kaspersky

Kaspersky® Endpoint Security for Business

Select

Ready for GDPR

O **Kaspersky Endpoint Security for Business Select** oferece a proteção baseada em HuMachine™ para diversas plataformas, inclusive servidores e endpoints Linux. Ele fornece segurança em vários níveis que detecta comportamentos suspeitos e bloqueia ameaças, inclusive ransomware. Os controles baseados em nuvem reduzem sua exposição a ataques, e os recursos de gerenciamento móvel ajudam a proteger dados em plataformas móveis.

As funcionalidades de proteção e gerenciamento de que você precisa

A Kaspersky Lab incorporou avançados recursos de nível corporativo nos níveis progressivos de nossas ofertas. Nós garantimos que a tecnologia seja descomplicada e flexível suficiente para ser usada por empresas de qualquer tamanho.

Qual é o nível certo para você?

- **SELECT**
- ADVANCED
- TOTAL

Varios níveis de proteção para

- Windows, Linux e Mac
- Servidores Windows e Linux
- Android e outros dispositivos móveis
- Armazenamentos removíveis

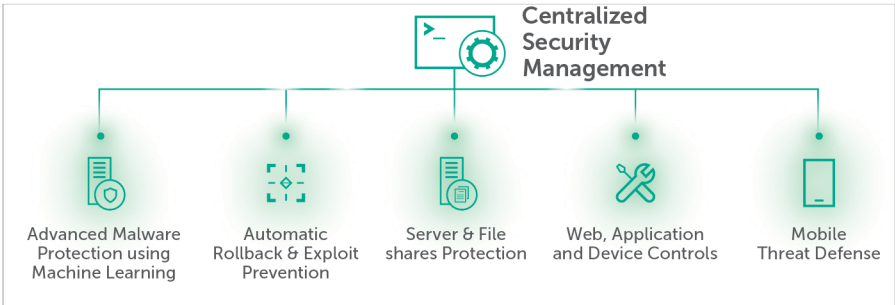
Segurança inigualável contra

- Exploits de software
- Ransomware
- Malware para dispositivos móveis
- Ameaças avançadas
- Ameaças sem arquivo
- Ataques baseados em PowerShell e em scripts
- Ameaças da Web

Recursos incluídos

- Antimalware próximo nível
- Avaliação de Vulnerabilidades
- Consultor de políticas de segurança
- Aprendizado baseado em IA
- Suporte a AMSI novo
- Verificação do tráfego criptografado novo
- Isolamento de processos
- Prevenção e reversão de exploits
- Firewall e gerenciamento do firewall do sistema operacional
- Proteção assistida na nuvem
- Agente de EDR integrado
- Integração com SIEMs via Syslog novo
- Controle de Aplicativos
- Controle da Web e de Dispositivos
- Proteção de servidores e contêineres próximo nível
- Suporte ao subsistema Linux no Windows novo
- Defesa contra ameaças em dispositivos móveis próximo nível
- Geração de relatórios

Veja mais detalhes em nossas páginas da Web aqui.



Proteção e controle da próxima geração para todos os endpoints

Um único console de gerenciamento

No console de gerenciamento com 'exibição única', os administradores podem ver e gerenciar todo o cenário da segurança e aplicar as políticas de segurança escolhidas a cada endpoint de sua empresa. Isso ajuda na rápida implementação da segurança e com o mínimo de interrupção ou inconvenientes, usando a ampla variedade de cenários pré-configurados.

Segurança adaptativa ágil

O produto foi criado para funcionar em qualquer ambiente de TI. Ele emprega uma pilha completa de tecnologias comprovadas da próxima geração e para evitar ataques detectados; os sensores internos e a integração com o Endpoint Detection and Response (EDR) permitem a captura de grandes volumes de dados para descobrir até os ataques mais obscuros e sofisticados.

Garantia de satisfação do cliente

Com nosso foco intenso em pesquisa e desenvolvimento, nossos produtos fornecem a segurança de que você precisa. Tomadores de decisão como você sempre expressam níveis incríveis de satisfação com os resultados obtidos, o que é confirmado regularmente por pesquisas e relatórios independentes.

Principais recursos

Principais recursos

Prevenção de exploits
Impede a execução de malware e a exploração de software, proporcionando uma camada extra de proteção contra ameaças desconhecidas de "dia zero".

Detecção de comportamento e reversão automática
Identifica e protege contra ameaças avançadas, incluindo ransomware, ataques sem arquivo e tomada do controle de contas de administrador. A detecção de comportamento bloqueia ataques, enquanto a reversão automática desfaz todas as alterações já realizadas.

Proteção contra criptografia de pastas compartilhadas
Um mecanismo anti-cryptor exclusivo é capaz de bloquear a criptografia de arquivos em recursos compartilhados realizada por um processo malicioso em execução em outra máquina na mesma rede.

Proteção contra ameaças à rede
Um malware que usa um ataque de saturação de buffer pode modificar um processo em execução na memória e, dessa forma, executar um código malicioso. A proteção contra ameaças à rede identifica ataques de rede e os bloqueia totalmente.

Console da Web
Para aprimorar a tolerância a falhas, você pode implementar nosso console da Web para gerenciar centralmente as máquinas físicas e virtuais, não apenas no ambiente de nuvem da Amazon, mas também do Microsoft Azure.

Recursos de segurança móvel

Tecnologia antimalware inovadoras
A associação de detecção baseada em ML, proativa e em nuvem resulta na proteção em tempo real. Proteção da Web, verificações sob demanda e programadas reforçam a segurança.

Implementação com provisionamento por conexão sem fio (OTA)
Permite pré-configurar e implementar aplicativos de maneira centralizada usando SMS, e-mail e o PC.

Ferramentas antirroubo remotas
Verificação do Chip, Bloqueio, Limpeza e Localização Remotos evitam o acesso não autorizado a dados corporativos, caso um dispositivo móvel seja roubado ou perdido.

Controle de aplicativos para dispositivos móveis
O controle de aplicativos protege dados sobre os softwares instalados e permite que os administradores imponham a instalação e o uso de aplicativos específicos.

Controles de endpoints na nuvem

Controle de Aplicativos
Reduz sua exposição a ataques, proporcionando controle total sobre quais softwares podem ser executados nos PCs e quando isso pode ser feito, com base nas listas brancas dinâmicas de nosso laboratório interno. Suporte a cenários de Permissão e Negação Padrão.

Listas brancas dinâmicas
Para melhorar a categorização de aplicativos, o Controle de Aplicativos usa um banco de dados de listas brancas dinâmicas desenvolvido pela Kaspersky Lab com base na sistematização do conhecimento de softwares legítimos.

Controle de dispositivos
Esse recurso permite que os usuários definam, programem e imponham políticas de dados que controlam armazenamentos removíveis e outros dispositivos periféricos, conectados a USB ou a qualquer outro tipo de barramento.

Sistema de Prevenção de Invasões Baseado em Host (HIPS)
Restringe o acesso a dados confidenciais e dispositivos de gravação usando bancos de dados de reputação locais e na nuvem (Kaspersky Security Network) sem afetar o desempenho de aplicativos autorizados.

Suporte e serviços profissionais

Você tem acesso à ajuda de profissionais sempre que precisa. Operando em mais de 200 países, com 34 escritórios em todo o mundo, oferecemos suporte 24 horas por dia, 7 dias por semana, 365 dias por ano. Aproveite nossos pacotes de suporte premium (MSA) ou ligue para nossa equipe de serviços profissionais para aproveitar ao máximo e alcançar o melhor retorno sobre o investimento na instalação da segurança da Kaspersky Lab.

Veja você mesmo

Experimente a True Cybersecurity pessoalmente! Acesse esta página **para fazer a avaliação da versão completa** do Kaspersky Endpoint Security for Business.

Kaspersky Lab
Encontre um parceiro perto de você: www.kaspersky.com/buyoffline
Kaspersky para empresas: www.kaspersky.com/business
Notícias sobre segurança de TI: business.kaspersky.com/
Nossa abordagem exclusiva: www.kaspersky.com/true-cybersecurity

www.kaspersky.com