G DATA

SIMPLY SECURE

PERFECTE BESCHERMING VOOR ONDERNEMINGEN

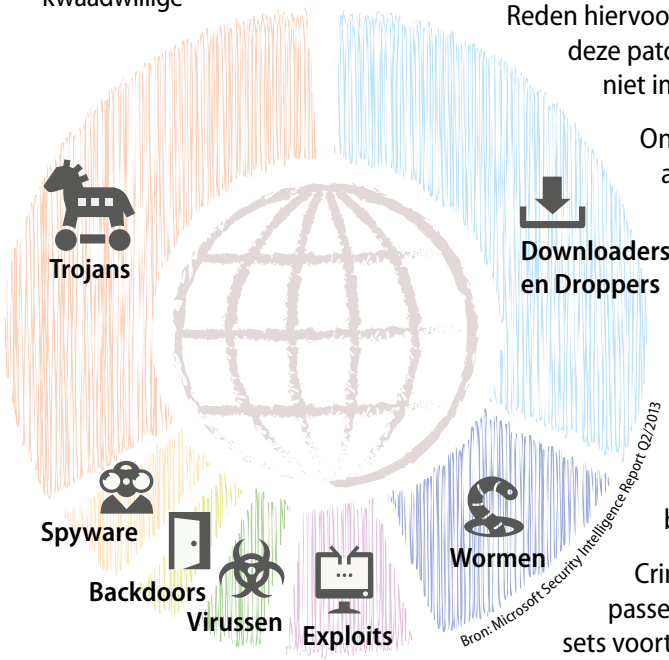
IT-BEVEILIGINGSSOFTWARE

DE HEDENDAAGSE UITDAGINGEN OP HET VLAK VAN BEVEILIGING

Bij hun dagelijkse activiteiten vertrouwen bedrijven in hoge mate op technologie. Ze hebben hun complete know how en hun belangrijkste financiële gegevens en klantinformatie op hun pc's en servers opgeslagen. Juist deze kritische systemen zijn toenemend het doelwit van professionele cybercriminelen.

TOENAME VAN DOELGERICHTE AANVALLEN

Bedreigingen voor een digitale infrastructuur variëren van algemene malwareaanvallen tot doelgerichte industriële spionage en van besmette gegevens tot productiviteitsverlies. Elke IT-component kan ten prooi vallen aan verwoestende gebeurtenissen, of het nu gaat om opzettelijke kwaadwillige aanvallen of om onvoorzien gegevensverlies waardoor cruciale workflows worden beïnvloed. Malware vormt daarbij de grootste bedreiging voor bedrijfsnetwerken met boosaardige programma's die hoge herstelkosten en verloren productiviteit tot gevolg hebben. Aanvallers worden echter steeds geraffineerder. Hun doel is niet langer ravage aan te richten. Met doelgerichte acties proberen ze nu heimelijk de zaken van de concurrentie te verstoren, financiële gegevens te stelen of de productontwikkeling te saboteren.



CYBERCRIMINALITEIT WORDT STEEDS PROFESSIONELER

Criminelen zoeken fouten en zwakke punten in populaire toepassingen en proberen deze te benutten om toegang te krijgen tot de apparaten waarop ze worden uitgevoerd.

Verrassend is wel dat heel wat systemen kwetsbaar blijven, zelfs nadat een patch werd uitgegeven. Reden hiervoor is dat beheerders deze patches gewoonweg niet implementeren.

Onderzoek heeft aangetoond dat organisaties zich bewust zijn van de risico's van aanvallen op toepassingen, maar dat PatchManagement voor velen een onbekend terrein blijft.

Criminelen passen hun tool-sets voortdurend aan om IT-bedrijfsnetwerken te hacken. Het aantal nieuwe malwaretypes neemt nog steeds toe, en het gaat ook alsmaar vaker om aanvallen die op maat van een specifiek netwerk zijn gemaakt, zoals Advanced Persistent Threats.

BEDREIGINGEN VAN BINNENUIT

De cybercriminelen worden bovendien een aardig handje geholpen door het zwakste punt in de beveiliging van de meeste organisaties: hun personeel.

Hackers maken steeds meer gebruik van sociale technieken om werknemers in de val te lokken zodat ze de deur openen naar de IT-systemen van hun organisatie. Dit kan door het openen van bedrieglijke berichten, het gebruik van geïnfecteerde USB-sticks, het bezoeken van websites, het invoeren van een wachtwoord of het downloaden van malware die zich in de bedrijfssystemen nestelt.

Het volstaat dus niet langer een netwerk te beveiligen tegen aanvallen van buitenaf. Organisaties moeten hun werknemers ook consequent en voortdurend bewust maken van potentiële dreigingen en uitdagingen.

TOENEMENDE COMPLEXITEIT VAN IT-BEVEILIGING

Zelfs als er geen kwaadaardige bedoelingen in het spel zijn, kan IT-technologie falen. Een harde schijffout kan vitale bestanden vernietigen en een defecte e-mailserver kan de interne en externe communicatie ernstig verstoren.

Bij IT-beveiliging gaat het er ook om dat organisaties zich zo goed mogelijk voorbereiden op het ergste scenario. Een hardwarefout kan weliswaar niet altijd worden vermeden, maar een organisatie kan er wel voor zorgen dat de IT-infrastructuur en gegevens

„DE BESCHERMING VAN INTELLECTUELE EIGENDOM, FINANCIËLE INFORMATIE EN DE REPUTATIE VORMT EEN CRUCIAAL ONDERDEEL VAN DE BEDRIJFSSTRATEGIE."

PricewaterhouseCoopers

in een handomdraai weer gebruiksklaar zijn. Bestaande bedrijfsnetwerken worden vaak beveiligd door een mengelmoes van beveiligingscomponenten met meerdere managementconsoles, niet-gestandaardiseerde workflows en conflicterende standaarden. Dit maakt het voor aanvallers veel gemakkelijker om door de mazen van het net te glippen. De complexiteit van het netwerk moet minimaal worden gehouden. Dit geldt ook wanneer er een volledig nieuw netwerk wordt opgezet.

Vanaf de eerste stappen moet beveiliging worden beschouwd als een vitale functie. Enkel zo kan de samenwerking tussen alle componenten worden gegarandeerd en wordt een economisch en efficiënt beheer mogelijk. Bedrijven die niet over voldoende tijd, geld of de kennis beschikken, vertrouwen op externe partners die IT-beveiliging als Managed Service aanbieden. De infrastructuur wordt beschermd zonder dat uw klant zich zorgen hoeft te maken over de configuratie en het beheer van de beveiligingsoplossing.

DE MOBIELE UITDAGING

De toename van mobiele apparatuur brengt meer complexiteit in de netwerkbeveiliging. In slechts enkele jaren tijd hebben smartphones en tablets wereldwijd bedrijfsnetwerken veroverd.

Werknemers krijgen toegang tot bedrijfsgegevens via hun mobiele apparaten die zowel door het bedrijf kunnen worden verstrekt als privé aangekocht. Uitgaven voor beheerlicenties van mobiele apparaten zijn dan ook spectaculair toegenomen. Het beveiligen van apparaten die zich regelmatig rond de netwerkperimeter bewegen, vereist een solide mobiele beveiligingsoplossing. Beheerders moeten ervoor zorgen dat de gegevensmobiliteit geen inbreuk betekent op de beleidslijnen omtrent de bedrijfsbeveiliging, terwijl werknemers optimaal gebruik moeten kunnen maken van mobiele apparaten.

ONDERZOEK OVER CYBERBEVEILIGING

Het volgende is gebleken uit een recent onderzoek dat werd uitgevoerd door TNS, een toonaangevende groep voor marktonderzoek en marktgegevens, en gepubliceerd door G DATA:

- Na de onthullingen van Edward Snowden is er een verhoogd bewustzijnsniveau ten aanzien van IT-beveiliging.
- De omvang van de schade, veroorzaakt door aanvallen, is toegenomen.
- Standaard maatregelen voor risicobeperking, zoals regelmatige back-ups en updates, worden op grote schaal toegepast, maar er is meer nodig om een organisatie te beveiligen.
- Hoewel er steeds meer mobiele apparaten worden gebruikt in bedrijven, is er een gebrek aan beveiligingsrichtlijnen voor hun gebruik.

Aanbevelingen op basis van de bevindingen van het onderzoek:

- IT-beveiliging en gegevensbescherming moet steeds de hoogste prioriteit krijgen.
- Het IT-beveiligingsbewustzijn in de maatschappij, de politiek en de bedrijven moet worden verhoogd.

MEER DAN ÉÉN DERDE VAN DE APPARATEN DIE WORDEN GEBRUIKT IN BEDRIJVEN ZIJN MOBIEL

Bron: G DATA

ONZE BEVEILIGINGSOPLOSSINGEN

Als een van de meest ervaren bedrijven in de IT-beveiliging, weten wij als geen ander hoe we ons snel kunnen aanpassen aan nieuwe en onbekende bedreigingen waarmee bedrijven in verschillende expertisegebieden te maken krijgen. Daarom kunnen we organisaties de juiste oplossing bieden voor hun specifieke beveiligingsbehoeften.

G DATA bedrijfsoplossingen bieden een betrouwbare beveiliging. Onze oplossingen beschermen uw klanten tegen malware, boosaardige insiders of productiviteitsverlies en zijn op maat gemaakt volgens hun behoeften. Bovendien kunnen onze producten worden afgestemd op de grootte van elk bedrijf. Daarnaast kan het functionele bereik op elk ogenblik worden aangepast door middel van optionele modules.

Wij combineren onze bekroonde beveiligingsoplossingen met een overzichtelijke beheerconsole en goed georganiseerde rapportagemogelijkheden.

Dit kan worden toegepast op elke netwerkgrootte, of er nu tien of tienduizend clients worden beheerd.

Met G DATA oplossingen kunnen niet alleen IT-componenten efficiënt worden beveiligd, maar ook de onderhouds- en beheerkosten worden beperkt.

PERFECTE CLIENTBEVEILIGING

Hybride CloseGap-beveiliging	Maximale beveiliging door proactieve herkenning op basis van virusdefinities
G DATA BankGuard	Veilig online betalingsverkeer – geen add-on voor de browser of andere software nodig
Gedragscontrole	Beveiligt ook tegen onbekende virussen
NIEUW! **Beveiliging tegen gemanipuleerde USB-apparaten**	De geïntegreerde USB KEYBOARD GUARD beschermt clients betrouwbaar tegen gemanipuleerde USB-apparaten die zich als toetsenbord voordoen
Geïntegreerde beveiliging tegen spam en e-mails met virussen	Add-on voor Microsoft Outlook en voor POP3- en IMAP-accounts
Sterke firewall	Bewaakt alle inkomende en uitgaande verbindingen en beschermt tegen DoS-aanvallen, poortscans en veel meer
GEOPTIMALISEERD! **Antivirus voor Linux-clients**	Beveiligt ook Linux-computers in het bedrijfsnetwerk tegen gevaren op internet. Nu met ondersteuning voor nog meer distributies

CENTRAAL BEHEER

Managed Services	Diensten met hoge marges aanbieden met de geïntegreerde administratieservice
Eenvoudige administratie en snel overzicht	Installaties, virusscans en rechten voor alle clients centraal beheren
Vereenvoudigd installatieoverzicht	Met statusmeldingen en weergave van het installatieverloop
Overzichtelijk dashboard	Voor een gebruiksvriendelijk overzicht van alle relevante informatie met contextgebaseerde helpfunctie
Extern beheer	Ook overal mogelijk via webinterface - zelfs met mobiele browsers
Apparaatcontrole	Bepaal wie USB-sticks, geheugenkaarten of branders mag gebruiken
Toepassingsbeheer	Bepaal welke programma's mogen worden geïnstalleerd of gestart
Surffilter en controle op het gebruik van internet	Blokkeer desgewenst websites die niet tot het dagelijkse werk behoren en beperk de surfduur
Active Directory-verbinding	Voor de overname van bestaande groepsstructuren en automatische client-installatie
GEOPTIMALISEERD! **Mobile Device Management**	Centraal beheer van Android- en iOS-toestellen met diefstalbeveiliging, app-beheer, bedrijfstelefoonboek, oproepfilter en veel meer (features kunnen per systeem verschillen)
Software- en hardwarelijst	Gedetailleerde weergave van de volledige inventaris
Deskundige ondersteuning per telefoon of e-mail	De supportafdeling werkt nauw samen met de developers in Duitsland

OPTIONELE MODULES

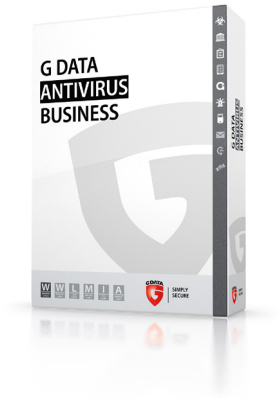
GEOPTIMALISEERD! **MailSecurity**	Centrale gateway-oplossing onafhankelijk van mailservers met virus- en spamfilter (SMTP/POP3) voor een onbeperkt aantal mailservers zoals Exchange, Notes enz. Inclusief plug-in voor MS Exchange 2007 tot 2013
Centrale client back-ups	Beveilig en beheer de gegevens op de bedrijfscomputers van uw klanten
PatchManagement	Centraal gestuurde patches voor software van Microsoft en derden

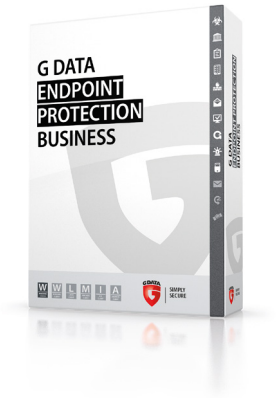
AANVULLENDE PRODUCTEN

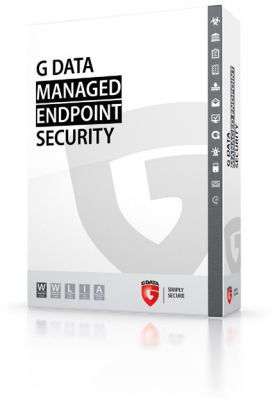
G DATA ANTIVIRUS VOOR MAC	Voor een naadloze bescherming van het netwerk: uitgebreide realtimebeveiliging tegen virussen, Trojans en andere vormen van malware speciaal voor MAC OS-clients

„DOOR HET VERMINDEREN VAN DE TIJD EN KOSTEN DIE WORDEN BESTEED AAN REACTIES OP MALWARE, HEEFT G DATA BIJGEDRAGEN TOT EEN HOGERE PRODUCTIVITEIT, EFFICIËNTIE EN BbetrouwbaarheID."

Chris Bates, IT Project and Infrastructure Manager, Redeem UK







ANTIVIRUS BUSINESS	CLIENT SECURITY BUSINESS	ENDPOINT PROTECTION BUSINESS	MANAGED ENDPOINT SECURITY
De basisbeveiliging voor het netwerk	Netwerkbeveiliging PLUS firewall en AntiSpam	Complete beveiliging PLUS PolicyManager	Complete beveiliging als Managed Service
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■
	■	■	■
	■	■	■
■	■	■	■
			■
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■
		■	■
		■	■
		■	■
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■
□	□	□	□
□	□	□	□
□	□	□	□
□	□	□	

■ Inbegrepen □ Optioneel

OP MAAT GEMAAKTE BEVEILIGINGSFUNCTIES

Elk bedrijf heeft verschillende vereisten en prioriteiten. Daarom biedt G DATA modulaire oplossingen zodat de bescherming kan worden gekozen die een netwerk nodig heeft.

Alle producten bevatten onze kernbeveiligingstechnologieën. Naast de traditionele antivirustechnologie, omvat dit ook de hybride DoubleScan-beveiliging die twee antivirusengines integreert in één prestatiegeoptimaliseerd virusscanproces.

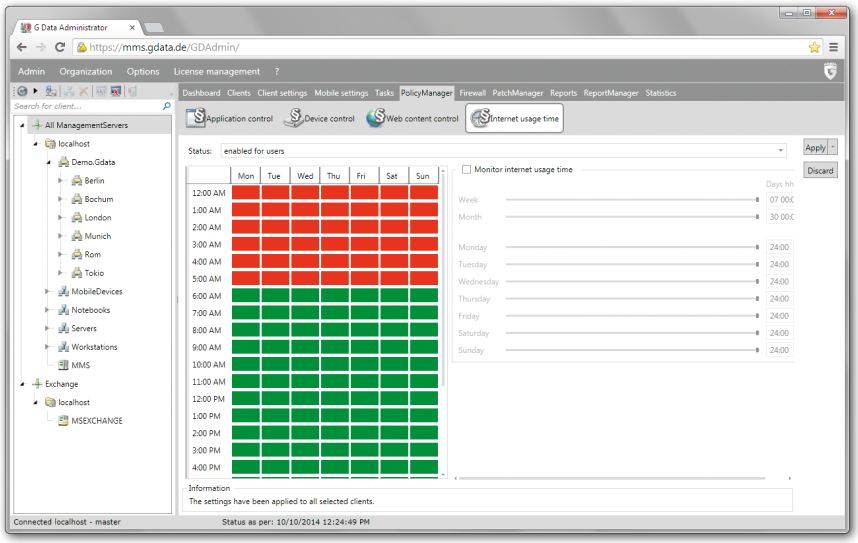
Proactieve technologieën zoals Behavior Blocker (gedragscontrole) en BankGuard verhinderen dat zelfs onbekende bedreigingen schade veroorzaken aan het netwerk.

POLICY MANAGER

PolicyManager biedt essentiële hulp bij het beveiligen van een netwerk en stelt bedrijven in staat hun gebruiksbeleidslijnen zonder al te veel kosten op te leggen. Met G DATA PolicyManager kunnen de gevaarlijkste aanvalsvectoren, zoals USB-sticks, websites en onbekende toepassingen worden beveiligd.

Door het gebruik van verwisselbare media, zoals USB-sticks, volledig te blokkeren, krijgt malware op deze media geen kans om het endpoint te besmetten.

Het is ook mogelijk om bedrijfsbeleidslijnen, zoals beperkt internetgebruik of een strikt toepassingsbeleid, op te leggen. Zo wordt de naleving en productiviteit over het hele netwerk gegarandeerd.



MOBILE DEVICE MANAGEMENT

Mobiele apparaten kunnen zowel een zegen als een vloek zijn. Smartphones en tablets hebben heel wat nieuwe workflowmodellen mogelijk gemaakt, maar kunnen een bedreiging vormen als ze niet correct zijn beveiligd. Apparaten die worden gebruikt voor zowel persoonlijke als bedrijfsdoeleinden kunnen onopzettelijk vertrouwelijke informatie lekken of malware in het bedrijfsnetwerk binnenhalen.

Mobile Device Management helpt bij het beheer en de beveiliging van mobiele apparaten met talrijke opties gaande van mobiele antivirustoepassingen tot diefstalbeveiliging en van het gebruik van blacklists tot een bedrijfstelefoonboek.

„DE GECENTRALISEERDE BEVEILIGING VAN G DATA BIEDT TALRIJKE AANPASSINGSOPTIES VOOR GEBRUIKERSGROEPEN EN IS BIJZONDER GEBRUIKSVRIENDELIJK.“

Olivier De Cock, municipal IT manager, Grâce-Hollogne

PATCH MANAGEMENT

Kwetsbaarheden in veelgebruikte software zijn de favoriete aanvalsvectoren van criminelen geworden. Om te verhinderen dat malware misbruik maakt van beveiligingsproblemen, moeten er regelmatig patches worden uitgevoerd op de software van alle endpoints. Maar zelfs wanneer een patch beschikbaar is, laten heel wat beheerders door tijd- of geldgebrek na deze patch te implementeren.

Dankzij de optionele PatchManagement-module kunnen organisaties het testen en implementeren van patches optimaliseren. Hierbij worden alle eventuele kwetsbaarheden in Windows, Java, Adobe Reader, Adobe Flash Player en andere producten van derden efficiënt gesloten.

OPTIONELE MODULES

Alle netwerkoplossingen kunnen worden uitgebreid met de modules PatchManagement, MailSecurity en ClientBackup.

MAIL SECURITY

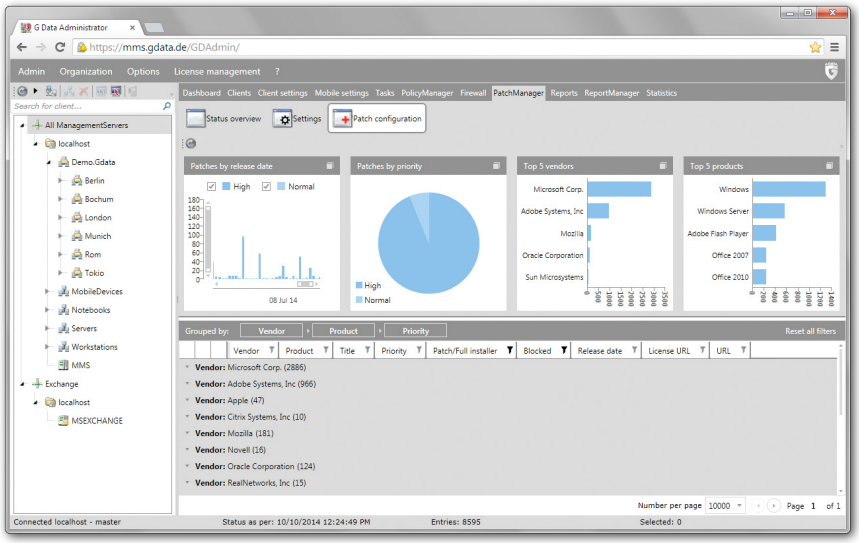
E-mail is een van de vaakst gebruikte infectievectoren. Bijlagen kunnen elk type programma bevatten, zowel nuttig als boosaardig, terwijl spamberichten tijd en middelen kosten.

MailSecurity beschermt e-mailberichten, zelfs voordat ze de clients bereiken. Binnenkomende en uitgaande e-mails worden altijd opgeschoond, ongeacht of MailSecurity wordt gebruikt als een invoegtoepassing voor Microsoft Exchange Server 2007 tot 2013 of als een onafhankelijke gateway.

CLIENT BACKUP

Uitgebreide malwarebeveiliging is cruciaal, maar in sommige gevallen volstaat een hardwaredefect of een stroomuitval al om gegevens te vernietigen.

Onze gecentraliseerde ClientBackup-module lost dit probleem op door regelmatig en automatisch een back-up te maken van de gegevens op alle bedrijfscomputers binnen een organisatie.



BELANGRIJKE VOORDELEN

ZORGELOZE IMPLEMENTATIE

Enkele muisklikken volstaan om de G DATA oplossingen te installeren, ongeacht de grootte van het netwerk. Dankzij onze eenvoudige installatiewizard kan de centrale servercomponent in een handomdraai worden geïnstalleerd. Via de beheerinterface van deze wizard, worden alle componenten snel aan het werk gezet, zelfs in heterogene omgevingen.

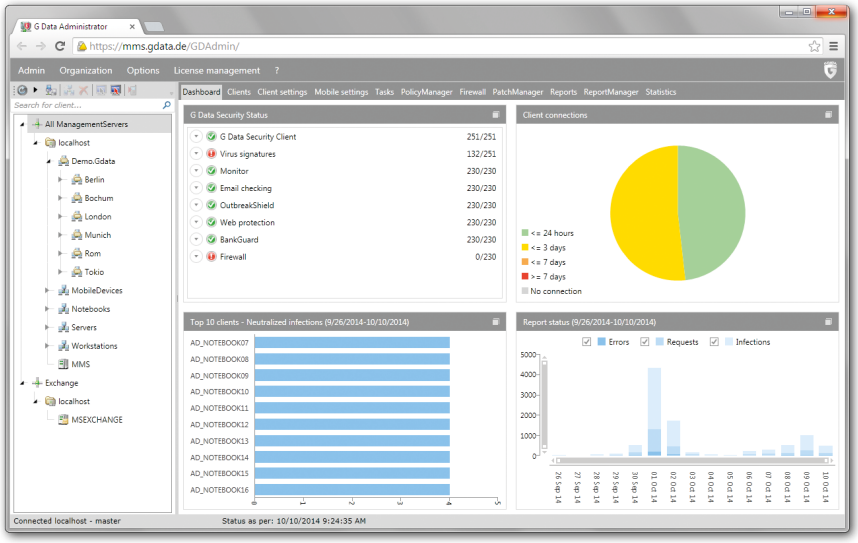
Desktopcomputer, laptop of mobiele client: onze oplossing kan overal worden ingezet zonder dat hiervoor fysieke toegang tot een netwerkapparaat is vereist. Via hun integratie met Active Directory maken G DATA oplossingen gebruik van bestaande netwerkstructuren, waardoor een volledig geautomatiseerde clientimplementatie mogelijk is.

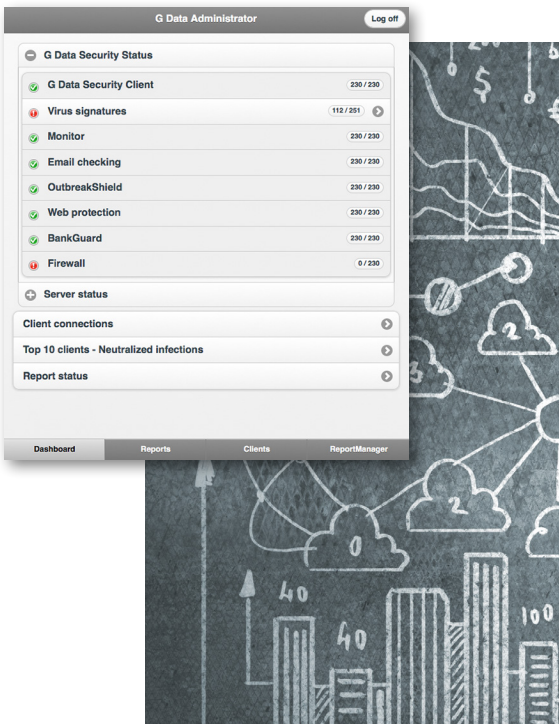
GOED GEÏNTEGREERD BEHEER

Implementatie, configuratie en bewaking: alle aspecten van het centraal beheer kunnen worden uitgevoerd met eenzelfde configuratiehulpprogramma. Elke oplossing wordt geleverd met G DATA Administrator. Met dit uitgebreide, maar gebruiksvriendelijke hulpmiddel kunnen beheerders het netwerk beheren zoals zij dat willen. Het goed gestructureerde dashboard biedt een overzicht van alle aspecten van de netwerkbeveiliging en maakt een snelle reactie op waarschuwingen mogelijk.

Het beheer wordt eenvoudig gemaakt door logisch georganiseerde moduletabbladen en uitgebreide contextgevoelige helpdocumenten. Met de configureerbare e-mailrapporten kunnen gebruikers aan de vereisten voldoen zonder dat ze hiervoor via de beheerderinterface hoeven te gaan.

Onze beheeroplossingen kunnen worden aangepast aan elke situatie. De beheerprogramma's zijn toegankelijk vanaf elke locatie. G DATA WebAdministrator is een beveiligde tool die via internet dezelfde opties biedt als G DATA Administrator. Het kan worden gebruikt vanaf elke pc met een webbrowser, binnen of buiten het bedrijfsnetwerk. Wanneer gebruikers onderweg zijn, kunnen ze met hun smartphone of tablet toegang krijgen tot G DATA MobileAdministrator. De beheerinterface is speciaal aangepast voor mobiele apparaten. Hierdoor wordt alles gebruiksvriendelijker, zelfs op kleine schermen.





LAGERE TOTAL COST OF OWNERSHIP

Onze oplossingen zijn ontworpen om de total cost of ownership te verlagen. G DATA Administrator verenigt alle beheeropties in één interface zodat organisaties tijd en geld besparen. Beheerders krijgen altijd toegang tot alle relevante instellingen en worden nooit vertraagd door complexe menu's.

Dankzij de gebruiksvriendelijke indeling van G DATA Administrator kunnen beheerders heel gemakkelijk leren werken met alle opties. Zelfs complexe functies worden kinderspel met deze goed gestructureerde interface.

INDIVIDUELE ONDERSTEUNING

Al onze oplossingen omvatten uitgebreide beveiligingsfuncties, optioneel uitgebreid door modules die overeenstemmen met de behoeften van het netwerk.

Als u niet zeker bent of een specifieke oplossing of module geschikt is voor het netwerk van uw klant, kunt u de hulp inroepen van onze online productadviseurs om de geschikte oplossing te vinden.

U kunt ook altijd persoonlijk contact opnemen voor individueel advies betreffende de specifieke behoeften van uw klanten.

MANAGED SERVICE

Voor organisaties die hun IT-beveiligingsoplossing liever uitbesteden, is G DATA MANAGED ENDPOINT SECURITY de perfecte oplossing.

Het biedt alle voordelen van onze G DATA beveiligingsoplossingen en van het gemak van een professioneel servicebeheer.

De IT-beveiligingspartner is verantwoordelijk voor de implementatie, de configuratie en het beheer. Via de externe mogelijkheden van MANAGED ENDPOINT SECURITY worden tijdrovende afspraken met technici vermeden.

Dit biedt uw klanten en hun werknemers de gelegenheid om zich te concentreren op hun kerntaken, zonder dat ze zich zorgen hoeven te maken over de netwerkbeveiliging.

SIMPLY SECURE

Omdat wij begrijpen wat de moderne uitdagingen op het vlak van beveiliging zijn, kunnen wij IT-beveiligingsoplossingen op maat creëren en zo oplossingen en voordelen bieden die voor klanten belangrijk zijn.

Als pioniers in de sector van antivirussoftware, bestrijden we al 30 jaar digitale bedreigingen. Onze beveiligingsexperts bij G DATA SecurityLabs (in Bochum, Duitsland) verzamelen informatie, evalueren nieuwe cyberbedreigingen en ontwikkelen oplossingen voor een proactieve bestrijding van cybercriminaliteit.

De recente onthulling van de Uroburos-spionagerootkit is een schoolvoorbeeld van ons baanbrekend onderzoek en de snelheid waarmee we reageren op nieuwe bedreigingen. Onze research vormt de basis voor onze innovaties en stimuleert het bewustzijn rond problemen omtrent beveiliging, privacy en IT.

Dankzij onze Duitse roots kunnen we meer leveren dan beveiliging alleen: wij bieden klanten en ondernemingen ook gemoedsrust. De strenge Duitse wetten op de bescherming van de persoonlijke levenssfeer garanderen ons dat er geen tussenkomst is van inlichtingendiensten.

Sinds de oprichting in 1985 is G DATA uitgegroeid tot een van de meest toonaangevende bedrijven in de IT-beveiligingssector. G DATA is actief in meer dan 90 landen en heeft meer dan 400 werknemers in dienst.

ONZE BEVEILIGINGSOPLOSSINGEN

Wij bieden uitgebreide beveiligingssoftwareoplossingen voor thuisgebruikers en zakelijke klanten.

Thuis: onze oplossingen zijn gemakkelijk te installeren en te bedienen. Ze leveren uitstekende prestaties en een uitgebreide beveiliging voor computers, laptops, tablets en mobiele apparaten die werken op Windows-, Mac OS- en Android-platformen. Wij beveiligen persoonlijke gegevens en identiteiten tegen alle aanvallen op deze apparaten of op thuisservers.

De betrouwbare en bekroonde beveiligingsmechanismen van de software vormen een effectieve bescherming tegen virussen, Trojaanse paarden, wormen, backdoors en andere cyberbedreigingen zoals exploits.

Er zijn niet alleen optionele modules voor back-ups en ouderlijk toezicht, maar ook geavanceerde browserbeveiligingsfuncties die manipulatie tijdens online bankieren en winkelen verhinderen.

Zakelijk: onze oplossingen beantwoorden aan elke uitdaging en bieden een betrouwbare, actuele bescherming tegen malwareaanvallen en andere risico's die voortvloeien uit het gebruik van digitale netwerken. De belangrijkste activa – personeel en intellectueel eigendom – worden door ons beschermd zodat organisaties optimaal voordeel kunnen halen uit nieuwe ontwikkelingen, bijvoorbeeld in de technologie van mobiele apparatuur.

Ons assortiment van technologisch geavanceerde producten kan uiterst nauwkeurig op maat worden gemaakt. G DATA biedt gebruiksvriendelijk clientbeheer zodat gebruikers snel en probleemloos aan de slag kunnen gaan.

Optionele modules, zoals voor PatchManagement, Backup en MailSecurity, vervolledigen de aanpassingsmogelijkheden.

BELANGRIJKE FEITEN

- Opgericht in 1985
- De eerste antivirussoftware ter wereld
- Hoofdkantoor, ontwikkel- en ondersteuningsteam in Duitsland
- In meer dan 90 landen actief met ruim 400 personeelsleden
- Uitgebreide IT-beveiligingsoplossingen voor thuisgebruikers en bedrijven.
- Technologie "Made in Germany"
- Ongeëvenaard record van overwinningen in vergelijkingstests
- Hoog percentage klantentrouw
- Voortreffelijke klantendienst en ondersteuning

„WIJ DOEN RESEARCH EN MAKEN ANALYSES OM EEN VEILIGE IT-TECHNOLOGIE TE GARANDEREN, NU EN IN DE TOEKOMST."

Ralf Benzmüller, hoofd van G DATA SecurityLabs

BEKROONDE BEVEILIGING

Ons onderzoek en onze productontwikkeling werden in de loop der jaren veelvuldig bekroond. G DATA producten zijn gecertificeerd om te voldoen aan de hoogste beveiligingsnormen.

In vergelijkingstests uitgevoerd door Stiftung Warentest, een gerenommeerde Duitse consumentenorganisatie, heeft ons product G DATA INTERNET SECURITY consequent een betere malwaredetectie aangetoond dan zijn concurrenten. En dat maar liefst zeven keer op rij sinds 2005.

Onze bedrijfsoplossingen combineren onze bekroonde beveiliging met een uitgebreid functieaanbod voor bedrijfsomgevingen.

- AV-TEST Approved Corporate Endpoint Protection (feb. 2015): AV-TEST heeft G DATA ANTIVIRUS BUSINESS 13 punten toegekend - de hoogste score voor beveiliging en bruikbaarheid - terwijl het product ook werd geprezen voor zijn voortreffelijke prestaties.
- Virus Bulletin VB100 (okt. 2014): *„De duidelijk vormgegeven G DATA console maakt de implementatie en bewaking van clientsoftware uiterst eenvoudig."*

ALTIJD TOT UW DIENST

De klantenservice en de medewerkers van de supportafdeling van G DATA staan paraat om alle vragen, zowel van de thuisgebruiker als van de zakelijke klant, snel en efficiënt te beantwoorden. Lokale telefoonnummers evenals e-mail maken contact opnemen snel en goedkoop.

Bij ons kan men erop vertrouwen dat we reageren op elke nieuwe technologische uitdaging, hoge malwaredetectiepercentages behouden en uitzonderlijke ondersteuningsniveaus bieden.

Onze producten zijn gemakkelijk te installeren en te gebruiken. Ze bieden een uitgebreide beveiliging en hun prestaties worden bevestigd door de talrijke prijzen en de resultaten uit vergelijkende tests waar G DATA als winnaar uit de bus komt.

Met G DATA kiezen uw klanten gewoonweg voor **SIMPLY SECURE.**

ONZE TECHNOLOGIEPARTNERS

B2B.GDATASOFTWARE.COM

SIMPLY SECURE

150136_GD_B2BI3V2-Brochure_NL_09 • 2510020915 • Onderhevig aan wijzigingen, fouten en drukfouten.