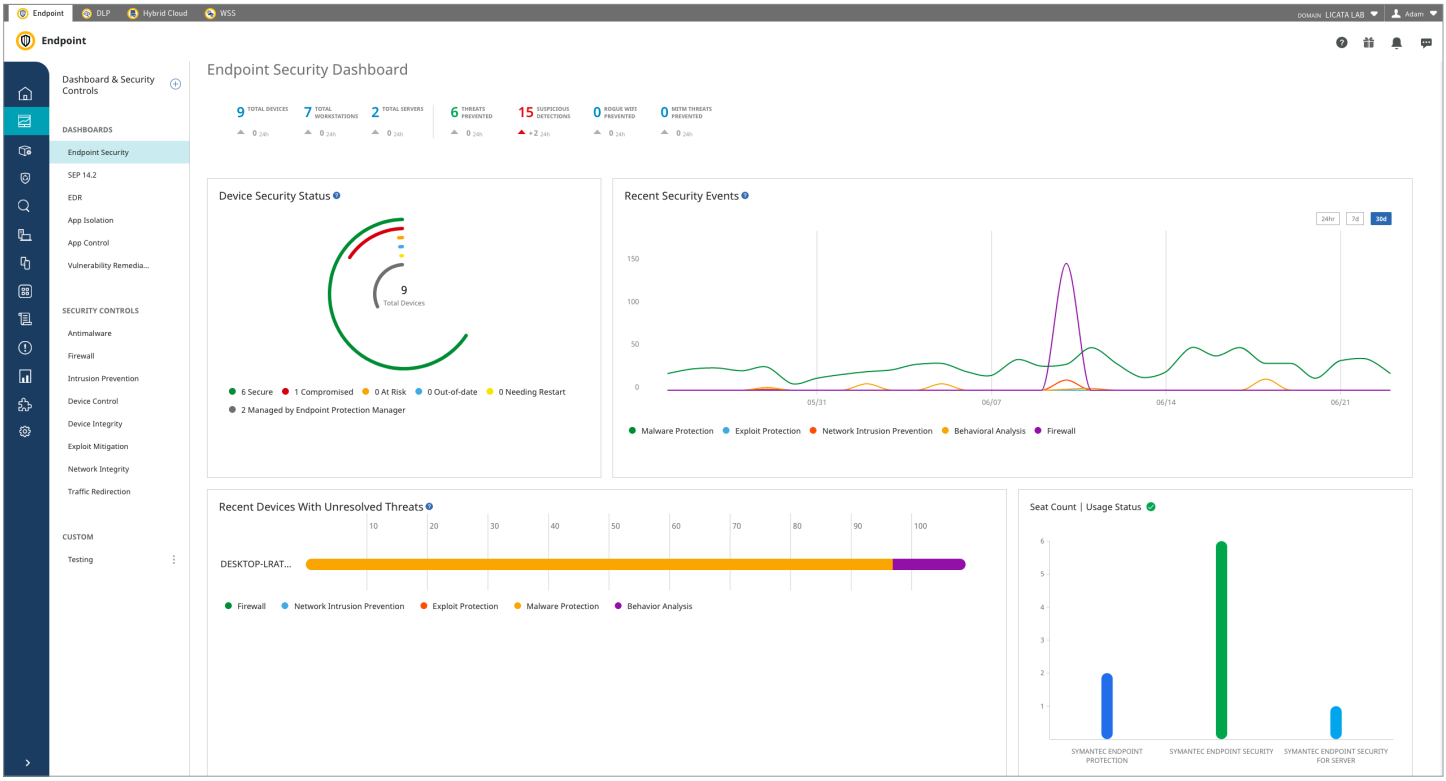
- A **Caça a ameaças** procura por incidentes de alta fidelidade e combina o poder da aprendizagem de máquina avançada e da experiência dos analistas de SOC para detectar as ferramentas, as táticas e os procedimentos utilizados pelos adversários. Ela garante que os ataques críticos sejam rapidamente identificados com o contexto relevante. Além disso, ela fornece acesso intuitivo aos dados globais de segurança da Symantec para auxiliar nos esforços de caça a ameaças de sua equipe.
- A **Resposta rápida** minimiza o tempo de correção de ameaças e de resposta a invasores em tempo real. As ferramentas e os manuais incorporados detêm as ameaças isolando os invasores e fornecem acesso interativo aos endpoints.

Proteja seu ambiente dinâmico de endpoints

Uma pilha de agente único reduz os esforços de segurança de seus endpoints integrando (e coordenando) as melhores tecnologias disponíveis de prevenção, detecção e resposta. Gerencie tudo por meio de um único sistema de gerenciamento baseado em nuvem (Integrated Cyber Defense Manager), minimizando o tempo, os recursos e os esforços necessários para configurar, distribuir, gerenciar e manter sua postura de segurança. Tudo o que você precisa pode ser acessado com um ou dois cliques, o que aumenta a produtividade do administrador e reduz o tempo de resposta para impedir rapidamente quaisquer eventos relacionados à segurança.

- O **Gerenciamento de segurança orientado por IA** atualiza políticas com mais precisão e menos configurações incorretas para aumentar a segurança.
- Os **Fluxos de trabalho simplificados** asseguram que tudo funcione em sintonia para aumentar o desempenho, a eficiência e a produtividade.
- As **Recomendações baseadas em contexto** ajudam a atingir o desempenho ideal ao eliminar tarefas de rotina e proporcionar decisões melhores.
- O **Gerenciamento autônomo da segurança** aprende continuamente com os comportamentos de administradores e usuários para melhorar as avaliações de ameaças, refinar as respostas e reforçar sua postura de segurança geral.

Figura 2: Interface do usuário do endpoint



Reduza a complexidade com o amplo portfólio da Symantec e as integrações com terceiros

O Symantec Endpoint Security é uma solução de base que facilita a integração para que as equipes de segurança de TI possam detectar ameaças em qualquer ponto da rede e lidar com elas por meio de uma resposta orquestrada. O Symantec Endpoint Security funciona em conjunto com outras soluções da Symantec e com produtos de terceiros por meio de aplicativos dedicados e APIs publicadas para reforçar sua postura de segurança. Nenhum outro fornecedor oferece uma solução integrada que orquestra uma resposta no endpoint (listas de bloqueio e correção) acionada pela detecção de uma ameaça na Web e nos gateways de segurança de email. As integrações específicas incluem:

- **Symantec Web Security Service:** redireciona o tráfego da Web de usuários do Symantec Endpoint Security em roaming para o Symantec Web Security Service e o Symantec CASB por meio de um arquivo PAC.
- **Symantec Web Gateway:** as APIs REST programáveis possibilitam a integração com uma infraestrutura de segurança de rede no local.
- **Symantec Validation and ID Protection:** autenticação multifator, incluindo smart cards PIV/CAC para o Symantec Endpoint Security no local e consoles de gerenciamento baseados em nuvem.
- **Symantec Content Analysis:** utiliza a área restrita dinâmica no local e outros mecanismos de ameaças para a análise aprofundada de arquivos suspeitos enviados pelo Symantec Endpoint Security.
- **Symantec Data Loss Prevention:** previne contra a exfiltração de dados de informações confidenciais por meio da inteligência de ameaças em tempo real de aplicativos suspeitos para o DLP.

Figura 3: Symantec Endpoint Security

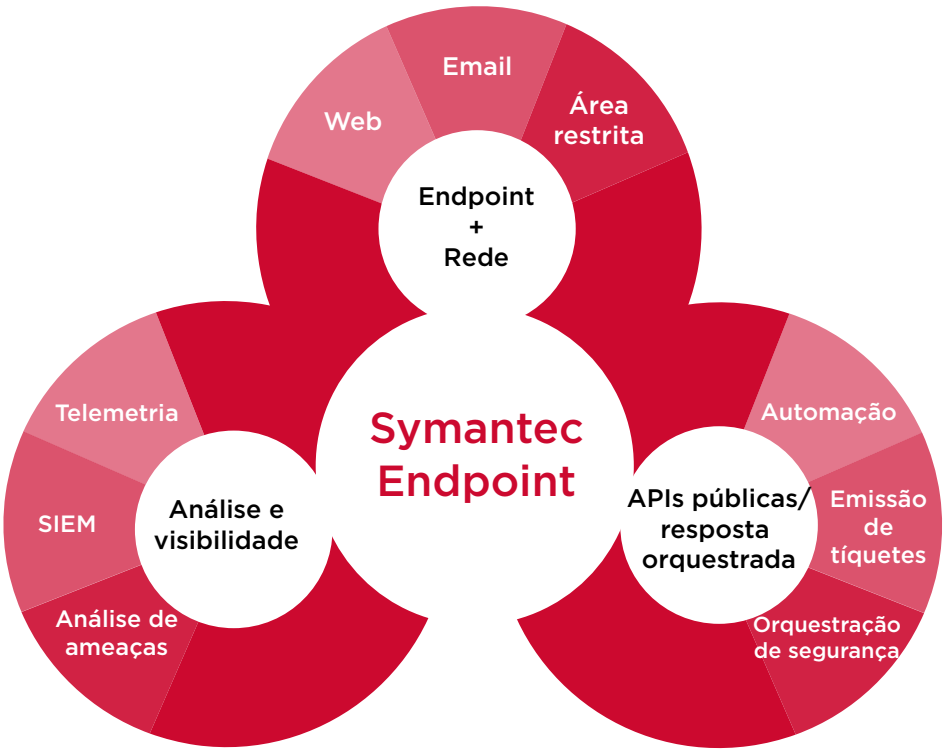


Figura 4: Opções de licenciamento

Recursos

	SEP	SES ENTERPRISE	SES COMPLETE
	Padrão do setor em proteção de endpoints. Nº 1 em proteção há cinco anos e agora também Nº 1 em desempenho pela AV Test.	Estende o SEP a todos os SOs e dispositivos, incluindo os móveis. Oferece o gerenciamento em nuvem.	Acrescenta proteção avançada, EDR, caça a ameaças e outras tecnologias para proteção total.
OPÇÕES DE GERENCIAMENTO	Local	Local, Nuvem, Híbrido	
AGENTES NECESSÁRIOS	AGENTE ÚNICO DA SYMANTEC		
COBERTURA DE DISPOSITIVOS Corporativos, BYOD, UYOD	Laptop, Desktop, Servidor	Celular, Tablet, Laptop, Desktop, Servidor	
COBERTURA DE SISTEMAS OPERACIONAIS	Windows, macOS, Linux	Windows (incluindo Modo S e Arm), macOS, iOS, Linux, Android	

Tecnologias de proteção

	SEP	SES ENTERPRISE	SES COMPLETE
PREVENÇÃO CONTRA ATAQUES			
A MELHOR PREVENÇÃO CONTRA ATAQUES DO SETOR	✓	✓	✓
DEFESA CONTRA AMEAÇAS A DISPOSITIVOS MÓVEIS		✓	✓
CONEXÃO DE REDE SEGURA		✓	✓
REDUÇÃO DA SUPERFÍCIE DE ATAQUE			
AVALIAÇÃO DE VIOLAÇÕES			✓
ISOLAMENTO COMPORTAMENTAL			✓
CONTROLE DE APLICATIVOS			✓
CONTROLE DE DISPOSITIVOS	✓	✓	✓
PREVENÇÃO CONTRA VIOLAÇÕES ...			
PREVENÇÃO CONTRA INTRUSÕES	✓	✓	✓
FIREWALL	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
...PREVENÇÃO CONTRA VIOLAÇÕES			
DISFARCE	✓	✓	✓
SEGURANÇA DO ACTIVE DIRECTORY			✓
RESPOSTA E CORREÇÃO			
DETECÇÃO E RESPOSTA EM ENDPOINTS			✓
ANÁLISE DE ATAQUES DIRECIONADOS EM NUVEM			✓
ANÁLISE COMPORTAMENTAL			✓
CAÇA A AMEAÇAS			✓
RESPOSTA RÁPIDA			✓
OPERAÇÕES DE TI			
DESCOBERTA E IMPLEMENTAÇÃO	✓	✓	✓
VERIFICAÇÕES DE INTEGRIDADE DO HOST	✓	✓	✓

Symantec™
A Division of Broadcom

Para obter informações sobre o produto, visite nosso site em: go.broadcom.com/ses

SED-EPS-PB101_PTB 25 de junho de 2020