ESET REMOTE ADMINISTRATOR

Features

www.eset.de

Remote Administration

	FUNKTION	VORTEILE & STÄRKEN
Zentrale Verwaltung	• Ermöglicht die Verwaltung aller 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	• 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 ändern.
Rollenbasierte Verwaltung	• Weist unterschiedlichen Nutzern des ESET Remote Administrators verschiedene Zugriffsrechte zu • Überprüft die Aktivitäten der Nutzer des ESET Remote Administrator • Erfordert Passwort-Komplexität	Delegieren Sie Verantwortlichkeiten an verschiedene Mitarbeiter oder Gruppen. Detaillierte Audit-Logs erleichtern das Compliance-Reporting. Die integrierte Komplexitäts-Prüfung stellt einen hohen Schutz der Administrator-Passwörter dar.
Remote Installation	• Führt Remote-Installationen der ESET Softwares auf mehreren 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 installieren.
Export/Import von Policies	• 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	• Aktiviert/Deaktiviert 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 wieder herstellt um eventuellen Versehen vorzubeugen. Alle Module, mit Ausnahme des Anti-Stealth-Moduls, werden außerdem automatisch beim System-Neustart wieder aktiviert.

Berichte, Logs und Notifikationen

	FUNKTION	VORTEILE & STÄRKEN
Echtzeit-Web-Dashboard	• 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 auf einen Blick Informationen zum Schutzstatus Ihres Netzwerks abzurufen. Die darzustellenden Informationen können im ESET Remote Administrator und im Dashboard definiert werden.
Multiple Logformate	• 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-Tools wie "Security Information and Event Management" (SIEM) weiter zu verwenden.
Ereignis-Notifikationen	• 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	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.
Berichte der Medien-Kontrolle	• Die Berichte der Wechselmedien-Kontrolle bieten verständliche Logs und Informationen für alle Ereignisse, die Wechseldatenträger betreffen	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 Support	• Unterstützt das RSA enVision SIEM Tool per Plugin	Die Unterstützung von RSA enVision gewährleistet einfachste Integration in dieses populäre Tool.
ESET SysInspector	• 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 UND STÄRKEN
Randomisierte Task Ausführung	• 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.
Verzögerte Updates	• 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	• Spart die Bandbreite der Unternehmensanbindung durch das einmalige Herunterladen der Updates 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-Profile für Außendienstmitarbeiter, die die Updates außerhalb des Netzwerks direkt von den ESET Servern laden. HTTPS wird ebenfalls unterstützt.
Schnellerer Datenbankzugriff	• Bietet optimierten Datenbankzugriff für alle sicherheitsrelevanten Daten der Endpoints	Optimierte Datenbankzugriffe steigern Ihre Produktivität durch schnellere Datenabgleiche aller Ihrer Endpoints und noch schnellere Berichterstellung.
Datenbank-Wartung	• 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	• 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.