Novell® ZENworks® Endpoint Security Management

Resumo do produto

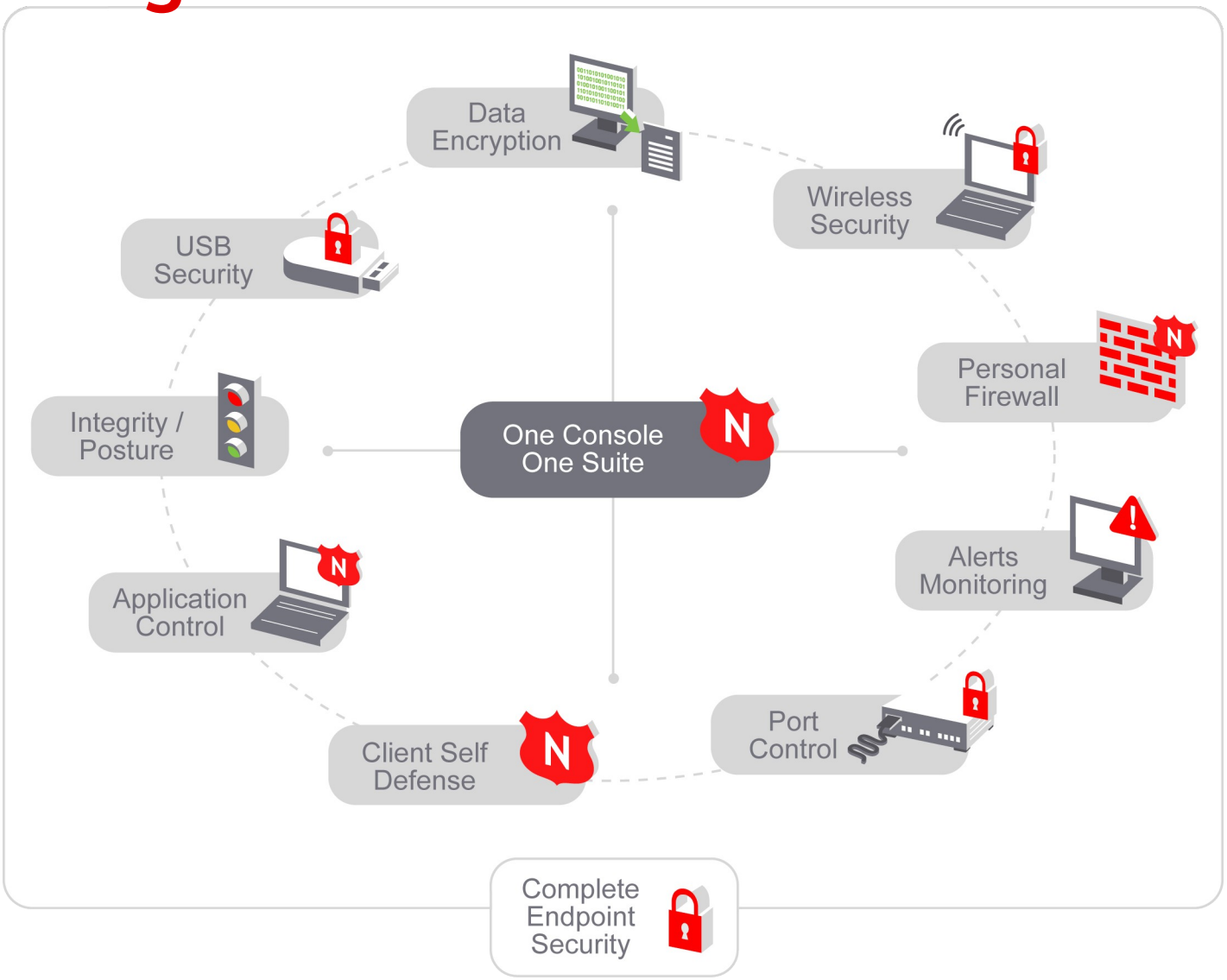
Novell®

O que é o ZENworks Endpoint Security Management?

- Segurança completa e centralizada para todos os dispositivos de ponto a ponto da rede
  - Protege os dados
  - Melhora a saúde do sistema e a produtividade dos usuários
  - Ajuda a atender a requisitos normativos

- A segurança de ponto a ponto tem como alvo as violações de dados comuns
  - Equipamentos perdidos ou roubados
  - Arquivos usados por terceiros
  - Sistemas violados, usuários mal-intencionados
  - Código mal-intencionado
  - Mídia removível
  - Conexões sem fio

ZENworks Endpoint Security Management

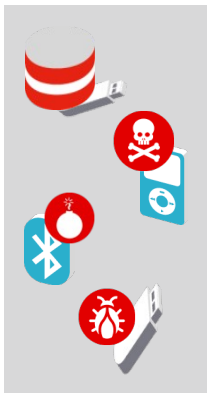


Por que seus clientes precisam da segurança de ponto a ponto?

- A maioria dos novos dados está nos dispositivos de ponto a ponto

- Os dispositivos móveis nem sempre estão protegidos pela segurança de perímetro e podem acessar redes que talvez não sejam seguras

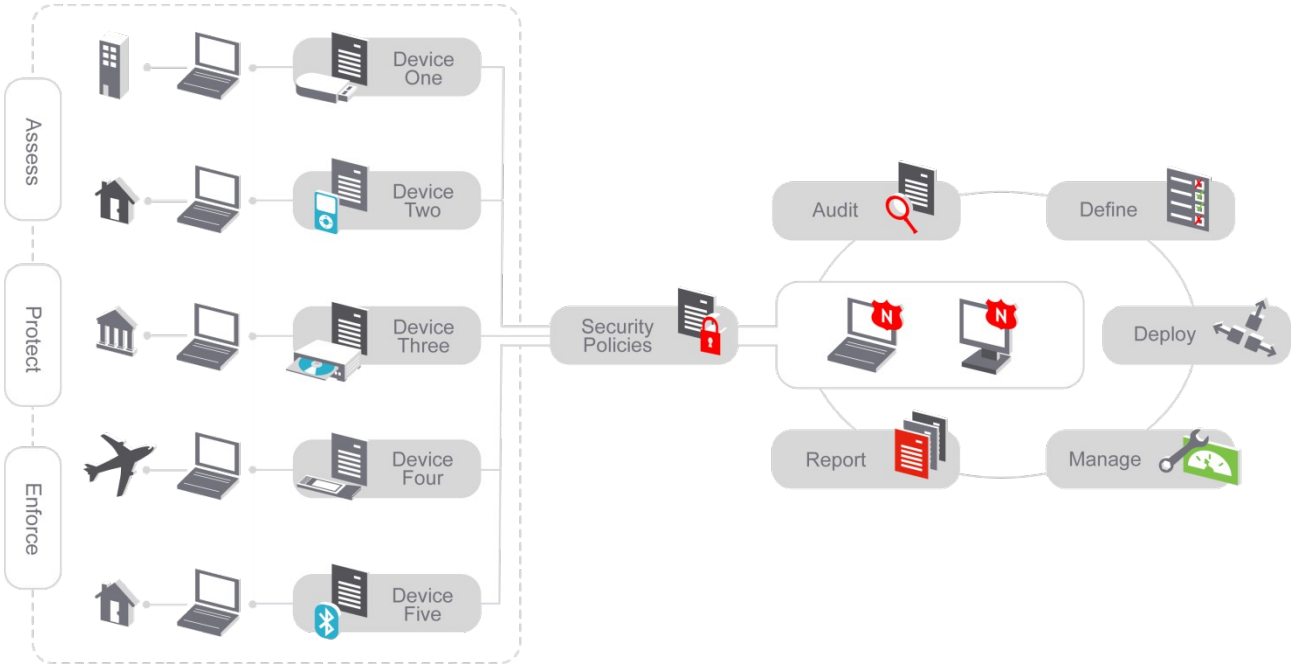
- As redes sem fio são abertas e/ou podem ser facilmente invadidas



- Os dispositivos de ponto a ponto de armazenamento em massa podem ser usados para copiar grandes volumes de dados do dispositivo
- Novas vulnerabilidades incluem o pod slurping e o thumbsucking (apropriação ilícita de dados por meio de iPods e dispositivos USB), o snarfing (roubo de arquivos ou identidades por meio de Bluetooth) e outros

Framework – Baseado em Localização

- Localização
- Regras específicas
- O ambiente da rede determina a localização



Características

1. Gerenciamento de Dispositivos de Armazenamento

- Desabilitar ou tornar acesso readonly para dispositivos de armazenamento removíveis como USB, iPods, Floppies e drives de CD/DVD
- Reportar o que foi escrito nesses dispositivos ou acessado à partir deles.

Características

2. Gerenciamento de Segurança de Wifi

- Desabilitar wireless, desabilitar wireless quando estiver na rede cabeada, desabilitar redes ad hoc
- Travar acesso a rede wireless por SSID, MAC, adaptador wireless.
- Gerenciar wireless WEP
- Configurar um mínimo de segurança requerido (sem criptografia, WEP 64, WEP 128, WPA)

Características

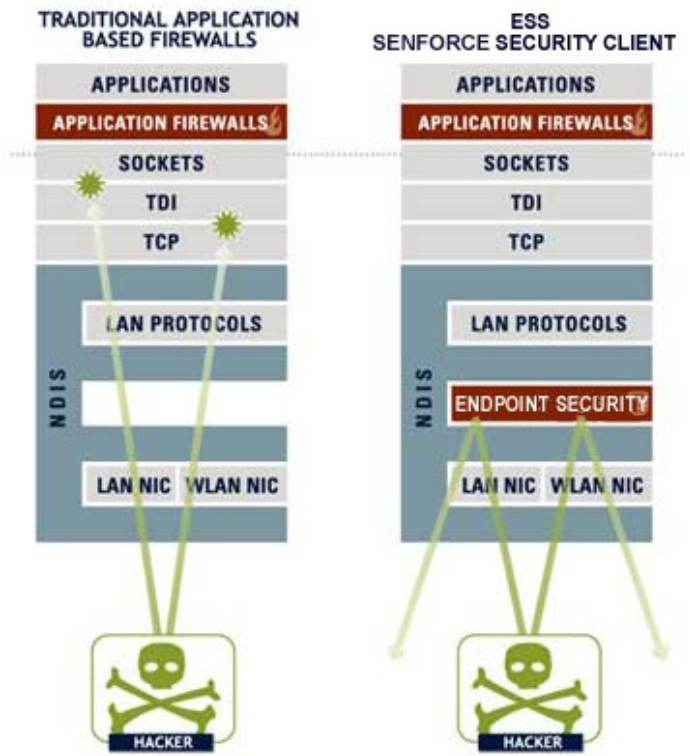
3. Enforcement do Uso da VPN para usuários Remotos

- Forçar o carregamento automático do software de VPN quando a máquina estiver for a do escritório
- Dados são encapsulados e criptografados para transmissão
- Tunneling completo e travamento das configurações do cliente para garantir que todo dado esteja protegido.

Características

4. Firewall Pessoal

- Firewall stateful de camada NDIS (integração com o driver)
- Protege contra ataques de exploit de protocolos
- Access Control Lists (ACLs) para ambientes confiáveis
- Configurações do Firewall controladas centralmente e propagadas rapidamente.
- Pode ser ajustado por localidade
- Não pode ser desligado pelo usuário (Mesmo usuários Administradores da estação)



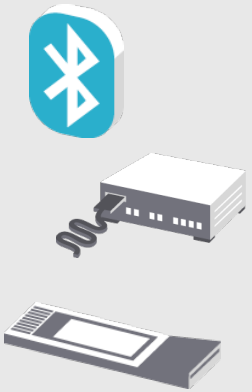
Características

5. Gerenciamento e Bloqueio de Aplicações

- Bloquear execução de aplicativos
- Bloquear aplicações rodadas à partir da rede
- Controle por localidade

6. Gerenciamento de Hardware de Comunicação

- Desabilita dispositivos por localidade
  - IrDA
  - Bluetooth
  - 1394 (Firewire)
  - Serial/Parallel ports



Sua oportunidade de mercado

- Os mercados do gerenciamento de mudanças e configurações (CCM) e do gerenciamento de segurança deverão crescer para **mais de US$ 5 bilhões** em 2010
  - Os principais estimuladores de mercado são a simplificação, o custo e a maximização do valor dos ativos de TI
  - Os novos estimuladores incluem a proteção de ponto a ponto contra o roubo de dados e a conformidade corporativa e normativa
- O público-alvo é a empresa de médio porte, com 100 a 5.000 funcionários ou mais
  - Mercados verticais nos setores governamental, educacional, de saúde, financeiro e de manufatura

Fonte: IDC 2006/2007, documentos 205437, 203294, 202880, 204693

Perguntas de qualificação

- Seu cliente…
  - Precisa evitar a perda de dados de dispositivos portáteis roubados ou perdidos?
  - Preocupa-se com funcionários que levam para casa dados confidenciais da empresa?
  - Armazena dados da empresa em unidades portáteis, iPods e outros dispositivos removíveis?
  - Usa conexões sem fio para funcionários móveis?
  - Sabe quais softwares estão instalados nos computadores dos funcionários?
  - Precisa que os funcionários móveis façam suas próprias atualizações de segurança?
  - Precisa atender a normas de segurança corporativas ou governamentais?
  - Deseja simplificar o gerenciamento de dispositivos de ponto a ponto do Windows?

O que o ZENworks Endpoint Security Management inclui?

Recursos

- Firewall avançado
- Uso obrigatório da VPN
- Sem fio
- Bluetooth
- Controle de acesso à rede
- Segurança de USB
- Armazenamento removível
- Criptografia
- Relatórios de conformidade
- Uso obrigatório de políticas
- Controle de aplicativos
- Autodefesa

Benefícios

- Reforço da segurança de ponto a ponto *em tempo real*
- *Alta* proteção contra ataques
- Segurança *sensível a contexto*, fora ou dentro da rede
- *Diretório* corporativo integrado, segurança de acordo com as necessidades dos usuários
- Gerenciamento centralizado
- Reforço 360 *abrangente*
- *Conformidade* predefinida
- *Facilidade* de distribuição

Quais são as necessidades ou os problemas comerciais do cliente?

- Gerenciar, controlar e reforçar a segurança de ponto a ponto
  - Inclua armazenamento removível, comunicações sem fio, controle de aplicativos, condição e integridade das máquinas, criptografia de dados e firewalls pessoais
- Proteger os dados corporativos contra hackers, malware, ataques de protocolo e roubo
  - Simplifique a segurança de ponto a ponto
  - Reduza os custos de TI
- Melhorar a conformidade com normas corporativas, industriais e governamentais

Reforçar a segurança de dispositivos de ponto a ponto

- O ZENworks Endpoint Security Management pode:
  - Bloquear a execução de arquivos de dispositivos de armazenamento em nível de driver
    - Desabilitar ou definir como “apenas leitura” os dispositivos de armazenamento removíveis (unidades USB portáteis, iPods, disquetes, etc.) e gravadores ópticos (unidades de CD/DVD)
    - Manter uma trilha de auditoria dos arquivos que são gravados em armazenamento removível
  - Proteger os dados com criptografia baseada em arquivo e segurança de dados em movimento que permanece com o arquivo
  - Bloquear o acesso sem fio por ID de adaptador
  - Definir requisitos mínimos de segurança para o acesso sem fio
  - Impedir que os usuários desativem o firewall pessoal
- Como resultado, os clientes podem:
  - Reduzir os gastos de TI com questões de segurança tática
  - Manter os sistemas de TI funcionando bem e os usuários produtivos impedindo ataques aos dados

Proteger os dados corporativos

- Simplifique o gerenciamento da segurança e reduza os custos de TI com um único console
- Proteja os dados no escritório, em casa e durante viagens com tecnologia que reconhece a localização
  - Assegure o uso obrigatório da VPN quando o dispositivo estiver fora do escritório
  - Controle o acesso à rede de dispositivos sem fio e portáteis
  - Encapsule e criptografe todos os dados antes da transmissão
  - Desabilite dispositivos pela localização, dentro ou fora da rede corporativa
- Bloqueie a execução ou o acesso à rede de aplicativos não autorizados
  - Controle o tráfego da rede com um firewall com informações de estado e baseado em sessão
  - Centralize as definições de políticas e publique-as em toda a organização via serviços de diretório (eDirectory, Active Directory, LDAP)
- Use procedimentos padrão automatizados para lidar com as ameaças de hackers, malware, ataques de protocolo e roubo

Melhorar a conformidade com normas

- Proteja informações confidenciais sobre pacientes, parceiros comerciais e clientes
  - Defina decisões sobre segurança para a organização inteira
  - Use políticas baseadas em diretório para padronizar os procedimentos para lidar com ameaças
  - Obtenha reforço da segurança e reparo 24x7, independentemente da localização ou do estado da conexão
  - Transmita, armazene e oculte políticas de segurança usando criptografia para impedir ataques
  - Impeça que funcionários descontentes burlem as medidas de segurança
- Torne o antivírus, a aplicação de patches para o Windows ou outros softwares uma exigência para os dispositivos não-compatíveis
  - Coloque dispositivos em quarentena (bloqueie o acesso à rede) até que os requisitos sejam atendidos
- Demonstre a conformidade com normas produzindo relatórios detalhados e auditáveis

Resumo do ZENworks Endpoint Security Management

1

- Reforçar a segurança de dispositivos de ponto a ponto
  - Permita mais agilidade e produtividade enquanto gerencia os riscos associados
  - Reduza a sobrecarga com um único console para configuração, gerenciamento e relatórios/alertas

2

- Proteger os dados corporativos armazenados em dispositivos de ponto a ponto
  - Proteja a saúde do sistema para aumentar o tempo ativo e a produtividade dos usuários

3

- Melhorar a conformidade com normas
  - Defina decisões de segurança centralmente para toda a organização a fim de que seu uso obrigatório não possa ser contornado
  - Forneça provas de conformidade documentadas


Novell®