DELL Technologies

Dell Trusted Devices

's Werelds meest veilige zakelijke pc[1]

Dell Technologies begrijpt dat de huidige beveiligingsuitdagingen bestaan uit het beheren van een evoluerend bedreigingslandschap met een moderne werkomgeving in het achterhoofd. Cybercriminelen maken gebruik van geavanceerde aanvallen die gericht zijn op meerdere kwetsbaarheden. Een effectieve beveiligingsstrategie voor eindpunten moet het volledige aanvalsoppervlak aanpakken. Daarom hanteert Dell een uitgebreide aanpak voor het beveiligen van apparaten boven en onder het besturingssysteem voor optimale veerkracht en apparaten waarop u kunt vertrouwen.

Boven het besturingssysteem:
Geïntegreerde beveiliging maakt deel uit van het plan.

Onder het besturingssysteem:
Intrinsieke beveiliging zit in het design.

Voorkom, detecteer en reageer op cyberaanvallen met **Dell SafeGuard and Response**.

Bescherm data op het apparaat en in de cloud met **Dell SafeData**.

Detecteer geknoei met het BIOS met **Dell SafeBIOS**.

U kunt erop vertrouwen dat er bij de levering niet met de hardware is geknoeid dankzij **Dell SafeSupply Chain**.

Beveilig gebruikersreferenties met **Dell SafeID**.

Houd informatie privé met **Dell SafeScreen** en **Dell SafeShutter**.

Onzichtbare, naadloze bescherming zorgt voor slimmere, snellere ervaringen.

Dell Trusted Devices bieden een veilige basis voor modern mobiel personeel. Onze uitgebreide reeks beveiligingsoplossingen voor eindpunten werken samen om apparaten zowel boven als onder het besturingssysteem te beveiligen. Deze krachtige combinatie houdt data veilig en gebruikers productief, ongeacht waar ze werken.

Boven het besturingssysteem

Voorkom geavanceerde cyberaanvallen met Dell SafeGuard and Response.

Dell SafeGuard and Response, mogelijk gemaakt door VMware® Carbon Black and Secureworks® biedt een uitgebreide aanpak van beheer van eindpuntbedreigingen. Kunstmatige intelligentie en machine learning detecteren en blokkeren proactief aanvallen op eindpunten, terwijl beveiligingsexperts helpen bij het opsporen en herstellen van geïdentificeerde bedreigingen op het eindpunt, op het netwerk en in de cloud.

Bescherm data op het apparaat en in de cloud met Dell SafeData.

Zorg ervoor dat gebruikers overal veilig kunnen samenwerken. Dell Encryption biedt granulaire beveiligingsmogelijkheden voor de versleuteling van alle data op de schijf, gedeelde data van meerdere gebruikers en data van afzonderlijke gebruikers met meerdere versleutelingscodes, en dit alles beheerd vanaf één dashboard om te voldoen aan naleving. Netskope gebruikt cloudbeveiliging en -toegang vanuit een datacentrische invalshoek, waarbij data en gebruikers overal worden beschermd, terwijl Absolute IT zichtbaarheid, bescherming en persistentie biedt buiten de bedrijfsfirewall.

Onder het besturingssysteem

Ontdek geknoei met Dell SafeBIOS.

BIOS-aanvallen zijn uiterst moeilijk te herkennen. Dell SafeBIOS waarschuwt u wanneer er met het BIOS is geknoeid, zodat u snel actie kunt ondernemen om het apparaat in quarantaine te plaatsen en te onderzoeken. Met exclusieve verificatie van Dell buiten de host blijft de vergelijkingsimage na de aanval op een beschermde en aparte locatie voor onderzoek na een aanval.[1]

U kunt erop vertrouwen dat er bij de levering niet met de hardware is geknoeid dankzij Dell SafeSupply Chain.

Dell Trusted Devices bevatten toonaangevende beveiliging in de toeleveringsketen en integriteitscontroles. Manipulatieaantonende zegels zorgen ervoor dat het apparaat ongeschonden aankomt. Voor hoogwaardige systemen kunt u de harde schijf opnieuw instellen volgens NIST-specificaties om een schone lei voor uw bedrijfsimago te garanderen.

Beveilig gebruikersreferenties met Dell SafeID.

Alleen Dell beveiligt gebruikersreferenties in een speciale beveiligingschip, zodat ze verborgen blijven voor malware die referenties zoekt en steelt.[1]

Houd informatie privé met Dell SafeScreen en Dell SafeShutter.

Zorg ervoor dat gebruikers vanaf elke locatie kunnen werken terwijl privédata veilig blijven.

Meer informatie op: Delltechnologies.com/endpointsecurity of neem vandaag nog contact op met uw aangewezen Dell specialist voor eindpuntbeveiligingen via endpointsecurity@dell.com.

[1] Gebaseerd op interne analyse van Dell, januari 2020.

Gepubliceerd in de VS 21/10 Oplossingsoverzicht