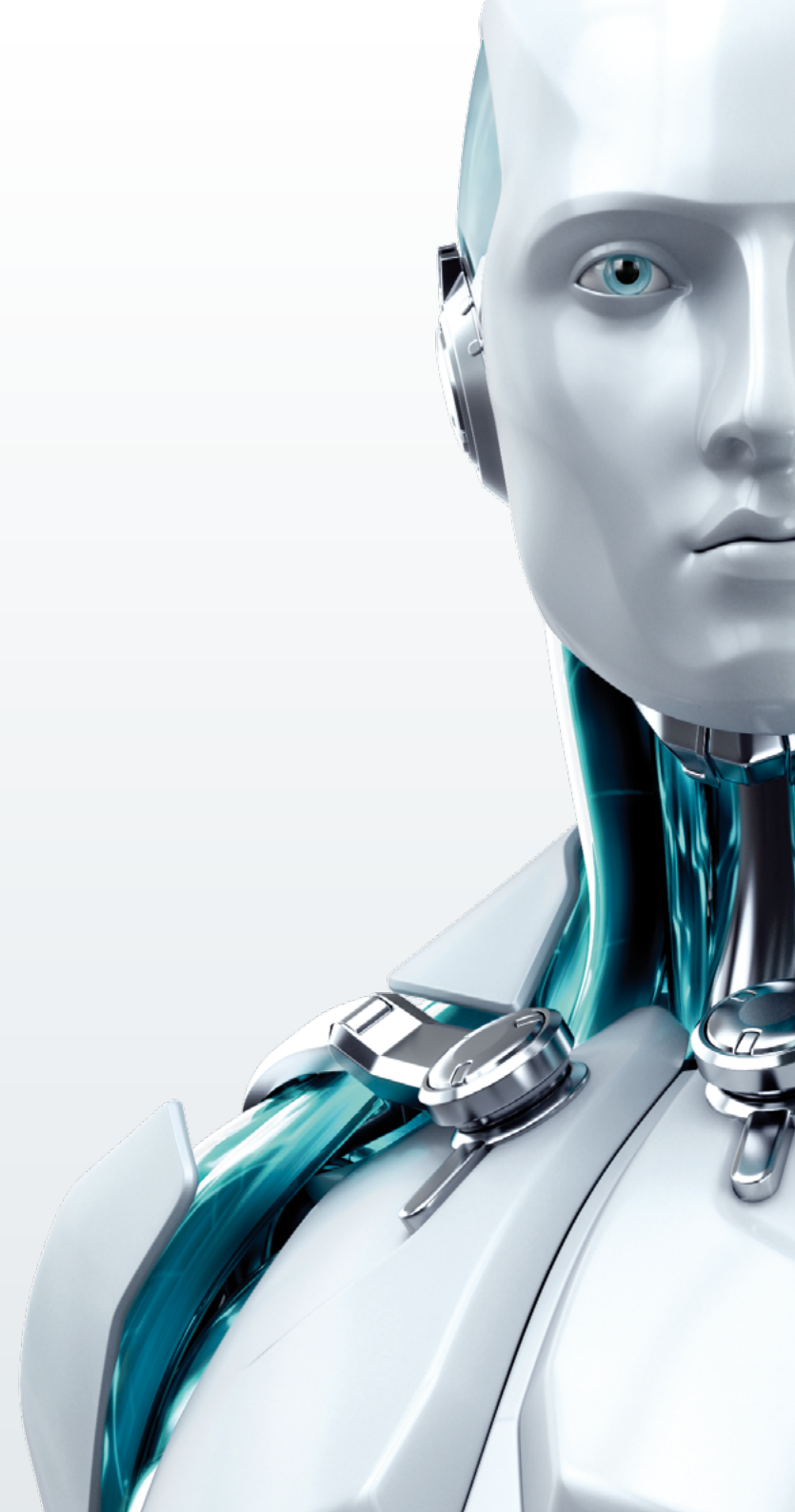


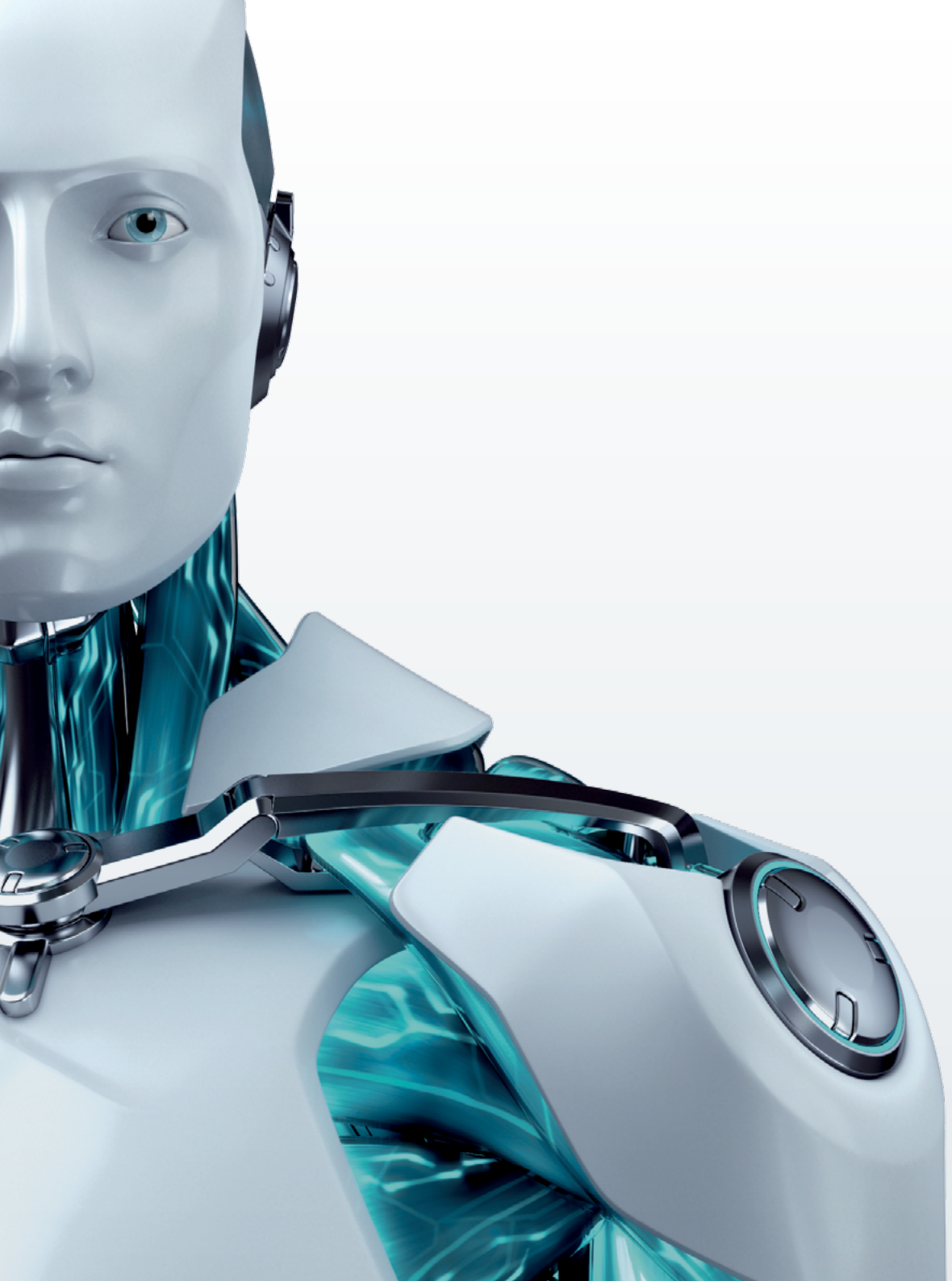
ESET ENDPOINT SOLUTIONS

FEATURES AUS
UNTERNEHMENSICHT



www.eset.de





Endpoint Schutz

	FUNKTION	VORTEILE & STÄRKEN
Antivirus / Antispyware	<ul style="list-style-type: none"> • Eliminiert alle Arten von Bedrohungen wie Viren, Rootkits, Würmer und Spyware • Optionale cloud-basierte Scans: Whitelisting bekannt vertrauenswürdiger Dateien über eine Reputationsdatenbank in der Cloud. Nur ausführbare Dateien und Archive werden optional in die Cloud übertragen 	Schützen Sie Ihre Unternehmensdaten vor Malware jeder Art, egal für welche Plattform sie entwickelt wurde. Die cloudbasierte Reputationsdatenbank beschleunigt Systemprüfungen und hilft, die Fehlalarmquote auf einem absoluten Minimum zu halten. Somit bleibt auch die Vertraulichkeit Ihrer Daten gewahrt.
Automatische Scans 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 Wechseldatenträgern.
Hostbasierter 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 	Unternehmensendpoints bleiben sicher, da das HIPS u.a. die ESET Sicherheitslösungen vor Manipulation durch Malware schützt. Kritische Systemeinträge der Registry, Prozesse, Anwendungen und Dateien werden darüber hinaus ebenfalls vor unautorisiertem Zugriff und Manipulation geschützt.
★ Client Antispam	<ul style="list-style-type: none"> • Filtert Spam effektiv am Endpoint aus • Scant alle eingehenden Mails auf Malware 	Lassen Sie automatisch unerwünschte Mails aussortieren, was die Effizienz Ihrer Mitarbeiter einerseits erhöht und andererseits das Risiko Opfer von Phishing Attacken zu werden minimiert. Basierend auf Nutzerkategorien lassen sich die Anforderungen für Business E-Mail-Verkehr einfach umsetzen.
Plattformübergreifender Schutz	<ul style="list-style-type: none"> • Erkennt und eliminiert Malware sowohl für Windows-, Mac- als auch Linux-Systeme 	Tauschen Sie Dateien und E-Mail-Anhänge zwischen Windows, Mac und Linux Endpoints mit dem guten Gewissen, dass Malware die für irgendeine dieser Plattformen konzipiert wurde, automatisch erkannt und eliminiert werden kann.
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 	Starten und säubern Sie infizierte Endpoints von CD oder USB und erhöhen somit die Chance der Datenwiederherstellung wenn alle anderen Optionen bereits ausgeschöpft scheinen.

★ *mit einem Sternchen gekennzeichnete Funktionen sind nur in der ESET Endpoint Security verfügbar; alle anderen aufgeführten Features sind auch in der ESET Endpoint Antivirus enthalten

Schutz vor Datendiebstahl

	FUNKTION	VORTEILE & STÄRKEN
★ Zwei-Wege-Firewall	<ul style="list-style-type: none"> • Verhindert unautorisierte Zugriffe auf Ihr Unternehmens-Netzwerk • Bietet Schutz vor Hacker-Attacken und Datenverlust 	Schützen Sie Ihre Unternehmensdaten und vitalen Informationen vor Verlust durch unautorisierte Verbindungen von oder nach außen.
Medienkontrolle	<ul style="list-style-type: none"> • Blockiert den Zugriff auf Ihre Systeme durch unautorisierte Medien oder Geräte • Erlaubt das Erstellen von Regeln und Parametern für spezifische Medien, Geräte, Benutzer und Clients 	Verhindern Sie das unerlaubte Kopieren von Unternehmensdaten auf USB-Sticks, CDs, DVDs und andere Wechselmedien. Durch flexible Policies zur Wechselmedien-Kontrolle können Sie den Zugriff für bestimmte Nutzer oder Gruppen basierend auf Geräteparametern wie Seriennummer, Hersteller-ID, Modell usw. definieren.
★ Erkennung vertrauenswürdiger Netzwerke	<ul style="list-style-type: none"> • Bietet automatisch strengeren Schutz beim Verbinden mit neuen oder unautorisierten Netzwerken 	Wahren Sie die Vertraulichkeit Ihrer Unternehmensdaten trotz dessen, dass Ihre Mitarbeiter unterwegs ständig zwischen vertrauenswürdigen Netzwerken und öffentlichen WLAN-Hotspots in Cafés, am Flughafen oder im Hotel wechseln. Verhindern Sie außerdem, dass Ihre Unternehmenskommunikation „belauscht“ wird.

Mitarbeitereffizienz

	FUNKTION	VORTEILE & STÄRKEN
★ 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 	Verhindern Sie unproduktives Surfen im Netz und setzen Sie Ihre Policies zur erlaubten Internet-Nutzung durch. Die können Sie durch das Blockieren von unerlaubten Webseiten oder Webseitenkategorien tun und somit auch verhindern, dass Ihre Mitarbeiter eventuell versehentlich unpassende, ungewollte oder andere nicht arbeitsrelevanten Seiten aufrufen.
Geringe Systemanforderungen	<ul style="list-style-type: none"> • Bietet bewährten Schutz und schont dabei Systemressourcen, damit Sie weiter Ihre eigentlichen Anwendungen voll nutzen können 	Verbesserter ROI durch störungsfreien Betrieb Ihrer Computer und verlängerter Nutzung auch älterer Systeme. Steigern Sie die Effizienz Ihrer Mitarbeiter allein schon dadurch, dass die Rechner nicht durch unnötig aufgeblähte Schutzsoftware verlangsamt werden.
Präsentations-Modus	<ul style="list-style-type: none"> • Blockiert während des Vollbildmodus von Anwendungen und Präsentationen Pop-Ups und andere rechenintensive Aufgaben 	Verhindern Sie peinliche Momente oder Störungen während Ihrer Slideshows, Präsentationen und anderer Vollbild-Anwendungen.
★ 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 	Verlängern Sie Hardware-Lebenszyklen und sparen Sie Geld durch das Minimieren von CPU- und RAM-Auslastung, sowie von Festplattenspeicher, der von der Sicherheitslösung beansprucht wird.

★ mit einem Sternchen gekennzeichnete Funktionen sind nur in der ESET Endpoint Security verfügbar; alle anderen aufgeführten Features sind auch in der 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 	<p>Behalten Sie die Kontrolle über Ihr IT-Budget. Der ESET Remote Administrator verwaltet alle bisherigen, aktuellen und kommenden ESET Lösungen. Verwalten Sie auf einfachste Weise sämtliche Endpoints, Server, Smartphones und sogar virtuellen Maschinen von einer einzigen Konsole aus, ganz egal ob im Netzwerk Windows-, Mac- oder Linux-Systeme geschützt werden.</p>
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 	<p>Rollenbasierte Administration vereinfacht das Delegieren von Verantwortlichkeiten innerhalb des IT-Teams. Detaillierte Audit-Logs erleichtern zudem das Compliance-Reporting.</p>
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 	<p>Die Sicherheitsregeln lassen sich einfach für verschiedene Gruppen an Mitarbeitern anwenden. Dynamische Gruppen lassen sich schnell, basierend auf verschiedenen Client-Status erstellen und erleichtern die Identifikation und Zuordnung von Clients, die wiederum Sicherheits-Ereignisse triggern können.</p>
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 	<p>Sparen Sie die Zeit Ihres IT-Teams durch Priorisierung von Notifikationen und dem Festlegen, welche Sicherheits-Ereignisse wichtig sind, wie detailliert und in welchen Intervallen berichtet werden soll, sodass das Team handlungsfähig bleibt, ohne nervige Belastung durch unaussagekräftige Warnmeldungen.</p>
Remote Installation	<ul style="list-style-type: none"> Führt Remote-Installationen der ESET Softwares auf mehrere Endpoints gleichzeitig aus 	<p>Lässt Ihre IT mit wenigen Klicks, von einer zentralen Stelle aus, ESETs Sicherheitslösungen im Netzwerk ausrollen.</p>
Export/Import von Policies	<ul style="list-style-type: none"> Erlaubt das Importieren, Exportieren und Bearbeiten von Policies im XML Format 	<p>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.</p>
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 	<p>Reduzieren Sie eventuelle Ausfallzeiten oder Verzögerungen während der Systemwartung durch das zentrale Aktivieren oder Deaktivieren der einzelnen Schutzmodule.</p>

Berichte, Logs und Notifikationen

	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 	Überblicken Sie den Schutzstatus Ihres Netzwerks schnell mit Echtzeit-Informationen zur Serverlast und Sicherheit. Sie können kritische Informationen damit praktisch von überall per Browser über das web-basierte Dashboard einsehen.
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 	Nutzen Sie die Vorteile der Daten-Speicherfunktionen um Zusammenhänge einzelner Sicherheits-Ereignisse schnell und einfach zu erkennen. Machen Sie außerdem die Daten les- und auswertbar für sogenannte „Security Information and Event Management“ (SIEM) Tools anderer Hersteller.
Berichte der Medien-Kontrolle	<ul style="list-style-type: none"> Die Berichte der Medien-Kontrolle bieten verständliche Logs und Informationen für alle Ereignisse Wechseldatenträger betreffend 	Überwachen Sie die Verwendung von Wechselmedien und -geräten im gesamten Netzwerk an einer zentralen Stelle.
RSA enVision Support	<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 	Geben Sie Ihren IT-Admins alle notwendigen Tools um potentielle Sicherheitslücken zu finden und proaktiv vorbeugende Maßnahmen zu treffen.

Update-Management

	FUNKTION	VORTEILE & STÄRKEN
Randomisierte Task Ausführung	<ul style="list-style-type: none"> Erlaubt das Setzen von Zeitfenstern, in denen geplante Sicherheits-Tasks ausgeführt werden 	<p>Verhindern Sie Systemeinträge durch verzögerte Antwortzeiten der Server oder hohe Antiviren-Last in virtuellen Umgebungen. Dieses Feature stellt sicher, dass zeitgleich geplante Aufgaben der Endpoints weder Ihre Systeme noch das Netzwerk ausbremsen.</p>
Update Rollback	<ul style="list-style-type: none"> Lässt Sie zu einem vorherigen Stand der Signaturdatenbank und der Module zurücksetzen 	<p>Vermeiden Sie Inkompatibilitäten oder andere Systemstörungen durch das Zurücksetzen der Virensignaturdatenbank und der Module mit ein paar wenigen Klicks.</p>
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) 	<p>Halten Sie Ihre Online-Systeme, die rund um die Uhr laufen müssen, in höchster Verfügbarkeit. Verhindern Sie Ausfälle durch Antiviren-Updates oder andere Ereignisse, die die Arbeit beeinträchtigen könnten.</p>
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 	<p>Halten Sie Ihre Internetverbindung für arbeitsbezogene Kommunikation frei, indem Sie den Update-Traffic der Antiviren-Software auf ein Minimum reduzieren.</p>
Schnellerer Datenbankzugriff	<ul style="list-style-type: none"> Bietet optimierten Datenbankzugriff für alle Endpoint sicherheitsrelevanter Daten 	<p>Ein schneller Datenbankzugriff bedeutet schnellere Berichterstattung und Datenabgleiche quer durch alle Ihre Endpoints, was wiederum die Produktivität der IT enorm erhöht.</p>
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 	<p>Speichern Sie nur Sicherheitslogs, die wichtig und aktuell sind, was wiederum die Datenbank schlank und somit die Serverlast gering hält.</p>
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 	<p>Kontrollieren Sie den Zugriff auf Netzwerkressourcen basierend auf der Client-Identität und der Compliance mit Ihrer Unternehmens-Policy. Das Microsoft Network Access Protection (NAP) Plugin erlaubt die vollständige Integration mit Ihren Unternehmens-Compliance-Policies.</p>



www.eset.de
www.eset.com

Copyright © 2012 ESET, spol. s r. o. ®, © 2012 DATSEC® Data Security e.K.

ESET, NOD32, ThreatSense sind Warenzeichen oder registrierte Warenzeichen von ESET LLC bzw. ESET spol. s.r.o.
DATSEC ist eine Marke von DATSEC Data Security e.K.. Weitere verwendete Firmen-, Produkt-, Handelsnamen usw. unterliegen im Allgemeinen marken-, patent- oder warenzeichenrechtlichem Schutz. Alle Angaben wurden sorgfältig erarbeitet.
100% Fehlerfreiheit kann jedoch nicht garantiert werden. Produktänderungen vorbehalten.
Aktueller Stand Juni 2012

Kontakt Information: