TD SYNNEX | HPE

AI-native beveiliging voor moderne netwerken

Moderne netwerken zijn kwetsbaarder dan ooit. Gebruikers, apparaten en toepassingen zijn nu overal en bedreigingen blijven evolueren. Beveilig jouw netwerk van edge naar cloud met intelligente, ingebouwde beveiliging die gelijke tred houdt met de huidige bedreigingen.

HPE Aruba Networking brengt beveiliging in het netwerk zelf en combineert AI-gestuurd inzicht met een Zero Trust-aanpak om toegang, gegevens en toepassingen te beschermen zonder de complexiteit toe te voegen.

Top 5 beveiligingsuitdagingen: en hoe je ze oplost

Uitbreiding van het aanvalsoppervlak

Gebruikers op afstand, IoT-apparaten en cloudapps verhogen het risico

- Controle van de toegang met op identiteit gebaseerde beleidsregels
- Zero Trust toepassen op alle gebruikers en apparaten

Onveilige toegang op afstand

Traditionele VPN's hebben moeite om bij te blijven

- Vervang oude toegang door Zero Trust Network Access
- Beveilig verbindingen zonder het netwerk bloot te leggen

Gegevensverlies in SaaS en cloud

Gevoelige informatie gaat verder dan de perimeter

- Bescherm gegevens in SaaS-omgevingen
- Bewaak en controleer het gebruik in alle toepassingen

Gelimiteerde zichtbaarheid en trage reactie

Bedreigingen blijven onopgemerkt tot het te laat is

- Realtime inzicht in het hele netwerk en de gebruikers
- Gebruik AI om problemen sneller te identificeren en op te lossen

Toenemende complexiteit van beveiligingstools

Meerdere oplossingen creëren silo's en hiaten

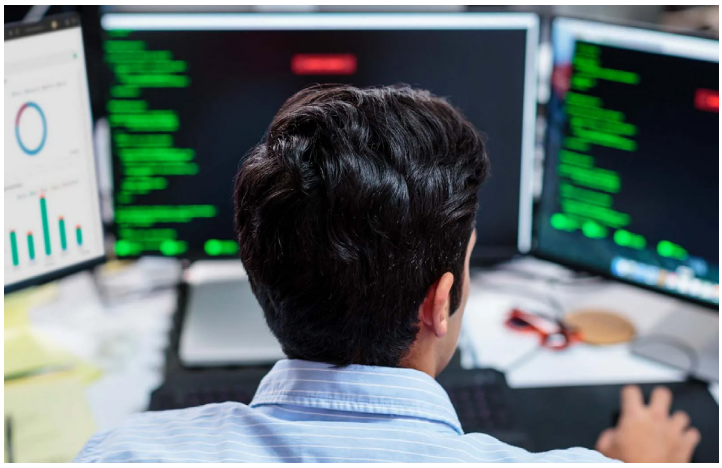
- Consolideer beveiliging in één uniform kader
- Beheer beleid en handhaving vanaf één platform

TD SYNNEX | HPE

HPE Aruba Networking Security-aanpak

HPE Aruba Networking levert een uniforme beveiligingsarchitectuur die on-premise bescherming combineert met cloud-native mogelijkheden.

Van toegangscontrole tot SASE en SSE, beveiliging wordt consistent toegepast in het hele netwerk, zodat gebruikers en toepassingen overal veilig kunnen verbinden.



Kernbeveiligingsoplossingen

Security Service Edge (SSE)

Cloud-gebaseerde bescherming voor gebruikers, apparaten en toepassingen, waar ze zich ook bevinden.

- Zero Trust Network Access (ZTNA) beveiligt de toegang tot applicaties
- Secure Web Gateway (SWG) inspecteert en beschermt webverkeer
- Cloud Access Security Broker (CASB) beschermt het gebruik van SaaS

Beleidshandhaving op de edge

Pas op rollen gebaseerde, identiteitsgestuurde beleidsregels direct binnen het netwerk toe, waardoor consistente bescherming wordt gegarandeerd voor alle verbindingen.

AI-gestuurde beveiliging en beheer

HPE Aruba Networking Central

Een cloud-native platform dat zichtbaarheid, controle en intelligentie samenbrengt. Het platform maakt gebruik van AI en bedreigingsinformatie om activiteiten te monitoren, beleid af te dwingen en risico's te detecteren zonder handmatige workloads toe te voegen.

SASE architectuur

Netwerk en beveiliging worden gecombineerd in één enkel framework, wat de implementatie vereenvoudigt en tegelijkertijd de bescherming in gedistribueerde omgevingen versterkt.

TD SYNNEX | HPE

Bedreigingsdetectie en reactie

Veiligheid stopt niet bij preventie.

Netwerkdetectie en reactie identificeert ongebruikelijk gedrag en potentiële bedreigingen

Contextbewust beleid past zich aan op basis van identiteit, apparaat en activiteit

Geautomatiseerde reacties verminderen de impact en versnellen de herstelwerkzaamheden

Waarom dit belangrijk is

Beveiliging moet in het netwerk worden ingebouwd, niet achteraf worden opgebouwd. Met HPE Aruba Networking kun je gebruikers, gegevens en toepassingen beschermen en tegelijkertijd activiteiten vereenvoudigen om zichtbaarheid te verbeteren en modern werken te ondersteunen.

Beveilig jouw netwerk van edge naar cloud

Ontdek hoe HPE Aruba Networking je helpt beschermd te blijven terwijl jouw business in beweging blijft.

Ontdek meer