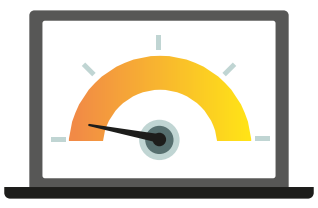
Sparen Sie Geld und Mühen Mit Kaspersky Endpoint Security Cloud

Gewöhnliches Szenario

manuell, langwierig
und teuer



Szenario mit Kaspersky Endpoint Security Cloud

einfach, schnell, automatisch, ohne Extrakosten

Bereitstellung der Sicherheitslösung

Installieren Sie die Endpoint-Anwendung mithilfe eines Flash-Laufwerks auf den einzelnen Computern

Fügen Sie eine Lizenz hinzu

Legen Sie die Parameter fest, mit denen Agents die Verbindung zur Verwaltungskonsole herstellen

Fügen Sie eine Liste der E-Mail-Adressen von Mitarbeitern ein, um allen einen Installationslink für die Anwendung zu senden

Das war´s. Alles andere geschieht automatisch

Erstellung von Sicherheitsrichtlinien

Eine Richtlinie komplett neu erstellen

Im besten Fall werden Sie vom Assistenten dazu aufgefordert, aus zahlreichen Parametern auszuwählen, deren Definition sie oftmals nicht kennen

Auf jedes Gerät wird automatisch die Standardrichtlinie angewendet

Bei Bedarf können Sie diese später anpassen und anhand einer Vorlage verschiedene Profile erstellen

Erkennung von Schatten-IT

Überprüfen Sie Ihren Router oder besorgen Sie sich einen Traffic Sniffer

Kaufen Sie sich einen teuren CASB[1]-Setup-Anschluss für Ihre IT-Infrastruktur

Öffnen Sie das Widget in der Verwaltungskonsole und mit wenigen Klicks:

1. Erhalten Sie einen Bericht zur Verwendung von Schatten-IT
2. Blockieren Sie Services/Nutzer und legen Ausnahmen für VIP-Nutzer fest

Phishing- und Malware-Schutz für Microsoft Office 365

Verwenden Sie den integrierten Schutz und hoffen Sie das Beste

Kaufen Sie Microsoft ATP - leider ziemlich teuer

Kaufen Sie eine E-Mail/Cloud-Lösung eines Drittanbieters

Schutz für alle wichtigen Anwendungen einschließlich Exchange Online, OneDrive, SharePoint Online und Teams ist bereits ohne zusätzliche Kosten in KES Cloud Plus integriert, da uns die Sicherheit Ihres Unternehmens ein Anliegen ist

Patch Management

Machen Sie die Verwaltung manuell oder mit einer Spezialsoftware

Sie müssen sich dabei immer entscheiden, ob Sie Schwachstellen tolerieren oder Ihre Kollegen mit Patch-Installationen belästigen wollen, wobei Ihre Kollegen natürlich nie Zeit dafür haben

Machen Sie die Installation nach Feierabend, obwohl Sie ja eigentlich ausspannen wollten

Planen Sie automatische Patch-Installationen außerhalb der Arbeitszeiten

Vergessen Sie „Freitag ist Patching-Tag“ und genießen Sie Ihre Freizeit

Antivirenscan

Denken Sie daran oder richten Sie Erinnerungen ein, um Datenbanken zu aktualisieren und Antivirenscans auf allen Computern im Büro durchzuführen

Belästigen Sie Nutzer mit geringerer Computerleistung während der Scans

Nie mehr manuelle Antivirenscans

KES Cloud scannt alle Computer im Hintergrund, wenn sie gerade nicht genutzt werden und wirkt sich damit nicht auf die Leistung aus

Full-Disk-Verschlüsselung

Wenn alle im selben Büro sitzen, können ruhig die im Betriebssystem vorhandenen Tools verwendet werden

BitLocker arbeitet jedoch am besten im Tandem mit einem lokalen Active Directory – und das ist im Home Office nicht verfügbar

Verschlüsseln Sie Geräte per Fernzugriff und direkt von der KES Cloud-Konsole unter Verwendung der im Betriebssystem integrierten Tools (BitLocker für Windows und FileVault für MacOS)

[1] Cloud Access Security Broker

kaspersky