

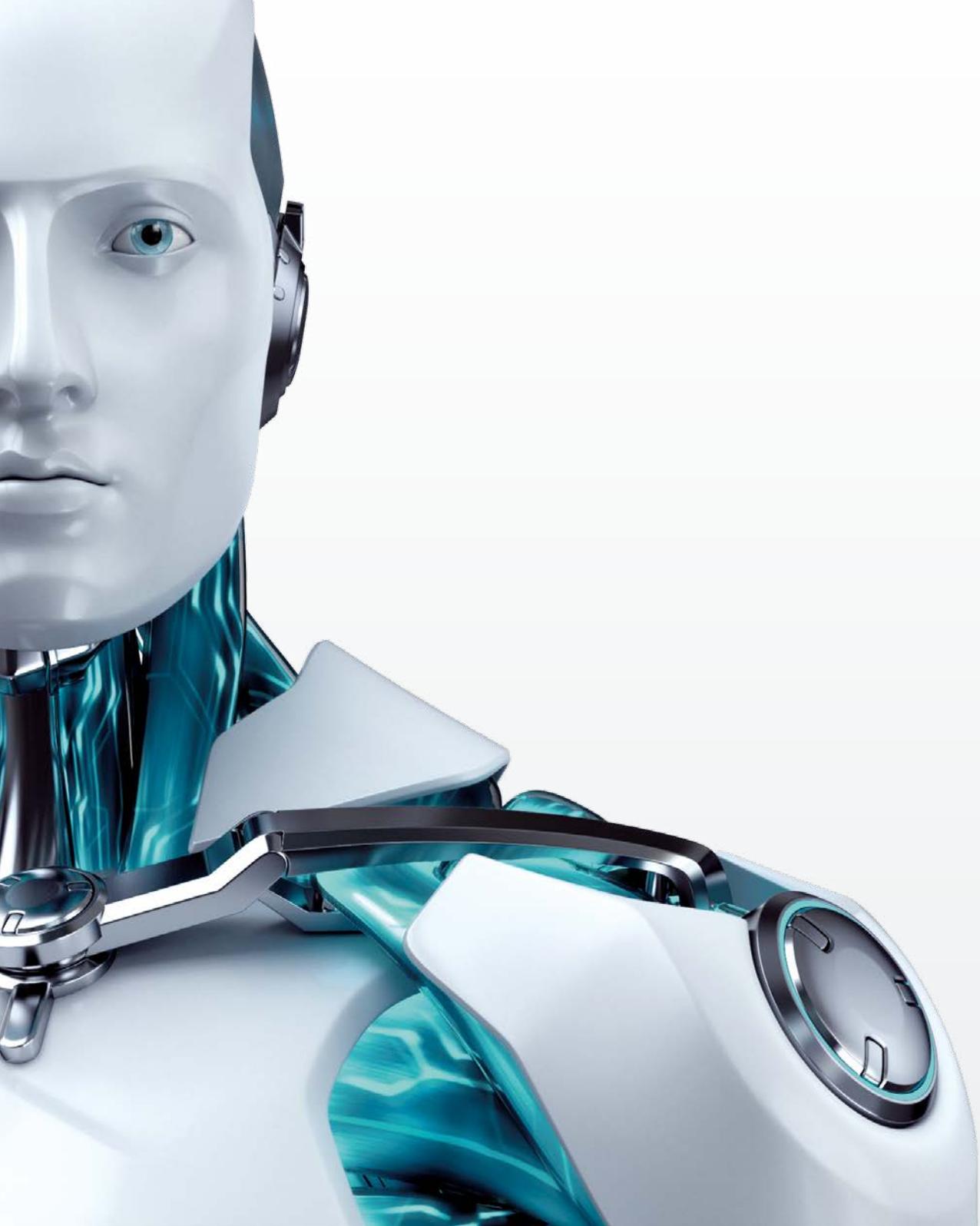


ENDPOINT SOLUTIONS

Features
IT Perspektive

ENJOY SAFER TECHNOLOGY™





Endpoint Protection

| | FUNKTION | VORTEILE & STÄRKEN |
|---|---|---|
| Antivirus / Antispyware | <ul style="list-style-type: none"> • Eliminiert alle Arten von Bedrohungen wie Viren, Rootkits, Würmer und Spyware • Optional: cloud-basierte Scans: Whitelisting bekannt vertrauenswürdiger Dateien über eine Reputationsdatenbank in der Cloud. Nur ausführbare Dateien und Archive werden optional in die Cloud übertragen | Störungsfreie Endpoints bedeuten störungsfreies Arbeiten. Mit ESETs Business Lösungen auf Ihren Endgeräten bleiben Ihre Daten sicher und geschützt. Keine vertraulichen Inhalte werden in die Cloud übertragen, lediglich Informationen über Archive und ausführbare Dateien. Diese Daten sind nicht persönlich rückverfolgbar und auf Wunsch werden gar keine Informationen gesendet. ESETs cloudbasierte Scans bedeuten schnellere Prüfungen, bessere Erkennungen und gleichzeitig eine geringste Fehlalarmquote. |
| Host-basierter Schutz vor Angriffen (HIPS) | <ul style="list-style-type: none"> • Erlaubt das Erstellen von Regeln für die Registry, Prozesse, Anwendungen und Dateien • Verhindert Angriffe auf die Schutzsoftware • Erkennt Bedrohungen basierend auf dem Systemverhalten | Passen Sie das Verhalten des gesamten Systems oder einzelner Teile dessen an. Unautorisierte Vorgängen werden blockiert und das HIPS Log liefert detaillierte Informationen für Audits und Berichte. Der integrierte Selbstschutz gewährleistet, dass die ESET Software nicht manipuliert werden kann und somit das Schutzniveau konstant erhalten bleibt. |
| Automatischer Scan von Wechselmedien | <ul style="list-style-type: none"> • Erlaubt automatische Malware-Scans von Wechselmedien sobald diese am Computer angeschlossen werden. • Auswahlmöglichkeiten: Automatisch Scannen / Nutzer fragen / Nicht scannen | Automatische Scans von Wechselmedien bieten zusätzlichen Schutz vor Offline-Bedrohungen auf USB-Sticks, CDs/DVDs und anderen Wechselmedienträgern. |
| ★ Modulbasierte Installation | <ul style="list-style-type: none"> • Bietet die Möglichkeit, während der Installation unter den folgenden Modulen zu wählen: Firewall, Antispam, Web-Kontrolle, Wechselmedien-Kontrolle, Microsoft NAP Unterstützung und Web-Schutz | Rollen Sie nur die wirklich am jeweiligen Endpoint benötigten Schutzmodule aus, damit Ihre Systeme noch optimaler arbeiten können, ohne Ressourcen unnötig belegen zu müssen. Zusätzlich können für optimales „Fine-Tuning“ jederzeit sämtliche installierten Komponenten remote aktiviert oder deaktiviert werden. |
| ★ Client Antispam | <ul style="list-style-type: none"> • Filtert Spam effektiv am Endpoint aus • Scant alle eingehenden Mails auf Malware | Starker Spamschutz mit Black-/ Whitelisting und Selbstlern-Funktionen, der für jeden Client einzeln oder ganze User-Gruppen genutzt werden kann. Die nahtlose Integration in Microsoft Outlook schützt vor Online Bedrohungen (POP3, IMAP, MAPI, HTTP) ohne zusätzlichen Administrationsaufwand. |
| Geringe Systemanforderungen | <ul style="list-style-type: none"> • Bietet bewährten Schutz und schont dabei Systemressourcen, damit Sie weiter Ihre eigentlichen Anwendungen voll nutzen können | Minimiert Performance-Verluste durch andere, unnötig aufgeblähte Antivirenlösungen und gewährt die volle Performance. Verlängert Hardware-Lebenszyklen durch die Unterstützung auch älterer Systeme ohne diese upgraden zu müssen. Spart Akkulaufzeiten der Laptops, die sich außerhalb des Netzwerks ohne Stromquelle befinden. |
| Plattformübergreifender Schutz | <ul style="list-style-type: none"> • Erkennt und eliminiert Malware sowohl für Windows-, Mac- als auch Linux-Systeme | Bietet besseren Schutz heterogener Netzwerke, da ESETs Security Lösungen für Windows ebenfalls in der Lage sind, Bedrohungen für Linux und/oder Mac OS X und umgekehrt zu erkennen. |
| ESET SysRescue | <ul style="list-style-type: none"> • Erlaubt das Erstellen von bootfähigen Rettungsmedien mit installiertem Malwarescanner um selbst hartnäckig infizierte Endpoints säubern zu können | Erhöhen Sie die Chance der Datenrettung im Notfall durch das Starten und Säubern hartnäckig infizierter Endpoints von CD oder einem USB-Stick. |

★ **Alle mit einem Sternchen** versehenen Funktionen sind nur in ESET Endpoint Security verfügbar
alle anderen aufgeführten Funktionen sind auch in ESET Endpoint Antivirus enthalten

Schutz vor Datendiebstahl

| | FUNKTION | VORTEILE & STÄRKEN |
|---|--|--|
| | Medienkontrolle <ul style="list-style-type: none"> • Blockiert den Zugriff unautorisierter Medien oder Geräte auf Ihre Systeme • Erlaubt das Erstellen von Regeln und Parametern für spezifische Medien, Geräte, Benutzer und Clients | Verwalten Sie zentral Regeln und Policies für Medien und Geräte durch das Verwenden eindeutiger Attribute wie Seriennummer, Hersteller, Modell und vielen mehr. Setzen Sie Lese-, Lese- und Schreib-Berechtigungen oder blockieren Sie den Zugriff einzelner Nutzer oder Nutzergruppen. Detaillierte Zugriffs- und Scan-Logs erleichtern zudem die Kontrolle der Policy-Anwendung und das Compliance-Reporting. |
| ★ | Webkontrolle <ul style="list-style-type: none"> • Beschränkt den Zugriff auf Webseiten durch verschiedene Kategorien • Erlaubt das Erstellen von Regeln für Nutzergruppen, und somit die Wahrung der Unternehmenspolicies | Regulieren und überwachen Sie den Zugriff auf Webseiten. Die Webseiten werden dabei automatisch in verschiedenen Kategorien (Gaming, Soziale Netzwerke und andere) über einen cloud-basierten Dienst klassifiziert. Verhindern Sie außerdem den Zugriff auf Seiten, die eine hohe Netzwerklast erzeugen und schützen somit die Bandbreite für Ihren eigentlichen Zweck. Erfüllen Sie so noch einfacher die Unternehmenspolicies für den Internetzugriff. |
| ★ | Erkennung vertrauenswürdiger Netzwerke <ul style="list-style-type: none"> • Bietet automatisch strengeren Schutz beim Verbinden mit neuen oder unautorisierten Netzwerken | Erstellen Sie striktere Policies für das Verbinden mit unautorisierten Netzwerken, wie öffentlichen WLAN. Definieren Sie vertrauenswürdige Netzwerke, sodass automatisch bei anderen die strengeren Regeln angewandt werden. Die Nutzer und die Daten auf deren Laptops bleiben geschützt, auch wenn zwischen vertrauenswürdigen Netzwerken und öffentlichen Hotspots in Cafés, Flughäfen oder Hotels gewechselt wird. |
| ★ | Zwei-Wege-Firewall <ul style="list-style-type: none"> • Verhindert unautorisierte Zugriffe auf Ihr Unternehmens-Netzwerk • Bietet Schutz vor Hacker-Attacken und Datenverlust | Die Firewall bietet ein einfaches Setup, granulare Einstellmöglichkeiten und ein umfangreiches Regelwerk, sowie einen intelligenten, selbstlernenden Trainingsmodus. Der ESET Remote Administrator beinhaltet zudem einen Firewall-Regel-Assistenten, der Ihnen hilft, der Masse an Regeln Herr zu werden und ein verschiedene Regelwerke im Netzwerk anzuwenden. |

★ **Alle mit einem Sternchen** versehenen Funktionen sind nur in ESET Endpoint Security verfügbar
alle anderen aufgeführten Funktionen sind auch in ESET Endpoint Antivirus enthalten

Remote Administration

| | FUNKTION | VORTEILE & STÄRKEN |
|---|--|--|
| Zentrale Verwaltung | <ul style="list-style-type: none"> Verwalten Sie alle ESET Sicherheitslösungen von einer zentralen Konsole aus | Der ESET Remote Administrator ermöglicht Ihnen das Verwalten sämtlicher Windows-, Mac- oder Linux-Systeme in Ihrem Netzwerk von nur einer Management-Konsole aus. Die Lösung unterstützt IPv6 Infrastrukturen und sogar Ihre Smartphones und virtuellen Maschinen können zentral verwaltet werden. |
| Dynamische Client-Gruppen | <ul style="list-style-type: none"> Erlaubt das Erstellen von statischen und dynamischen Client-Gruppen und ein automatisches Zuweisen in Gruppen anhand von verschiedenen Client-Parametern | Erstellen Sie Nutzergruppen mit verschiedenen Parametern, wie Betriebssystem, Client-Name, IP-Maske, erkannte Bedrohungen und mehr. Setzen Sie spezielle Policies für verschiedene Gruppen, in die die Clients automatisch zugeordnet werden, sobald sich deren Parameter entsprechend ändern. |
| Rollenbasierte Verwaltung | <ul style="list-style-type: none"> Weisen Sie verschiedene Zugriffsrechte verschiedenen Nutzern des ESET Remote Administrator zu Sehen Sie die Aktivitäten der ESET Remote Administrator Nutzer Setzen Sie Passwort-Komplexität durch | Delegieren Sie Verantwortlichkeiten an verschiedene Mitarbeiter oder Gruppen. Detaillierte Audit-Logs erleichtern das Compliance-Reporting und die integrierte Passwortprüfung stellt einen hohen Schutz der Administrator-Passwörter durch eine Komplexitäts-Prüfung dar. |
| Remote Installation | <ul style="list-style-type: none"> Führt Remote-Installationen der ESET Softwares auf mehrere Endpoints gleichzeitig aus | Rollen Sie die ESET Endpoint Lösungen und andere MSI-basierte Installer per Push-Installation im Netzwerk aus. Der ESET Remote Administrator kann neben den ESET Endpoint Lösungen für Windows auch die neuen Generationen an Endpoint Lösungen für Mac und Linux ausrollen. |
| Exportieren/Importieren von Policies | <ul style="list-style-type: none"> Erlaubt das Importieren, Exportieren und Bearbeiten von Policies im XML Format | Sparen Sie Zeit und beugen Sie Fehlern vor, indem Sie einmalig die Konfigurationseinstellungen festlegen und diese anschließend auf den gewünschten Endpoints oder Gruppen automatisch anwenden lassen oder dorthin exportieren. |
| Remote Modulverwaltung | <ul style="list-style-type: none"> Aktivieren/Deaktivieren Sie remote die am Client installierten Schutzmodule wie Firewall, Antispam, Echtzeit-Dateischutz, Web-Schutz und E-Mail-Client-Schutz Eine automatische Reaktivierung kann gesetzt werden für: 10 min, 30 min, 1 Stunde, 4 Stunden oder nie | Vereinfachen Sie Systemwartungen oder Fehlerdiagnosen durch das zentrale Aktivieren oder Deaktivieren der installierten Module. Darüber hinaus können Sie einen automatischen Timer setzen, der den vorherigen Zustand automatisch wieder herstellt um eventuellen Versehen vorzubeugen. Alle Module, mit Ausnahme des Anti-Stealth-Moduls, werden außerdem automatisch beim System-Neustart wieder aktiviert. |

Berichte, Logs, Benachrichtigungen

| | FUNKTION | VORTEILE & STÄRKEN |
|-------------------------------------|--|---|
| Echtzeit-Web-Dashboard | <ul style="list-style-type: none"> Bietet eine komplette Übersicht über Ihren Netzwerkstatus und lässt Sie den Schutzstatus von praktisch überall schnell per Browser einsehen | Greifen Sie auf das web-basierte Dashboard von der Konsole oder überall anders im Netzwerk zu, um schnell Informationen auf einen Blick zum Schutzstatus Ihres Netzwerks abzurufen. Die darzustellenden Informationen können im ESET Remote Administrator und im Dashboard definiert werden. |
| Multiple Logformate | <ul style="list-style-type: none"> Lässt Sie die Logdateien in den gängigsten Formaten speichern - CSV, Nur-Text, Windows Ereignisanzeige – per SIEM Tools auswertbar Logs werden zusätzlich zur späteren Verarbeitung lokal am Endpoint gespeichert | Sammeln Sie alle benötigten Daten einfach und schnell zur weiteren Verarbeitung. ESET unterstützt multiple Log-Formate, was es noch einfacher macht, diese in Drittanbieter "Security Information and Event Management" (SIEM) Tools weiter zu verwenden. |
| Ereignis-Notifikationen | <ul style="list-style-type: none"> Erlaubt das Hinterlegen von Log- und Berichte-Parametern oder das Wählen aus über 50 Templates für verschiedene System- oder Client-Ereignisse Optional können außerdem Schwellwerte für Ereignis-Notifikationen gesetzt werden | Hilft schnell, mögliche Probleme zu identifizieren und so das Netzwerk-Monitoring und Compliance-Reporting zu vereinfachen. Setzen Sie Prioritäten und Zeitintervalle für Notifikationen, und ob diese sofort oder zu festgelegten Zeiten verschickt/erstellt werden sollen. Erstellen Sie Regeln für Notifikationen, skalieren Sie den Umfang von Logs und leiten Sie Notifikationen als E-Mail, Systemlog, SNMP Trap oder Textdatei weiter. |
| Berichte der Medienkontrolle | <ul style="list-style-type: none"> Die Berichte der Wechselmedien-Kontrolle bieten verständliche Logs und Informationen für alle Ereignisse Wechselmedienträger betreffend | Detaillierte Logs zur Verwendung von Wechselmedien und -datenträgern vereinfachen Compliance Reports von einer zentralen Stelle aus. Die Berichte beinhalten Zeitstempel, Benutzername, Computername, Gruppenname, Ereignisdetails und die durchgeführte Aktion. |
| RSA enVision | <ul style="list-style-type: none"> Unterstützt das RSA enVision SIEM Tool per Plugin | Die Unterstützung von RSA enVision gewährleistet einfachste Integration in diese populäre Drittanbieter SIEM Tool. |
| ESET SysInspector | <ul style="list-style-type: none"> Führt Tiefenanalysen der Endpoint-Systeme durch und lässt mögliche Sicherheitslecks schnell auffinden | Identifizieren Sie alle laufenden Prozesse, installierte Software, Hardware-Konfigurationen aller Endpoints. Entdecken Sie mögliche Sicherheitsrisiken oder Inkompatibilitäten durch das automatische Vergleichen zweier Snapshots des Endpoints. |

Netzwerkgeschwindigkeit und –stabilität

| | FUNKTION | VORTEILE & STÄRKEN |
|--------------------------------------|--|---|
| Randomisierte Task Ausführung | <ul style="list-style-type: none"> Erlaubt das Setzen von Zeitfenstern, in denen geplante Sicherheits-Tasks ausgeführt werden | Setzen Sie ein beliebiges Zeitfenster, in dem geplante Tasks ausgeführt werden sollen. Minimieren Sie z.B. die Antiviren-Last in virtuellen Umgebungen oder die Auslastung von Netzwerk-Freigaben durch mehrere, gleichzeitig laufende Scans, damit Ihre Nutzer weiter ungestört arbeiten können. |
| Update Rollback | <ul style="list-style-type: none"> Lässt Sie zu einem vorherigen Stand der Signaturdatenbank und der Module zurücksetzen | Vermeiden Sie Inkompatibilitäten oder andere Systemstörungen durch das Zurücksetzen der Virensignaturdatenbank und der Module auf einen bekannt funktionierenden Stand mit ein paar wenigen Klicks. Halten Sie falls notwendig weitere Updates zurück, optional als temporäres Rollback oder bis zum händischen Update. |
| Verzögerte Updates | <ul style="list-style-type: none"> Bietet die Möglichkeit von 3 speziellen Update-Servern zu laden: Testupdates (Beta-Nutzer), Reguläre Updates (normale Nutzer) und verzögerte Updates (ca. 12 Stunden hinter dem regulären Update) | Stellt saubere Updates sicher und hält den Fokus auf die Verfügbarkeit kritischer Systeme. Wenden Sie Antivirus-Updates zuerst auf weniger kritischen Systemen an um sie nach erfolgreichem Rollout auf den kritischen Systemen zu installieren, zusätzlich mit der Möglichkeit, den Update-Cache zu leeren. |
| Lokaler Update-Server | <ul style="list-style-type: none"> Spart die Bandbreite der Unternehmensanbindung durch das Herunterladen der Updates nur einmalig in einen Mirror-Ordner Sichere (HTTPS) Kommunikation kann optional genutzt werden | Nutzen Sie den ESET Remote Administrator als zentralen Update-Server für Ihr Unternehmen und minimieren Sie so die Internetlast. Definieren Sie zusätzliche Update-Profilen für Außendienstmitarbeiter, die die Updates außerhalb des Netzwerks direkt von den ESET Servern laden. HTTPS wird ebenfalls unterstützt. |
| Schnellerer Datenbankzugriff | <ul style="list-style-type: none"> Bietet optimierten Datenbankzugriff für alle Endpoint sicherheits-relevante Daten | Optimierte Datenbankzugriffe steigern Ihre Produktivität durch schnellere Datenabgleiche aller Ihrer Endpoints und noch schnellere Berichterstellung. |
| Datenbank-Wartung | <ul style="list-style-type: none"> Erlaubt das Setzen von Datenbank-Attributen, wie Zeitfenster und Schwellwerte für Einträge, die in der Datenbank gespeichert werden sollen | Halten Sie die Datenbank fehlerfrei, schnell zugriffsbereit und in einer vernünftigen Größe. |
| Microsoft NAP Support | <ul style="list-style-type: none"> Rollt ein serverseitiges System Health Validator (SHV) Plugin und einen clientseitigen System Health Agent (SHA) aus Garantiert vollen Netzwerkzugriff nur für Clients, die Ihre Anforderungen erfüllen und limitiert/blockiert den Zugriff aller anderen | Hilft beim Sicherstellen von Compliance und Netzwerk-Überwachung (Verfügbarkeit/ Status). Das SHA Plugin sammelt Informationen des Clients und kommuniziert mit der Serverseite innerhalb des NAP Frameworks. Setzen Sie Client Compliance Anforderungen wie: Stand der Signaturdatenbank, Antivirus Produktversion, Schutzstatus, Verfügbarkeit des Virenschutzes und Firewall-Status. Erzwingen Sie Compliance z.B. durch forcierte Datenbankupdates. |



www.eset.de

Copyright © 1992 – 2014 ESET, spol. s r. o., ESET, das ESET-Logo, NOD32, ThreatSense, ThreatSense.Net und/oder andere aufgeführte Produkte von ESET, spol. s r. o., sind eingetragene Warenzeichen von ESET, spol. s r. o. Andere hier erwähnte Firmennamen oder Produkte können eingetragene Warenzeichen ihrer Eigentümer sein. Hergestellt nach den Qualitätsstandards von ISO 9001:2000. Aktueller Stand Jan. 2014 Bestellnr.: ESET-BE-FEATURES

Kontakt Information: