Symantec Endpoint Protection 14

A Solução Mais Completa de Segurança de Terminais para a Geração em Nuvem

Num relance

Proteja os pontos de extremidade de todos os vetores de ataque com eficácia líder do setor com uma arquitetura de agente único

- Defenda-se contra ransomware e outras ameaças emergentes com proteção em várias camadas que une tecnologias sem assinatura, como aprendizado de máquina avançado, análise de comportamento e prevenção de exploração com recursos de proteção comprovados, como prevenção de intrusões, análise de reputação e muito mais.
- Obtenha visibilidade aprimorada de arquivos suspeitos por meio de proteção ajustável para tomar melhores decisões sobre políticas
- Use técnicas de fraude para expor adversários ocultos e determinar sua intenção de melhorar a postura de segurança
- Proteja aplicativos comumente usados contra explorações de vulnerabilidades e isole aplicativos suspeitos de atividades mal-intencionadas

Realize a defesa cibernética integrada em escala

- Detectar ameaças em qualquer lugar e responder com o SEP integrando-se à infraestrutura de segurança de rede, como gateways de e-mail e web
- Integrar com EDR para investigação e resposta a incidentes, alavancando o mesmo agente SEP
- ntegrar-se à infraestrutura de TI existente para automação e orquestração com APIs abertas

Ativar negócios com um alto desempenho, solução leve

- Otimizar a frequência de atualização de conteúdo para endpoints com restrições de largura de banda de rede sem comprometer a eficácia da segurança
- Aumente o desempenho com um agente leve e conjuntos de definições de vírus que exigem um uso mínimo da largura de banda da rede (70% menos em comparação com o SEP12)
- Detecção de velocidade com técnicas de design avançadas e pesquisa de nuvem patenteada em tempo real que proporciona tempos de digitalização mais rápidos (15% mais rápido em comparação com o SEP12)

Introdução

Com a natureza em constante evolução do ambiente de TI de hoje, os invasores estão usando ataques mais sofisticados para se infiltrar nas redes e o endpoint representa a última linha de defesa. As organizações estão mais preocupadas com danos cibernéticos e interrupções, já que os ataques de ransomware estão crescendo, como ficou evidente com os surtos de WannaCry e Petya. Além disso, o uso em expansão dos invasores de ataques furtivos e sem arquivos combinados com a “vida fora da terra” (alavancando ferramentas comuns de TI para ataques) ameaça a confidencialidade, a integridade e a disponibilidade dos ativos de endpoint.

Então, o que as equipes de segurança podem fazer para lidar com ataques cibernéticos? O gerenciamento de produtos e tecnologias de vários pontos é esmagador e os desafios se acumulam ao gerenciar a segurança em várias regiões geográficas com diversos sistemas operacionais e plataformas. Com recursos limitados e orçamentos limitados, as equipes de segurança querem tecnologias fáceis de gerenciar que possam se integrar umas com as outras para melhorar a segurança geral. Eles não precisam de “apenas outro produto pontual”. Veja a Figura 1.

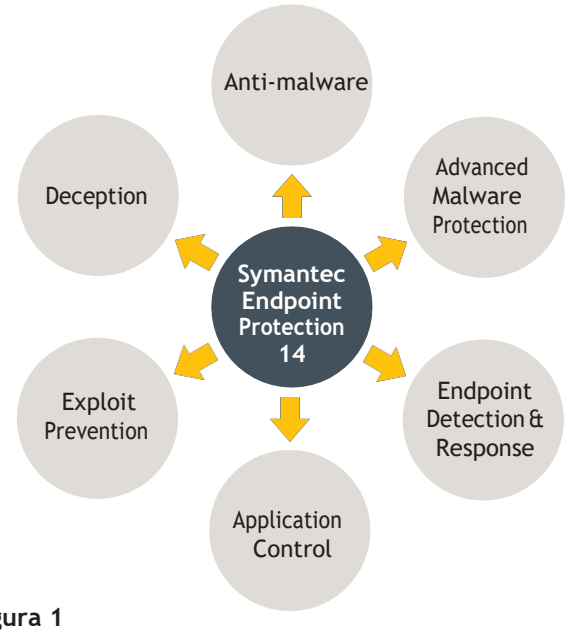

Figura 1

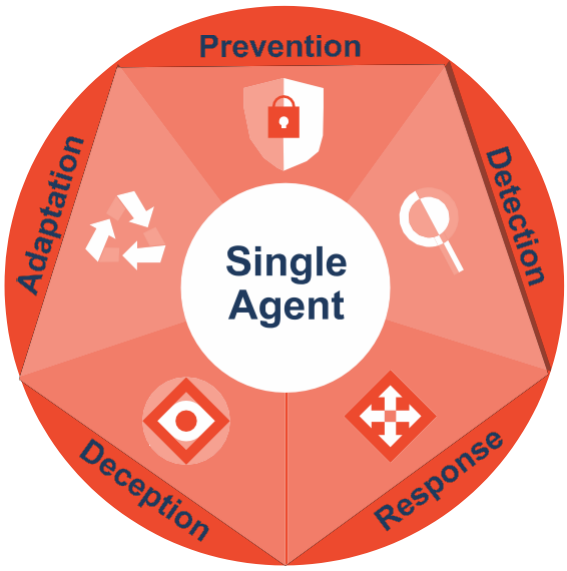

Figure 2. The SEP Security Framework

O Symantec Endpoint Protection (SEP) oferece proteção superior e multicamadas para interromper as ameaças, independentemente de como elas atacam seus endpoints. O SEP integra-se à infraestrutura de segurança existente para fornecer respostas orquestradas para lidar com ameaças rapidamente. O agente SEP simples e leve oferece alto desempenho sem comprometer a produtividade do usuário final, para que você possa se concentrar em seus negócios. O SEP permite que a equipe de segurança seja executada em muitos casos de uso de segurança, conforme descrito pela estrutura de segurança da Figura 2.

Proteja Edpoints de todos os Vetores de Ataque na Eficácia Líder do Setor com uma Arquitetura de Agente Único

PREVENÇÃO

O SEP protege endpoints independentemente de onde os atacantes atacam na cadeia de ataque, como mostra a Figura 3. A eficácia de segurança do SEP lidera o setor como validado por terceiros. Este nível

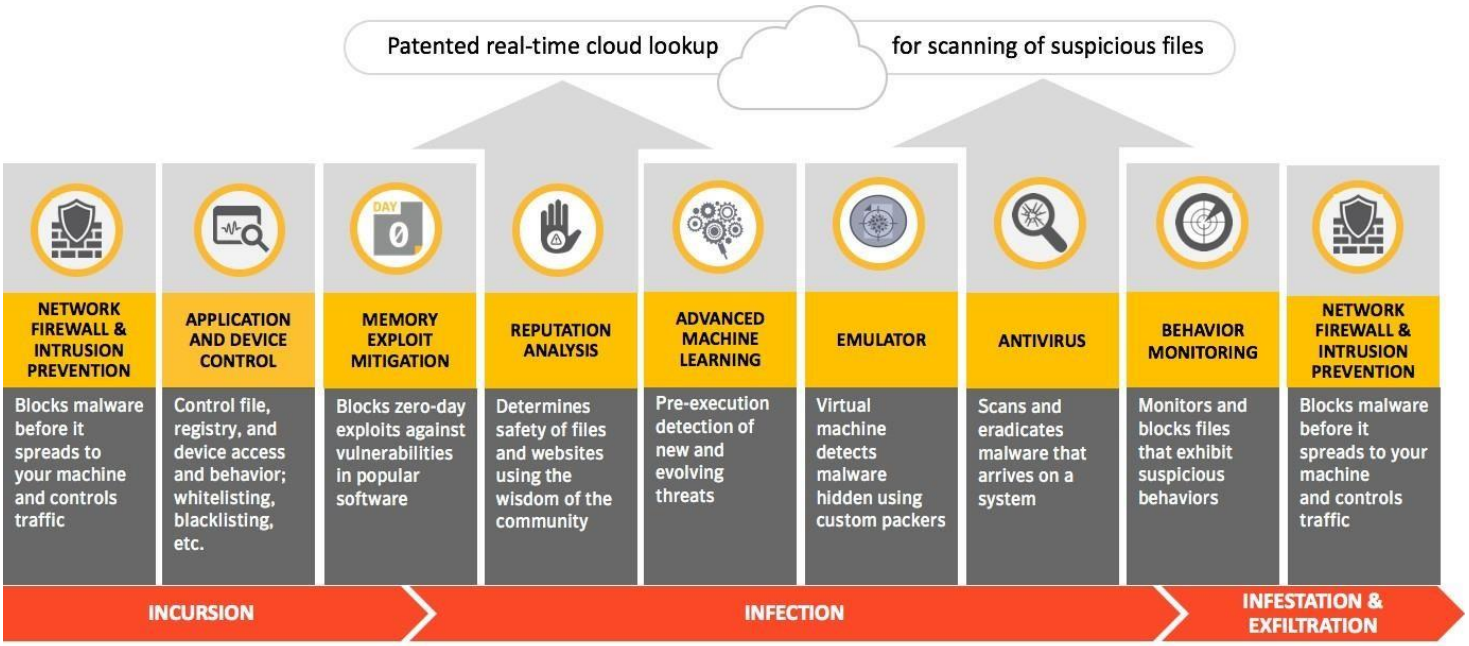

Figura 3.

de prevenção só é possível com uma combinação de tecnologias principais e novas tecnologias de ponta.

TECNOLOGIAS DE ASSINATURA

- **Linguagem Avançada de Máquinas (AML)** - detecta ameaças novas e em evolução, pré-execução.
- **Mitigação de Exploit de Memória** – bloqueia explorações de dia zero contra vulnerabilidades em softwares populares.
- **Monitoramento de Comportamento** - monitora e bloqueia arquivos que exibem comportamentos suspeitos.

RECURSOS AVANÇADOS

- **Rede de Inteligência Global(GIN)** – a maior rede de inteligência de ameaças civis do mundo, informada por 175 milhões de terminais e 57 milhões de ataques por 157 países. Os dados coletados são analisados por mais de mil pesquisadores de ameaças altamente qualificados para fornecer visibilidade única e inovações de segurança de ponta contra ameaças.
- **Reputation Analysis** – determina a segurança de arquivos e sites usando técnicas de inteligência artificial na nuvem e alimentado pelo GIN.
- **Emulador** - Usa uma lite-sandbox para detectar malware polimórfico escondido por empacotadores personalizados.
- **Nuvem de Ameaças Inteligentes** Os recursos de varredura rápida usando técnicas avançadas, como pipelining, propagação de confiança e consultas em lote, tornaram desnecessário o download de todas as definições de assinatura para o endpoint para manter um alto nível de eficácia. Portanto, apenas as informações mais recentes sobre ameaças são baixadas, reduzindo o tamanho dos arquivos de definição de assinaturas em até 70%, o que, por sua vez, reduz o uso de largura de banda.
- **Integração do Secure Web Gateway** – Novas APIs REST programáveis possibilitam a integração com a infraestrutura de segurança existente, incluindo o Secure Web Gateway, orquestrando uma resposta no endpoint para interromper rapidamente a disseminação da infecção.

PRINCIPAIS CAPACIDADES

- **Antivirus** - verifica e erradica malware que chega em um sistema.
- **Prevenção de firewall e intrusão** - bloqueia malware antes de se espalhar para a máquina e controla o tráfego.
- **Controle de aplicativos e dispositivos** controla o acesso e comportamento do arquivo, registro e dispositivo; também oferece listas de permissões e listas negras.
- **Power Eraser** – uma ferramenta agressiva, que pode ser acionada remotamente, para lidar com ameaças persistentes avançadas e corrigir malwares persistentes.
- **Integridade do host** – garante que os terminais estejam protegidos e em conformidade, aplicando políticas, detectando alterações não autorizadas e conduzindo avaliações de danos com a capacidade de isolar um sistema gerenciado que não atenda aos seus requisitos.
- **System Lockdown** - permite que aplicativos listados em branco (conhecidos como bons) sejam executados ou bloqueie aplicativos em lista negra (conhecidos por serem ruins) da execução.

Além disso, somente o SEP permite que as equipes de segurança de TI ajustem o nível de detecção e bloqueio para otimizar a proteção e obter visibilidade aprimorada dos arquivos suspeitos para cada ambiente do cliente, conforme mostrado na Figura 4. Essa segurança ajustável chamada Intensive Protection é disponibilizada com uma nova nuvem console que se integra automaticamente ao SEP Manager local e fornece um fluxo de trabalho fácil para colocar arquivos suspeitos na lista negra ou colocar na lista de permissões todos os falsos positivos.

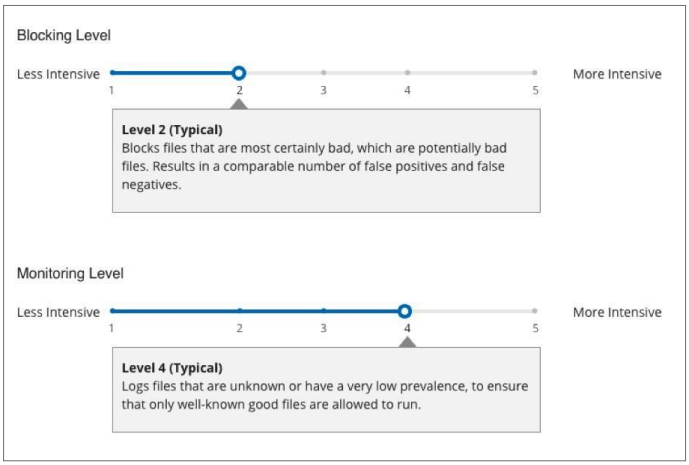

Figure 4. Monitoramento e bloqueio ajustáveis estão disponíveis via Proteção Intensiva.

A arquitetura de agente único da Symantec permite que as equipes de segurança de TI adicionem tecnologia de segurança inovadora com implantação simplificada, o que significa que não são necessários novos agentes.

DETECÇÃO E RESPOSTA (EDR)

Symantec Advanced Threat Protection: O Endpoint fornece investigação e resposta a incidentes utilizando os recursos integrados do EDR no SEP. Ele pode ser implantado em uma hora para expor ataques avançados com aprendizado de máquina de precisão, análise

comportamental e inteligência de ameaças, minimizando os falsos positivos e ajudando a garantir altos níveis de produtividade para as equipes de segurança. Os recursos de EDR da Symantec permitem que os respondentes de incidentes pesquisem, identifiquem e contenham rapidamente todos os endpoints afetados, enquanto investigam ameaças usando o sandbox local e baseado na nuvem. Além disso, o registro contínuo da atividade do sistema oferece suporte a visibilidade completa do Endpoint e consultas em tempo real.

Symantec EDR:

- **Detecta e expõe** – Reduza o tempo para violar a descoberta e exponha rapidamente o escopo.
- **Investiga e contém -** Aumenta a produtividade da resposta de incidentes e garante a contenção de ameaças.
- **Resolves**– Rapidamente conserta endpoints e garante que a ameaça não retorne.
- **Melhora os investimentos de segurança** – Integrações pré-construídas e API pública.

DECEPTION

A SEP Deception1 planta os deceptors (isto é, iscas) para expor os adversários escondidos e revelar a intenção e as táticas do atacante através da visibilidade antecipada, de modo que a informação possa ser usada para melhorar a postura de segurança. O SEP Deception oferece detecção precisa e perspicaz, ao mesmo tempo em que oferece rapidez no valor.
Os clientes conjuntos do Symantec Endpoint Protection e do Symantec Managed Security Services se beneficiam do monitoramento em tempo real 24x7 do SEP Deception e da resposta de uma equipe global de especialistas. A Symantec é o único fornecedor de plataforma de proteção de terminais que oferecem o deception.

SEP Deception:

- Usa iscas e engodos para segurança proativa para expor e atrasar os invasores.
- Determina a intenção do invasor de melhorar a postura de segurança.
- Fornece Deception em escala para simplificar a implantação e o gerenciamento.

ADAPTAÇÃO

O SEP Hardening é uma solução de defesa de aplicativos avançada em nuvem que fornece proteção abrangente para aplicativos, isolando aplicativos suspeitos e protegendo aplicativos confiáveis. Ao contrário dos produtos pontuais de outros fornecedores de isolamento de aplicativos, o SEP Hardening, em combinação com o SEP, oferece eficácia sem precedentes contra malware e aplicativos suspeitos. Além disso, o SEP Hardening mantém uma alta produtividade dos funcionários, apoiando totalmente os fluxos de trabalho padrão dos funcionários.

SEP Hardening:

- Segurança abrangente de aplicativos, minimizando a superfície de ataque.
- Visibilidade sem precedentes, descobrindo e categorizando todos os aplicativos de endpoint.
- Velocidade mais rápida de valor, aproveitando a arquitetura de agente único do SEP.

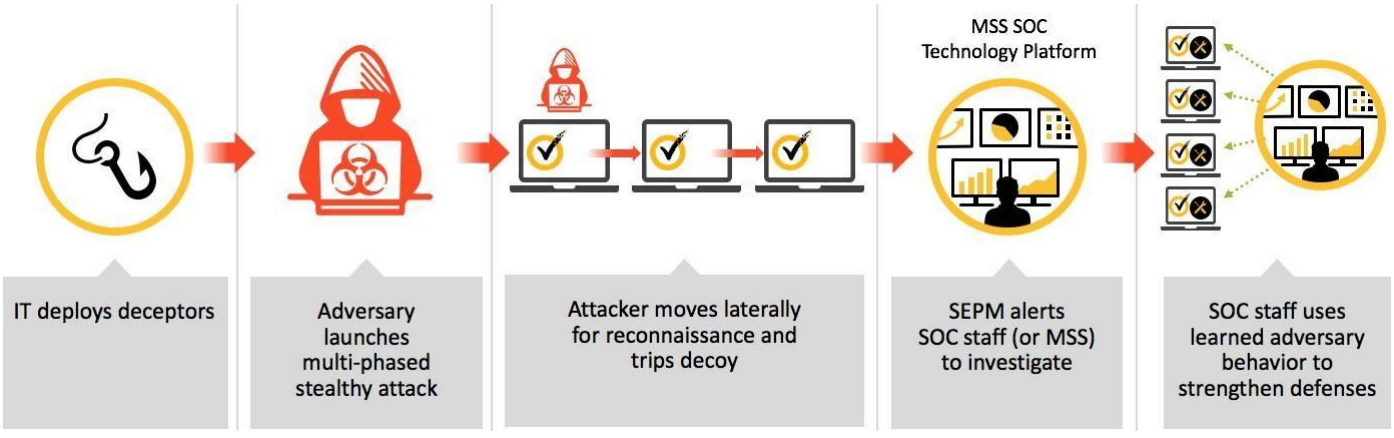

Figura 5. How SEP Deception works?

[1] Consulting services are required to configure and deploy the SEP Deception feature.

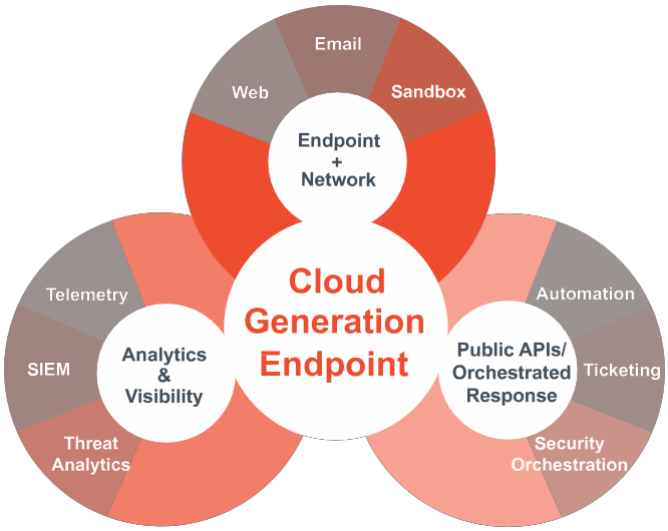

Figura 6.

Realize a defesa cibernética integrada em escala

A maioria das grandes organizações oferece suporte a ambientes globais de TI que estão se tornando cada vez mais complexos. Muitas soluções implementadas só fazem um trabalho muito específico. Portanto, as organizações precisam de uma solução de proteção de endpoint que ofereça maior valor e melhor proteção geral, integrando-se a outras soluções de segurança de TI para compartilhar inteligência e defender a rede em conjunto.

O SEP 14 é um produto básico que facilita a integração para que as equipes de segurança de TI possam detectar ameaças em qualquer lugar da rede e lidar com essas ameaças com respostas orquestradas. O SEP 14 trabalha ao lado de soluções Symantec (por exemplo, como um componente chave da Plataforma de Defesa Cibernética Integrada e com produtos de terceiros (via APIs publicadas) para fortalecer a postura de segurança. A Plataforma Integrada de Defesa Cibernética da Symantec unifica a segurança local e na nuvem para proteger os usuários, informações, mensagens e a Web, com uma inteligência de ameaças inigualável. Nenhum outro fornecedor fornece uma solução integrada que orquestra uma resposta no endpoint (listas negras e remediação) desencadeada pela detecção de uma ameaça no gateway de rede (ou seja, segurança da Web e de email entradas).

Habilite os negócios com uma solução leve e de alto desempenho

Atualizações de conteúdo grandes e/ou frequentes consomem largura de banda, reduzem o desempenho do terminal e comprometem a produtividade. Otimizar as atualizações de conteúdo e oferecer uma melhor detecção de ameaças é uma situação vantajosa para todos. Esses recursos reduzem o fardo da equipe de TI em programar atualizações frequentes de segurança. E os usuários finais não têm o incômodo de atualizações de segurança que afetam a produtividade.

O SEP 14 oferece melhor proteção com melhor desempenho e menores requisitos de largura de banda. A Symantec pontua consistentemente no topo em testes de desempenho de terceiros, incluindo testes de Benchmark do Enterprise Endpoint Security Performance da Passmark Software para Windows 7 e Windows 10. Visite o Symantec Performance Center para validação adicional de terceiros symantec.com/products/performance-center.

Aumentos significativos de desempenho no SEP incluem::

- Reduzindo os tamanhos das atualizações de conteúdo em 70%[2]
- Entrega de tempos de varredura de detecção 15% mais rápidos[2]

Em comparação com os fornecedores emergentes, o SEP oferece menos complexidade de terminais, reunindo vários recursos em um único agente leve. A tentativa de combinar os recursos de segurança de endpoints da Symantec exigiria vários fornecedores emergentes, várias soluções e, certamente, vários agentes.

[2] Gains from SEP 12 to SEP 14.

System Requirements

Client Workstation and Server System Requirements*

Windows® Operating Systems

- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows 10 November Update (2015) (32-bit, 64-bit)
- Windows 10 Anniversary Update (2016) (32-bit, 64-bit)
- Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 update for April 2014
- Windows Server 2012 R2 update for August 2014
- Windows Server 2016

Windows Hardware Requirements

- 1.9 GHz CPU or higher
- 1 GB of RAM (2 GB recommended)
- 530 MB of free space on the hard disk

Macintosh® Operating Systems

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13

Mac Hardware Requirements

- 64-bit Intel Core 2 Duo or later
- 2 GB of RAM
- 500 MB of free space on the hard disk

Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2, ESX 2.5 or later
- VMware ESXi 4.1 – 5.5
- VMware ESX 6.0
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V)
- Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Oracle Cloud
- Virtual Box by Oracle

Linux Operating System (32-bit and 64-bit versions)

- Amazon Linux
- CentOS 6U3, 6U4, 6U5, 6U6, 7, 7U1, 7U2, 7U3; 32-bit and 64-bit
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit
- Fedora 16, 17; 32-bit and 64-bit
- Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7 - 7.3
- SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP3; 32-bit and 64-bit; 12
- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP3; 32-bit and 64-bit
- Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

Linux Hardware Requirements

- Intel Pentium 4 (2 GHz CPU or higher)
- 1 GB of RAM
- 7 GB of free space on the hard disk

Manager System Requirements

Windows® Operating Systems

- Windows Server 2008 (64 bit), including R2)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2012 R2
- Windows Server 2016

Web Browser

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x through 55.x
- Google Chrome 61.x
- Microsoft Edge

Hardware

- Intel Pentium Dual-Core or equivalent minimum
- 2 GB of RAM (8 GB recommended)
- 8 GB or more free space on the hard disk

Database

Embedded database included or choose from the following:

- SQL Server 2008, SP4
- SQL Server 2008 R2, SP3
- SQL Server 2012, RTM - SP3
- SQL Server 2014, RTM - SP2
- SQL Server 2016, RTM, SP1

SEP Hardening Supports the Following Operating Systems:

- Windows 7 (64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (64-bit)
- Windows 8 (64-bit)
- Windows Embedded 8 Standard (64-bit)
- Windows 8.1 (64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (64-bit)
- Windows 8.1 update for August 2014 (64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (64-bit)
- Windows 10 (64-bit); Windows 10 November Update (2015) (64-bit)
- Windows 10 Anniversary Update (2016) (64-bit)
- Windows 10 Creators Update (2017) (64-bit)

* Para obter uma lista completa dos requisitos do sistema, visite a página de suporte