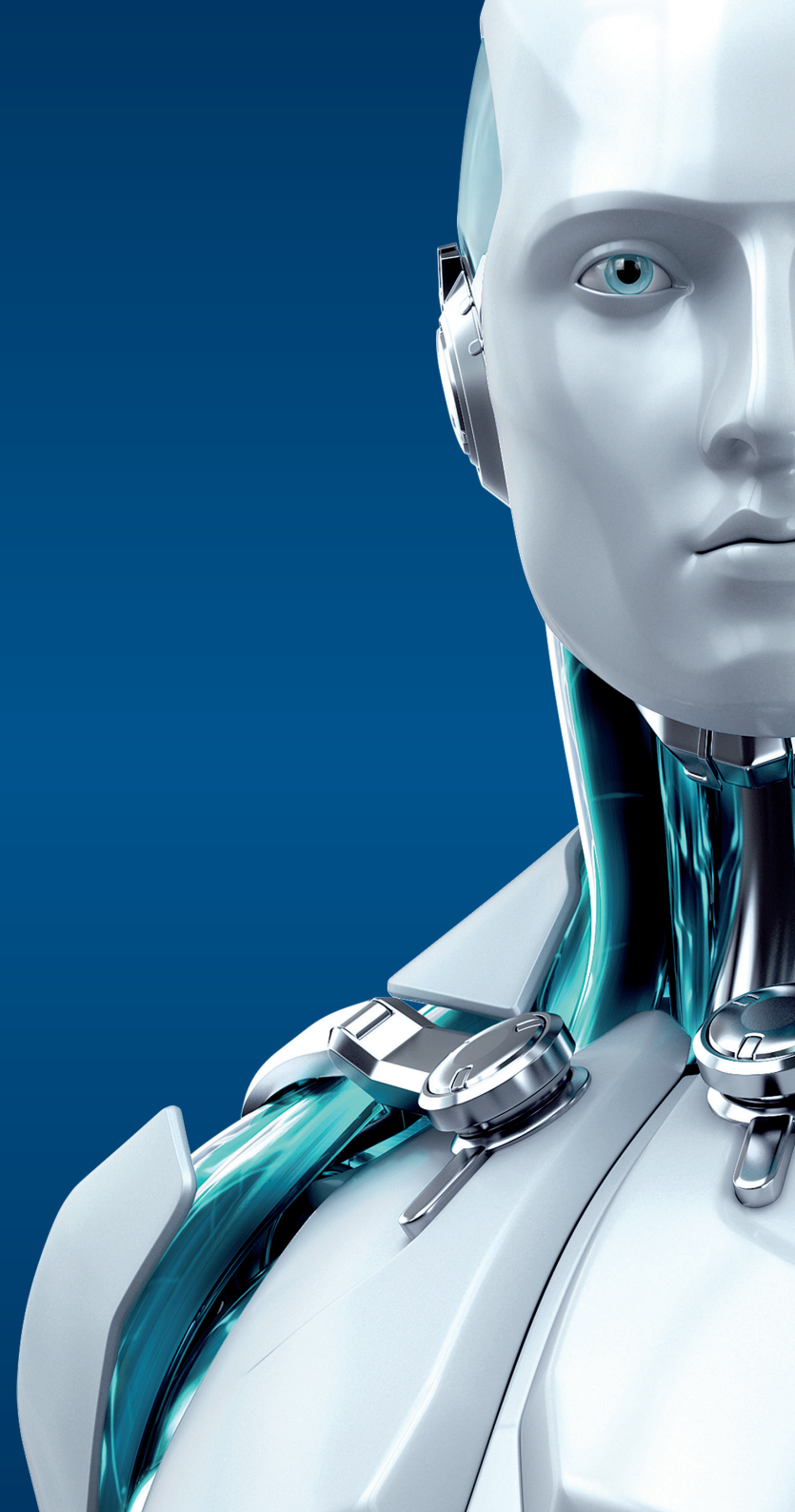




ENDPOINT SECURITY

FOR ANDROID

ENJOY SAFER TECHNOLOGY™





ENDPOINT SECURITY FOR ANDROID

O ESET Endpoint Security for Android protege a força de trabalho móvel da sua empresa com a tecnologia proactiva do ESET NOD32®.

Analisa todas as aplicações, ficheiros e cartões de memória em busca de malware. O sistema anti-roubo protege os dispositivos que podem ser remotamente bloqueados ou limpos em caso de perda ou roubo. Os utilizadores são ainda poupados de chamadas e SMS indesejadas e os administradores de sistemas podem aplicar políticas de segurança a todos os dispositivos, de modo a que sejam cumpridas as políticas da empresa.

Protecção de Endpoints

Protecção em Tempo Real	Protege todas as aplicações e ficheiros em tempo real utilizando a tecnologia proactiva ESET NOD32®, optimizada para plataformas móveis. O sistema avançado ESET LiveGrid®, juntamente com as funcionalidades avançadas de análise, protege os smartphones e os tablets da empresa.
Análise a Pedido	Analisa e remove ameaças presentes na memória integrada e nos sistemas de armazenamento. A análise corre em segundo plano e pode ser colocada em pausa pelo utilizador. É possível definir também o tempo exacto para executar uma análise.
Análise no Carregamento	Permite que uma análise total seja efectuada enquanto o dispositivo está a carregar
Anti-Phishing	Protege os utilizadores contra tentativas de aquisição de palavras-passe, dados bancários e outras informações sensíveis por parte de sites falsos.
Protecção contra remoção	Previne que a aplicação seja removida sem password de administração
Filtro de Chamadas e SMS	Protege os utilizadores de chamadas indesejadas e SMS a partir de números desconhecidos, contactos seleccionados ou durante períodos de tempo pré-definidos.

Segurança dos Dispositivos

Dá ao administrador a opção de executar políticas de segurança básicas em toda a força de dispositivos móveis. A aplicação notifica automaticamente o utilizador caso as definições do dispositivo não estejam em conformidade com as políticas de segurança da empresa e sugere alterações a implementar.

Definições de Segurança do Dispositivo	Defina o nível de segurança mínimo (Password, PIN, Padrão) e defina os requisitos de complexidade da palavra-passe. Defina o número máximo de tentativas falhadas de desbloqueio após as quais o dispositivo assume automaticamente os valores de fábrica. Defina quando o código do ecrã de bloqueio expira Defina o temporizador do ecrã de bloqueio Solicite aos utilizadores que encriptem os seus dispositivos móveis Bloquee a utilização da câmara integrada
---	--

Política de Definições do Dispositivo – permite aos administradores verificarem as definições predefinidas de um dispositivo para determinarem se estão em concordância com as políticas da empresa. Os administradores podem verificar a utilização de memória, a ligação Wi-Fi, as chamadas, as aplicações instaladas a partir de fontes desconhecidas para além da loja Google Play e muito mais.

Anti-Roubo

Comandos Remotos	Todos os comandos remotos podem ser activados através do ESET Remote Administrator, por SMS com autenticação de dois factores, ou através da interface do administrador. - especialmente útil para empresas que não estão a usar gestão remota ou quando o administrador não está presente.
Bloqueio Remoto	Bloqueia remotamente os dispositivos perdidos ou roubados. Após o bloqueio, nenhum utilizador não autorizado conseguirá aceder aos dados armazenados no dispositivo. Quanto o dispositivo é encontrado, um comando remoto desbloqueia-o para que possa voltar a ser utilizado.
Localização Remota	Localize remotamente o dispositivo e segue as coordenadas GPS.
Remote Wipe	Elimina com segurança todos os contactos, mensagens e dados armazenados na memória interna do dispositivo, e nos dispositivos amovíveis. Os processos avançados de limpeza asseguram que não é possível restaurar os dados eliminados. Após a limpeza remota, o ESET Endpoint Security for Android continua instalado no dispositivo, por isso é possível executar-se novos comandos Anti-Roubo.
Sirene Remota	Quando activado, uma sirene soa no dispositivo, mesmo que esteja em modo silencioso. O dispositivo em falta é ainda bloqueado automaticamente.
Restauro das Definições de Fábrica	Remove todos os dados disponíveis no dispositivo ao destruir os ficheiros e ao restaurarem o dispositivo para as definições de fábrica.
Mensagem Personalizada	O Administrador pode enviar uma mensagem personalizada a um determinado utilizador ou a um grupo de utilizadores.
Informações no Ecrã de Bloqueio	O administrador pode definir dados personalizados (nome da empresa, email, mensagem) a serem mostrados quando o telefone está bloqueado.
Sim Correcto	Quando um cartão SIM não autorizado é inserido, o dispositivo é automaticamente bloqueado e as informações enviadas ao administrador.
Contactos de Administração	Contém uma lista de números de telefones de administração protegida por password. Os comandos SMS para controlar o dispositivo só podem ser enviados a partir desses números de confiança. Para além disso esses números são usados para notificações ligadas às acções Anti-Roubo.



O Suporte técnico gratuito no seu idioma e o know how da ESET garantem que poderá contar com uma equipa dedicada de especialistas que o vão ajudar a ultrapassar quaisquer questões que surgirem aquando da instalação ou utilização das nossas soluções.

Controlo de Aplicações

Permite aos administradores verificarem as aplicações instaladas, bloquearem o acesso às mesmas e ainda solicitarem a remoção de determinados programas em particular.

Controlo de Aplicações	Defina manualmente as aplicações a bloquear Bloquear por categoria - jogos, redes sociais Bloquear por permissões – aplicações que registem a localização ou acedam à lista de contactos Bloquear por fonte – aplicações instaladas a partir de lojas de aplicações alternativas Definir excepções à regra – whitelist de aplicações Definir uma lista de aplicações mandatórias para cada dispositivo
Auditoria de Aplicações	Verifica as aplicações e o acesso a dados pessoais e empresariais, permitindo ao administrador monitorizar e controlar as permissões.

Facilidade de Utilização

Importação/Exportação de definições	Se os dispositivos móveis não forem geridos pelo ESET Remote Administrator, os administradores de sistema podem partilhar facilmente as definições de um dispositivo para outro, exportando-as para um ficheiro e importando-as para onde desejarem.
Centro de Notificações	Os utilizadores podem aceder a todas as notificações num único local, juntamente com instruções de como resolverem o problema. Isto torna simples garantir o cumprimento das regras das empresas.
Administração local	Os administradores podem configurar e gerir o dispositivo localmente mesmo que a empresa não use o ESET Remote Administrator. Todas as definições das aplicações são protegidas por uma password de administração, mantendo a segurança sob controlo.
Identificação Melhorada do Dispositivo	Durante o processo de adesão de dispositivos, os mesmos são colocados numa lista de permissão de modo a que apenas os dispositivos autorizados se possam ligar ao ESET Remote Administrator. Isto simplifica a identificação individual de dispositivos - por nome, descrição e IMEI.
Assistentes de Configuração Passo-a-Passo	Os assistentes de configuração passo-a-passo após a instalação estão disponíveis para a configuração de funcionalidades seleccionadas, tornando simples todo o processo.
Gestão Remota	As soluções ESET Endpoint são totalmente geríveis através do ESET Remote Administrator. Faça o deployment, execute tarefas, defina políticas, junte relatórios, obtenha notificações e no fundo um visão geral da segurança da sua rede - tudo através de uma única consola de gestão baseada na web.
Administrador de Licenças ESET	Torna possível a gestão transparente das licenças, a partir de um único local, via browser web. Pode agregar, delegar e gerir todas as licenças a nível local em tempo real, mesmo que não esteja a utilizar o ESET Remote Administrator.

Copyright © 1992 – 2015 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2008.