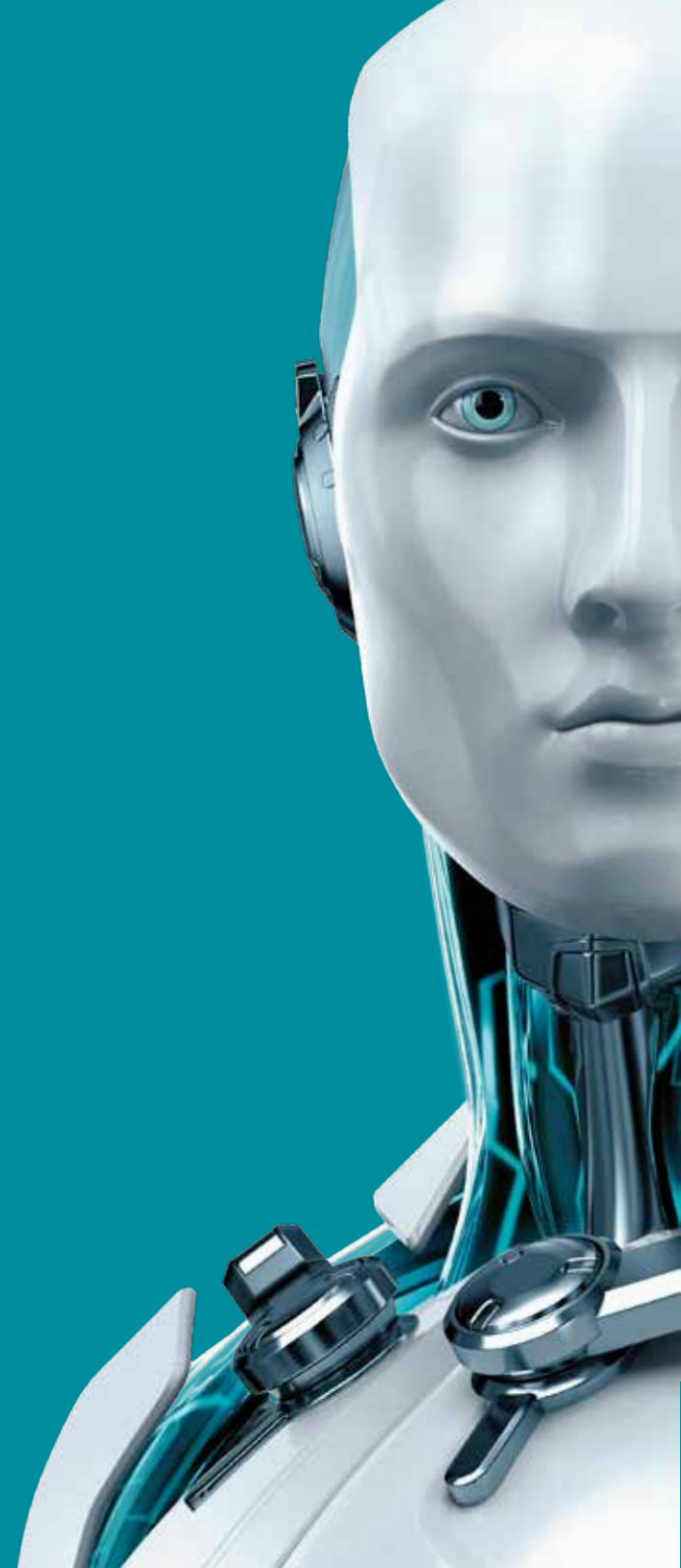
SECURITY

PARA MICROSOFT SHAREPOINT SERVER

30 ANOS DE INOVAÇÃO CONTÍNUA EM SEGURANÇA

BUSINESS

ENJOY SAFER TECHNOLOGY™



SECURITY
PARA MICROSOFT SHAREPOINT SERVER

Mantenha o SharePoint limpo, escaneando arquivos dentro da base de dados de SharePoint. Fornece proteção de servidor completa.

Previne que ameaças maliciosas e usuários não autorizados achem brechas na segurança do sistema e é totalmente gerenciável através do Administrador Remoto 6 ESET.

Versões de SharePoint suportadas:

Microsoft SharePoint Server 2016

Microsoft SharePoint Server 2013

Microsoft SharePoint Server 2010

Microsoft SharePoint Enterprise 2010

Microsoft Office SharePoint Server 2007

Proteção de SharePoint Server

Antivírus e antispyware	Elimine todos os tipos de ameaças, incluindo vírus, rootkits, worms e spyware. **Escaneamento opcional na nuvem:** Listas brancas de arquivos seguros de acordo com a base de dados de reputação de arquivo na nuvem para melhor detecção e escaneamento mais rápido. Apenas informação sobre arquivos executáveis e arquiváveis é enviada para a nuvem – tais dados não são pessoalmente atribuíveis.
Escaneamento de banco de dados	O administrador pode decidir rodar um escaneamento meticuloso da base de dados em horários fora do pico, automatizar a limpeza no devido local e reforçar a inspeção de vários documentos ou versões de objetos em qualquer site de SharePoint disponível. As consultas na base de dados podem ser paralelizadas em múltiplas linhas de escaneamento para melhorar de forma significativa o tempo de escaneamento por demanda.
Regras de objetos da base de dados	Tanto para o escaneamento por demanda quanto para o escaneamento por acesso um conjunto separado de decisões lógicas está disponível e pode lidar com atributos que variam desde tamanho do arquivo ou conteúdo real do objeto escaneado até inspeção de arquivo; permite customizações ilimitadas por qualquer cadeia de regras desejada e ações subsequentes para executá-las.
Suporte de Virtualização	O Cache Local Compartilhado da ESET armazena metadados de arquivos já escaneados dentro do ambiente virtual, de modo que arquivos idênticos não sejam escaneados novamente, resultando na melhoria da velocidade do escaneamento. As atualizações de módulo da ESET e a base de dados de assinaturas de vírus são armazenadas fora da localização padrão, de modo que elas não tenham que ser baixadas todas as vezes que uma máquina virtual for revertida para o snapshot padrão.
Bloqueador de Exploit	Fortalece a segurança dos aplicativos como navegadores de web, leitores de PDF, clientes de e-mail e componentes Microsoft Office que podem comumente sofrer exploits. Monitora comportamentos de processos e procura por atividades suspeitas típicas de exploits. Fortalece a proteção contra ataques direcionados e exploits previamente desconhecidos, por exemplo, ataques de dia zero.
Escaneador de Memória Avançado	Monitora o comportamento de processos maliciosos e os escaneia uma vez que apareçam na memória. Isso permite prevenção efetiva contra infecção, mesmo de um malware demasiadamente ofuscado.
Suporte de Cluster Nativo	Permite que você configure a solução para replicar automaticamente as configurações quando instaladas em um ambiente de cluster. Nosso assistente de instalação intuitivo torna fácil a interconexão de diversos nós instalados do ESET Security para MS SharePoint dentro de um cluster e os gerencia como um, eliminando a necessidade de replicar mudanças na configuração manualmente para outros nós no cluster.
Escaneamento de armazenagem	Permite que você facilmente programe escaneamentos por demanda do Armazenamento de Anexos de Rede (NAS). Combinado com o Cache Local Compartilhado da ESET instalado dentro da rede, isso pode reduzir drasticamente a quantidade de operações de entrada/saída nos drives da rede.

Proteção ao acesso de dados

Anti-Phishing	Protege contra as tentativas de falsos websites em adquirir informação sensível.
Controle de equipamento	Bloqueia aparelhos portáteis não autorizados de se conectar a seu servidor. Permite que você crie regras para que grupos de usuários cumpram com as políticas da sua empresa. Bloqueio moderado – notifica o usuário final que seu aparelho foi bloqueado e dá a opção de acessá-lo com o registro de atividade.

Opções de escaneamento e atualização

Escaneamento em estado ocioso	Auxilia na performance do sistema fazendo um escaneamento total proativamente quando o computador não está em uso. Ajuda a acelerar escaneamentos subsequentes preenchendo o cache local.
Reversão de atualização	Permite que você reverta a versão anterior dos módulos de proteção e a base de dados de assinatura de vírus. Permite que você congele as atualizações como desejar – opte por reversão temporária ou adiamento até as mudanças serem feitas de forma manual.
Atualizações adiadas	Proporciona a opção de download a partir de três servidores especializados em atualização: pré-lançamento (usuários beta), lançamento regular (recomendado para sistemas não críticos) e lançamento adiado (recomendado para empresas com sistemas críticos – aproximadamente 12 horas depois do lançamento regular).
Servidor de atualização local	Economiza a banda larga da empresa baixando as atualizações apenas uma vez para um servidor espelho local. A força de trabalho móvel faz a atualização diretamente do ESET Update Server quando o espelho local não está disponível. O canal de comunicação seguro (HTPPS) é suportado.

SUPORTE TÉCNICO LOCAL GRÁTIS

Faça mais com a ajuda de nossos especialistas. De plantão para fornecer suporte técnico quando você precisar, em seu idioma.

Usabilidade

Exclusões do processo	O administrador pode definir processos que são ignorados pelo módulo de proteção em tempo real – todas as operações de arquivo que podem ser atribuídas a esses processos privilegiados são consideradas seguras. Isso é especialmente útil para processos que frequentemente interferem na proteção em tempo real, como o backup e a migração ao vivo da máquina virtual. O processo excluído pode acessar até mesmo arquivos ou objetos não seguros sem dar alertas.
Provedor de Instrumentação de Gerenciamento de Windows (WMI)	Proporciona a possibilidade de monitorar funcionalidades chave do ESET Server Security através da estrutura da Instrumentação de Gerenciamento de Windows. Isso permite a integração do ESET Server Security em um gerenciamento terceirizado e em um software de Gerenciamento e Correlação de Eventos de Segurança (SIEM), como o Microsoft System Center Operations Manager, o Nagios, entre outros.
Visibilidade da Interface Gráfica do Usuário (GUI) Customizável	A visibilidade da Interface Gráfica do Usuário (GUI) para usuário final pode ser programada para Completa ou Terminal. Escondendo a Interface Gráfica do Usuário completamente, o processo "egui.exe" não roda de forma alguma, resultando em um consumo de sistema ainda mais baixo pela solução da ESET.
Administrador de Licenças ESET	Torna possível lidar com todas as licenças de forma transparente, de um único lugar com o navegador da web. Você pode combinar, delegar e gerenciar todas as licenças centralmente em tempo real, mesmo se você não estiver usando o Administrador Remoto.
Instalação baseada em componentes	Permite que você escolha quais componentes instalar: – Proteção de Sistema de Arquivo em Tempo Real – Web e e-mail – Controle do aparelho – Interface Gráfica do Usuário (GUI) – Coletor de logs ESET – ESET SysInspector – Ajuda off-line
Gerenciamento Remoto	As soluções de servidor da ESET são totalmente gerenciáveis através do Administrador Remoto ESET. Instale, rode tarefas, determine políticas, colete logs, obtenha notificações e um panorama geral da segurança de sua rede – tudo através de um único console gerenciado via web.
Coletor de Logs ESET	Uma ferramenta simples que coleta todos os logs relevantes para solução de problemas, assistida pelo suporte técnico da ESET e que os agrupa em um único arquivo que pode ser enviado por e-mail ou colocado em um drive de rede compartilhada para acelerar o processo de solução de problemas.