KASPERSKY lab

IS ER EEN REVOLUTIE IN IT-BEVEILIGING... OF IS HET IJDELE HOOP?

Hoe u verschillende beveiligings-oplossingen kunt beoordelen, de feiten van de hype kunt onderscheiden en de juiste beveiliging voor uw bedrijf kunt kiezen

www.kaspersky.nl

Wanneer u uw huidige IT-beveiligingsstrategie aan het evalueren bent om er zeker van te zijn dat uw bedrijf goed is beveiligd tegen de steeds complexere dreigingen en aanvallen van nu, proberen veel beveiligingsleveranciers u over te halen voor hun producten.

Maar hoe komt u erachter welke technologieën werkelijk optimaal beveiligen, welke methoden uw productiviteit kunnen schaden, welke opties kwetsbare plekken in uw beveiliging onbeschermd laten en welke beveiligingsstrategieën het meest geschikt zijn voor uw specifieke bedrijfsbehoeften?

Zoals geldt voor de meeste IT-strategiebeslissingen, moet u ook voor deze eerst de feiten onderscheiden van de hype, zodat u kunt beoordelen welke technologieën waarmaken wat ze beloven.

ER STAAT VEEL OP HET SPEL

Door de voortdurende toename van zowel het aantal en de complexiteit van moderne malware, internetaanvallen en cybercriminaliteit groeien de risico's voor bedrijven. Daarom is het belangrijker dan ooit dat u de meest effectieve beveiliging kiest.

Er staat veel meer op het spel dan alleen uw IT-budget. Een ontoereikende beveiligingsoplossing kan uiterst kostbare en langdurige gevolgen hebben voor een bedrijf:

- Ransomwareaanvallen kunnen belangrijke bedrijfsgegevens versleutelen, waardoor de dagelijkse bedrijfsprocessen ingrijpend worden verstoord.
- Het lekken van vertrouwelijke klantgegevens kan leiden tot verstoorde relaties, omzetverlies en eventueel juridische problemen.
- Verlies van gegevens met betrekking tot ontwerpen en ander intellectueel eigendom kan de moeizaam verworven marktvoorsprong van een bedrijf verkleinen.

Een enquête onder 5500 bedrijven in 26 landen wees uit dat:

- **90% het slachtoffer is geweest van een beveiligingsincident**
- **46% vertrouwelijke gegevens heeft verloren as gevolg van een beveiligingsdreiging**

Bron: Corporate IT Security Risks Survey, Kaspersky Lab

WAAROM ZIJN BEDRIJVEN NOG STEEDS KWETSBAAR?

IT-beveiligingsoplossingen zijn natuurlijk al jaren beschikbaar. Waarom vallen bedrijven dan nog steeds ten prooi aan aanvallers? Daar is geen eenduidig antwoord op te geven.

Criminelen weten al lang dat er veel geld is te verdienen aan een geslaagde aanval op een bedrijf. Daarom steken ze steeds meer energie in het bedenken van slimmere technologieën. De potentiële voordelen zijn zo groot dat cybercriminaliteit niet zal verdwijnen. Criminelen zullen blijven proberen om de bestaande beveiligingstechnologieën te omzeilen.

Maar de bedrijven die aan hen ten prooi vallen, spelen hier ook een rol in.

SCHIETEN BEDRIJVEN TEKORT?

Sommige bedrijven nemen ten onrechte aan dat ze nooit het doelwit zullen worden en implementeren alleen heel eenvoudige beveiligingsmaatregelen. Helaas zijn alle bedrijven een mogelijk doelwit. Zelfs de diefstal van vertrouwelijke gegevens over klanten en werknemers kan cybercriminelen veel voordeel opleveren. Het bedrijf heeft dan te kampen met financieel verlies en een beschadigde reputatie.

Er zijn ook bedrijven die hebben geïnvesteerd in de bescherming van de belangrijkste onderdelen van hun IT-infrastructuur, maar onbedoeld andere delen onbeschermd hebben gelaten.

Sommige bedrijven vertrouwden zelfs op een of andere revolutionaire, 'aanvalsdichte' technologie, die uiteindelijk de belofte niet wist waar te maken.

Vooral deze laatste categorie is zorgwekkend, omdat zo'n bedrijf mogelijk het slachtoffer is geworden van marketingpraatjes. Het bedrijf heeft dan een vals gevoel van veiligheid gekregen door ongegronde beweringen en mogelijk besloten de oorspronkelijke beveiliging, die altijd prima functioneerde, in te ruilen voor een nieuwe technologie.

Dit scenario toont aan dat sommige bedrijven bereid zijn om de feiten aan de kant te schuiven en inhoudsloze beweringen te geloven. Waarom doen bedrijven dat?

WIE GAAT DE STRIJD WINNEN?

De strijd tussen cybercriminelen en beveiligingsleveranciers is al jaren bezig. Dat leidt bedrijven af van hetgeen waarop ze zich willen richten: kernactiviteiten uitvoeren, nieuwe producten en diensten ontwikkelen, meer klanten binnenhalen en een groter marktaandeel behalen. Cybercriminaliteit en zelfs IT-beveiliging kunnen ongewenste afleidingen zijn: ze vergen tijd die het bedrijf liever zou besteden aan andere werkzaamheden.

Er ontstaat een hang naar 'de goede oude tijd', toen bedrijven niet hoefden na te denken over cyberaanvallen en IT-beveiligingsrisico's. Die tijd is voorbij. Cybercriminaliteit zal absoluut niet verdwijnen.

FRUSTRATIE LEIDT TOT SLECHTE BEVEILIGING

Een nieuwe beveiligingsoplossing die een afdoende oplossing voor nu en de toekomst belooft zonder dat u updates hoeft uit te voeren en constant beheer vereist is - dat klinkt als muziek in de oren van een bedrijfseigenaar.

Helaas bestaat zo'n magische oplossing niet en die zal er ook nooit komen.

Maar wanneer een bedrijf allerlei indrukwekkende beweringen over nieuwe beveiligingsproducten hoort, kan het verlangen naar een veiliger bedrijfsomgeving leiden tot irrationele beslissingen. En dat is riskant. Dit is vooral het geval als een bedrijf net het slachtoffer is geweest van een beveiligingsincident en haast heeft om een nieuwe beveiligingsstrategie te vinden. Soms worden dan niet alle mogelijkheden van verschillende leveranciers goed overwogen.

IS BEVEILIGING VAN DE VOLGENDE GENERATIE DE OPLOSSING?

De toevoeging 'volgende generatie' aan een productnaam kan een sterke uitwerking hebben. Wie wil immers de 'oude generatie' kopen als er een nieuwe generatie producten verkrijgbaar is met uitgebreidere en betere mogelijkheden?

Helaas begrijpen de marketingteams van sommige leveranciers de kracht van bepaalde woorden maar al te goed. En ze gebruiken die om goedgelovige bedrijven te overtuigen.

Wat betekent beveiliging van de volgende generatie eigenlijk?

Er is geen ANSI- of ISO-standaard waaraan een beveiligingsproduct moet voldoen om de aanduiding 'volgende generatie' te verdienen. U moet daarom zelf onderzoek doen om te beslissen of de term 'volgende generatie' inhoud heeft of dat deze slechts een pakkende term is waarmee een marketingteam u het idee wil geven dat een beveiligingsproduct gebruiksvriendelijk en betrouwbaar is.

BEVEILIGING IS EEN CONTINU PROCES... EN DAT VEREIST TOEGEWIJDE LEVERANCIERS

Er bestaat geen alternatief voor bescherming op basis van informatie over geavanceerde dreigingen. Maar om deze informatie te verkrijgen, is een groot team van beveiligings- en dreigingsexperts nodig. Maar weinig leveranciers kunnen zich een dergelijke investering veroorloven.

De leveranciers die wel kunnen investeren in wereldwijde beveiligingsinformatie, steken ook veel tijd in het anticiperen op nieuwe dreigingen. Daarnaast proberen ze erachter te komen op welke manier cybercriminelen hun technieken verbeteren, zodat er ook oplossingen zijn wanneer een nieuw soort aanval wordt ingezet.

Vaak **klinken** producten van de volgende generatie heel indrukwekkend, maar in werkelijkheid is effectieve IT-beveiliging niet zo glamoureus. Leveranciers die uitgebreide beveiliging voor bedrijven leveren, erkennen dat het een zware taak is. Het vereist tijd, investeringen en aanzienlijke expertise. Een magisch alternatief bestaat niet.

HET DREIGINGSLANDSCHAP BEPAALT UW BEVEILIGINGSSTRATEGIE

Het is essentieel dat alle bedrijven zich beschermen tegen alle mogelijke IT-dreigingen:

- Bekende dreigingen
- Onbekende dreigingen
- Geavanceerde dreigingen

Dat brede dreigingslandschap vereist een meerlaagse aanpak van bedrijfsbeveiliging.

Bedrijven kunnen niet precies voorspellen waar hun beveiligingssystemen mee te maken krijgen. Een bedrijf dat vertrouwt op één oplossing van de volgende generatie kan dan ook bijzonder kwetsbaar zijn wanneer een aanval wordt ingezet.

Omdat cybercriminelen continu proberen om de beveiligingssystemen van bedrijven te slim af te zijn, begaan bedrijven een fout als hun beveiliging bestaat uit één enkele laag. Meerdere, overlappende beveiligingslagen voorkomen dat cybercriminelen meteen vrij spel hebben wanneer één laag is doorbroken.

UW MIDDELEN BEPALEN UW BEVEILIGINGSBEHEER

Geen enkel bedrijf wil te veel tijd besteden aan het beheer van beveiliging. Daarom is het ook belangrijk dat uw beveiligingsoplossing bestaat uit één geïntegreerde console waarmee u de beveiliging voor alle endpoints, met inbegrip van mobiele apparaten en servers, kunt instellen en beheren.

Vervolgens hoeft u alleen maar te kiezen tussen een beveiligingsoplossing die gebruikmaakt van een beheerinfrastructuur op locatie of die een beheerconsole in de cloud biedt, zodat u geen server op locatie nodig hebt. In de meeste gevallen bieden oplossingen met een console op locatie zeer gedetailleerde beveiligingscontrole, maar de implementatie en het beheer ervan vergen tijd en inzet.

Sommige oplossingen met consoles in de cloud kunnen daarentegen het beveiligingsbeheer vereenvoudigen. Deze oplossingen zijn bijzonder geschikt voor bedrijven met erg kleine IT-teams en bedrijven die al het beveiligingsbeheer liever uitbesteden aan een externe consultant.

Oplossingen met een cloudgebaseerde console kunnen aanzienlijke voordelen opleveren:

- Omdat de console in de cloud zit, hebt u geen server op locatie nodig voor beveiligingsbeheer.
- De initiële implementatie verloopt veel sneller.
- Continu beveiligingsbeheer vereist minder tijd en inspanning.
- Het beheer kan overal worden uitgevoerd, met elk apparaat dat toegang heeft tot internet.

MARKETINGMYTHES OVER DE VOLGENDE GENERATIE

Laten we eens kijken naar de grootste mythes over de beveiliging van de volgende generatie.

Mythe 1: Traditionele anti-virusbeveiliging is niet meer noodzakelijk

Dit is waarschijnlijk de grootste mythe over IT-beveiliging. Hoewel definitiegebaseerde anti-virusbeveiliging niet beschermt tegen onbekende en geavanceerde dreigingen, is het een erg belangrijk element in elke meerlaagse IT-beveiliging. Het is nog steeds een effectieve manier om bekende malware te blokkeren. Verder gebruiken de beste moderne beveiligingstechnologieën de kracht van de cloud om nieuwe definities sneller te leveren, zodat bedrijven beschermd zijn tegen nieuwe malware.

ErzijnalteveelbedrijvendiehebbenondervondendathetnegerenvandeessentiëleIT-beveiligingslaag kan leiden tot kostbare en beschamende incidenten: 'perfecte' beveiligingsoplossingen missen hun doel of blokkeren onterecht goedaardige communicatie.

Mythe 2:
Beveiligingsupdates verminderen IT-prestaties

We herinneren ons allemaal de tijd waarin IT-beveiliging net bestond: anti-virusupdates waren soms langzaam en onpraktisch en verslechterden de computerprestaties. Er is sindsdien veel veranderd.

Gelukkig zijn er nu beveiligingsoplossingen die een minimale impact op prestaties hebben, maar die wel de beveiliging verbeteren door regelmatig updates tegen nieuwe risico's uit te voeren. Ook werken ze afzonderlijk verschillende beveiligingslagen bij om de bescherming constant op een hoog niveau te houden.

Mythe 3:
Beveiliging die connectiviteit minimaliseert kan afdoende bescherming bieden

Sommige oplossingen worden gepromoot met de 'aanbeveling' dat ze betrekkelijk weinig beveiligingsupdates uitvoeren om de impact op computerprestaties te minimaliseren. Dit is echter niet de ideale manier om bandbreedte op uw bedrijfsnetwerk vrij te maken of om uw bedrijf efficiënt te beschermen.

Regelmatige updates voor zowel definities die bekende malware blokkeren als voor heuristische modellen die onbekende dreigingen detecteren, zijn cruciaal om te garanderen dat uw verdediging snel kan reageren op nieuwe dreigingen. Verder zorgen regelmatige updates er ook voor dat foutieve identificaties, en daardoor onnodige en tijdrovende verstoringen, tot een minimum beperkt blijven.

Waar het om gaat is dat deze updates worden uitgevoerd op een manier die de productiviteit niet beïnvloedt.

Mythe 4:
De revolutie is begonnen... en het is de volgende generatie!

Als het om de bescherming van uw bedrijf gaat, zijn marketinghype en pakkende slogans niet goed genoeg. Als er zo veel op het spel staat, tellen alleen echte prestaties en het bewijs dat er effectieve bescherming wordt geboden. Onderzoek daarom altijd wat er achter het label 'volgende generatie' schuilgaat.

BEVEILIGING DIE IS GEBASEERD OP ECHTE RESULTATEN

Wij horen vaak dat Kaspersky Lab al 'volgende generatie' was ver voordat andere beveiligingsleveranciers dat waren. Maar 'volgende generatie' is een nogal vage term die gemakkelijk kan worden misbruikt. Daarom vermijden wij deze liever.

Volgens sommigen belichaamt onze combinatie van 'machine learning' en vermaarde beveiligingsexperts de 'volgende generatie'. Voor ons is dat gewoon iets wat wij al jaren doen. Het maakt deel uit van ons streven om superieure beveiliging te ontwikkelen en niet afhankelijk te zijn van trendy marketingtermen.

Wij houden het liever bij de feiten, vermijden de hype en zetten onze missie voort om de sluwste cybercriminelen te slim af te zijn. Wij vinden dat onze resultaten in onafhankelijke tests het bewijs leveren.

Onze beveiligingstechnologieën zijn al drie jaar achter elkaar de meest geteste en meest bekroonde. Onze producten eindigden in een groot aantal onafhankelijke tests vaker op de eerste plaats en vaker in de top 3 dan de producten van welke leverancier ook.

MEERLAAGSE BEVEILIGING VAN UW GEHELE IT-INFRASTRUCTUUR

Onze meerlaagse beveiligingsaanpak - met definitiegebaseerde bescherming en heuristische en gedragsanalyse, Automatic Exploit Prevention en allerlei andere geavanceerde technologieën - vormt een belangrijke reden waarom onze beveiligingsoplossingen betere resultaten leveren dan andere.

Bovendien kunnen wij eerder reageren op nieuwe dreigingen dankzij de dreigingsinformatie die we verkrijgen van ons cloudondersteunde Kaspersky Security Network (KSN).

Daardoor kunnen wij het volgende realiseren:

- Hogere detectiescores
- Minder false positives

Wij bieden verschillende geïntegreerde beveiligingsoplossingen waarmee u al uw endpoints (desktops, laptops, servers, smartphones en tablets) kunt beschermen. Daarnaast bieden we een scala aan speciale beveiligingsopties waarmee u onder meer opslagsystemen en virtuele machines kunt beveiligen.

Onafhankelijke tests die het aantal 'foutieve identificaties van legitieme software als malware tijdens systeemscans' onderzoeken, hebben uitgewezen dat de technologieën van Kaspersky Lab geen enkele false positive opleverden.

De tests werden in januari en februari 2016 uitgevoerd door het AV-TEST Institute.

UW BEVEILIGINGSOPLOSSING KIEZEN

Kaspersky Endpoint Security Cloud is ontwikkeld om te voldoen aan de specifieke behoeften van middelgrote bedrijven, vooral bedrijven die erg kleine of helemaal geen IT-beveiligingsteams hebben. Omdat deze oplossing is toegespitst op kleine en middelgrote bedrijven, biedt deze:

- Bescherming van Windows-desktops en -laptops, Windows-file servers en mobiele Android- en iOS-apparaten*

- Gemakkelijk beheer via een cloudconsole die:
  – tijd en geld bespaart omdat u geen specifieke server nodig hebt
  – de initiële implementatie vereenvoudigt door gebruiksklare beveiligingsoplossingen te bieden

- Flexibele licentieverlening: een jaarlicentie of een maandabonnement dat de mogelijkheid biedt uw beveiliging aan te passen wanneer uw bedrijfsbehoeften veranderen
  *Functies variëren afhankelijk van het apparaat en het platform.

Kaspersky Endpoint Security for Business biedt gedetailleerde beveiliging voor grotere organisaties en bedrijven met bijzonder hoge beveiligingsvereisten. Deze oplossing beschermt een grote verscheidenheid aan platforms:

- Desktops en laptops: Windows, Mac en Linux
- File servers: Windows, Linux en FreeBSD
- Mobiele apparaten: Android, iOS en Windows

WAT IS DE VOLGENDE STAP?

Vraag volgende keer dat een leverancier een beveiligingsoplossing van de volgende generatie aanprijst om onafhankelijke testresultaten, zodat u zelf kunt zien wat voor resultaten deze beveiligingstechnologieën werkelijk leveren.

Maar u hebt nu ook gezien hoe goed Kaspersky Lab-beveiliging al ruim drie jaar presteert in onafhankelijke tests, dus waarom zou u onze beveiligingsoplossingen niet nu proberen op uw eigen computers en mobiele apparaten?

U kunt een proefversie van Kaspersky Endpoint Security Cloud 30 dagen GRATIS uitproberen. Ga naar de online cloudconsole op cloud.kaspersky.com

BIJLAGE 1

Voorbeeldbedrijven en hun ideale beveiligingsoplossing van Kaspersky Lab

We kijken naar drie verschillende soorten bedrijven, evalueren hun beveiligingsbehoeften en bepalen welke beveiligingsoplossing van Kaspersky Lab het best voldoet aan de vereisten van elk bedrijf.

BEDRIJF A

- Klein adviesbureau met 60 werknemers
- Personeel werkt thuis of heeft flexibele werkplaatsen in het kantoor
- Voor alle verschillende taken zijn laptops, smartphones en tablets nodig
- Er wordt voor veel taken gebruik gemaakt van internet
- Tijdelijke medewerkers zoals stagiairs en uitzendkrachten, hebben soms tot zes maanden toegang tot vertrouwelijke bedrijfsgegevens nodig
- Geen intern IT-ondersteuningsteam: het bedrijf heeft een externe IT-consultant ingehuurd die beperkte ervaring in IT-beveiligingsbeheer heeft
- Zeer beperkte IT-infrastructuur
  - Maakt gebruik van cloudgebaseerde servers in plaats van interne servers
  - Voor afdrukken, opslag en dergelijke worden de gebruikelijke kleine kantoorsystemen gebruikt
- Beperkt IT-budget
  - Meeste personeelsleden gebruiken eigen laptops, smartphones en tablets

BEDRIJFSVEREISTEN VOOR BEVEILIGINGSOPLOSSING

- Verregaande bescherming tegen internetdreigingen
- Vereenvoudigd beveiligingsbeheer waarvoor geen gespecialiseerde ervaring nodig is, zodat een externe IT-ondersteuningsmedewerker gemakkelijk de bedrijfsbeveiliging kan beheren
- Eenvoudige licentieverlening: kan online en jaarlijks worden betaald
- Geen investeringen in extra IT-hardware vereist
- Mogelijkheid om een breed scala aan apparaten te beveiligen, waaronder verschillende modellen laptops, tablets en smartphones (met inbegrip van iOS-apparaten)
- Eenvoudige schaalbaarheid, zodat de pc's en mobiele apparaten van nieuw personeel snel kunnen worden beveiligd

DE IDEALE BEVEILIGINGSOPLOSSING VAN KASPERSKY LAB

Kaspersky Endpoint Security Cloud met een jaarlicentie

- Beschermt tegen bekende, onbekende en geavanceerde dreigingen, waaronder internetdreigingen
- Biedt een gemakkelijk te gebruiken cloudconsole die het beveiligingsbeheer vereenvoudigt
- Vereenvoudigde licentieverlening: jaarlicenties die online kunnen worden ingesteld en vernieuwd
- Minder investeringen nodig. Omdat de beheerconsole in de cloud zit, hebt u geen server op locatie nodig voor beveiligingsbeheer
- Ondersteunt Windows-computers, iPhones, iPads en Android-smartphones en -tablets
- Kan worden aangepast aan veranderende behoeften. Als er nieuw personeel wordt aangenomen, kunnen dankzij de cloudgebaseerde console snel extra computers en mobiele apparaten worden beveiligd

Kaspersky Endpoint Security Cloud biedt bedrijf A de juiste combinatie van beveiliging en gebruiksvriendelijkheid, en vereist niet dat het bedrijf investeert in extra hardware of gespecialiseerde training voor het personeel. Vereenvoudigd beheer via de cloudgebaseerde console, waardoor het bedrijf een externe consultant kan inhuren om de beveiliging van alle bedrijfscomputers, -smartphones en -tablets in te stellen en te beheren.

BEDRIJF B

- Bouwbedrijf dat de komende drie jaar wil uitbreiden naar tien andere steden
- Heeft momenteel honderd mensen in dienst, maar dat aantal neemt de komende twaalf maanden toe
- Voor elk nieuw project is extra personeel nodig, onder meer opzichters en inkopers
- Het aantal tijdelijke medewerkers varieert in elke fase van het project
- De meeste werknemers werken het grootste deel van de tijd niet op kantoor
- Er wordt voor veel taken gebruik gemaakt van internet
- Groot aantal tijdelijke medewerkers, onder wie projectmanagers en gespecialiseerde uitzendkrachten, heeft zes tot twaalf maanden toegang tot vertrouwelijke bedrijfsgegevens nodig
- Geen apart budget om de beveiliging uit te breiden voor alle nieuwe werknemers: de kosten worden gedekt voor elk project dat het bedrijf binnenhaalt
- Eén fulltime IT-beheerder
- Zeer beperkte IT-infrastructuur:
  - Cloudgebaseerde server in plaats van interne servers
  - Voor afdrukken, opslag en dergelijke worden de gebruikelijke kleine kantoorsystemen gebruikt
- Beperkt IT-budget
  - Meeste personeelsleden gebruiken eigen laptops, smartphones en tablets

Bedrijfsvereisten voor beveiligingsoplossing

- Vereenvoudigd beveiligingsbeheer waarvoor geen gespecialiseerde ervaring nodig is, zodat een externe IT-ondersteuningsmedewerker gemakkelijk de bedrijfsbeveiliging kan beheren
- Geen investeringen in extra IT-hardware vereist
- Geen toegewezen jaarbudget voor IT-beveiliging nodig: de beveiliging kan worden aangepast wanneer er nieuwe projecten zijn
- Onmiddellijke schaalbaarheid zonder complexe licentieverlening of contracten, mogelijkheid tot onmiddellijke betaling voor de toevoeging van nieuwe gebruikers
- Mogelijkheid om een breed scala aan apparaten te beveiligen, waaronder verschillende modellen laptops, tablets en smartphones (met inbegrip van iOS-apparaten)
- Mogelijkheid om verscheidene gebruikspatronen te beheren, waardoor verschillende beveiligingsregels kunnen worden ingesteld voor verschillende functies

De ideale beveiligingsoplossing van Kaspersky Lab

Kaspersky Endpoint Security Cloud met een maandabonnement

- Beschermt tegen bekende, onbekende en geavanceerde dreigingen, waaronder internetdreigingen
- Biedt een gemakkelijk te gebruiken cloudconsole die het beveiligingsbeheer vereenvoudigt
- Minder investeringen nodig. Omdat de beheerconsole in de cloud zit, hebt u geen server op locatie nodig voor beveiligingsbeheer
- Een jaarbudget of jaarlicentie is niet nodig. Een maandabonnement biedt het bedrijf de mogelijkheid om het aantal beveiligde gebruikers elke maand te laten variëren
- Ondersteunt Windows-computers, iPhones, iPads en Android-smartphones en -tablets
- Afzonderlijke beleidsregels kunnen via de console in de cloud worden ingesteld
- Kan worden aangepast aan veranderende behoeften. Als er nieuw personeel wordt aangenomen, kunnen dankzij de cloudgebaseerde console snel extra computers en mobiele apparaten worden beveiligd

Omdat snelle, kostenbesparende schaalbaarheid cruciaal is voor bedrijf B, is een maandabonnement op Kaspersky Endpoint Security Cloud de perfecte keuze. Er hoeft niet vooraf te worden betaald voor een jaarlicentie. Het bedrijf kan het aantal gebruikers verhogen of verlagen afhankelijk van de behoeften. Daardoor beschikt het bedrijf over flexibele beveiliging en behoudt het tegelijkertijd controle over de kosten.

BEDRIJF C

- Ontwikkelt B2B-software, heeft 500 werknemers
- Verwacht de komende twaalf maanden 30% te groeien
- Zet wervingsprogramma's op voor extra ontwikkelaars, testers, IT-experts, salespersoneel en anderen
- Meeste personeel werkt op kantoor en via het Local Area Network (LAN)
- Senior managers werken met vertrouwelijke klantgegevens die veilig moeten worden opgeslagen
- Uitgebreide interne IT-infrastructuur, met inbegrip van servers, opslagsubsystemen, LAN
- Maakt gebruik van verschillende serverplatforms, waaronder een Windows-server voor productie, Linux voor netwerkbeheer en Mac-computers voor ontwerpers
- Werknemers hebben de beschikking over gestandaardiseerde bedrijfslaptops die worden ondersteund door het interne IT-team
- Er is een specifiek jaarbudget voor IT
- Moet voortdurend nieuwe technologieën toepassen om het potentiële marktaandeel te vergroten
- Zeer gespecialiseerd intern IT-ondersteuningsteam beheert de infrastructuur van het bedrijf
- Vanwege de grote verscheidenheid aan functies, zoals ontwikkelaars, teamleiders, klantenservice, administratie en ander kantoorpersoneel, moet het bedrijf veel verschillende beveiligingsregels instellen en beheren

Bedrijfsvereisten voor beveiligingsoplossing

- Geavanceerde beveiligingsfuncties die kunnen worden beheerd door de interne IT-beveiligingsspecialisten
- Kan volledig worden geïmplementeerd in het bedrijfs-LAN
- Mogelijkheid om een zeer breed scala aan platforms te ondersteunen, met inbegrip van Windows, Linux en Mac
- Ondersteuning voor het beheer van mobiele apparaten
- Mogelijkheid om een groot aantal verschillende beveiligingsregels te ondersteunen, waaronder webbeheer, opstartrestricties voor applicaties en nog veel meer
- Geavanceerde encryptie om vertrouwelijke gegevens te beschermen

De ideale beveiligingsoplossing van Kaspersky Lab

Kaspersky Endpoint Security for Business ADVANCED

- Beschermt tegen bekende, onbekende en geavanceerde dreigingen, waaronder internetdreigingen
- Uitgebreidere beveiligingsfuncties, met inbegrip van flexibele beheertools
- Alle endpointbeveiligingsfuncties en het beveiligingsbeheer worden lokaal uitgevoerd
- Biedt één enkele, geïntegreerde beheerconsole voor alle ondersteunde apparaten die draait op een server op locatie
- Beveiligt Windows, Linux en Mac
- Omvat MDM-functies (Mobile Device Management)
- Biedt gedetailleerd beleidsbeheer, zodat u complexe beveiligingsregels kunt instellen
- Omvat flexibele data encryptiefuncties

Bedrijf C heeft een complexere IT-infrastructuur met een grotere verscheidenheid aan platforms die moeten worden beveiligd, zoals Windows-, Mac- en Linux-computers. Daarnaast heeft het bedrijf extra beveiligingsfuncties nodig, zoals data encryptie en flexibele beheertools. Kaspersky Endpoint Security for Business ADVANCED is daarom de juiste oplossing. Deze optie geeft het bedrijf ook gedetailleerdere controle over de IT-beveiliging, waardoor het gespecialiseerde interne IT-team afzonderlijke beveiligingsregels kan instellen voor alle verschillende functies binnen het bedrijf.