# Moderne datacenters vragen om een nieuwe beveiligingsaanpak

→ Virtualisatie, cloud en door software gedefinieerde netwerken herdefiniëren het datacenter

→ Werklasten, toepassingen en gegevens zijn nu overal, verspreid over multicloudomgevingen

→ Gebruikers verplaatsen zich buiten de bedrijfsgrenzen en zijn in toenemende mate mobiel, en gebruiken resources vanaf vele apparaten

→ Tegenwoordig is het datacenter ongelooflijk complex en organisaties moeten heroverwegen hoe ze beveiliging aanpakken

Beveiligingsteams besteden **76%** van hun tijd aan het beveiligen van het datacenter, verdeeld als volgt:*

**47%** Servers

**20%** Klantgegevens

**24%** Endpoints

**57%** is het erover eens dat gegevens in de openbare cloud het moeilijkst te verdedigen zijn**

Slechts **38%** heeft zijn datacenter gesegmenteerd*

Beveiligingsfunctionarissen erkennen algemeen dat beveiliging een probleem heeft met menselijk kapitaal:***

Wereldwijd zegt **25%** van de beslutvormers op het gebied van beveiliging dat personeelstekorten een grote uitdaging zijn en dat ze moeite hebben met het vinden van personeel met de juiste vaardigheden. Dit personeelsprobleem wordt versterkt als er te veel niet-geïntegreerde point-producten te beheren zijn.

Hoe worden gegevens gestolen? Via mensen****

**81%** van inbreuken door hacking was mogelijk door gestolen en/of zwakke wachtwoorden

**86%** van kwaadaardige payloads komt binnen **73%** via e-mail en **13%** via internet

Gegevensbronnen:
* Jaarlijks Cisco Cybersecurity Report 2017
** Jaarlijks Cisco Cybersecurity Report 2018
*** Forrester: 'The Zero Trust eXtended (ZTX) Ecosystem' door Chase Cunningham
**** Verizon: '2017 Data Breach Investigation', Executive Summary en Full Report

## Het moderne datacenter heeft drie belangrijke beveiligingsbehoeften

### Zichtbaarheid

Zie alles, met volledige zichtbaarheid van gebruikers, apparaten, netwerken, toepassingen, werklasten en processen

### Segmentering

Voorkom dat aanvallers zich lateraal (oost-west) over het netwerk verplaatsen dankzij microsegmentering en whitelisting van toepassingen

### Bescherming tegen bedreigingen

Identificeer inbreuken sneller met meerlaagse bedreigingssensoren om snel te detecteren, blokkeren en reageren om diefstal van gegevens en operationele disruptie te voorkomen

## Het is tijd voor een nieuwe benadering van de beveiliging van uw gegevens, toepassingen en dynamische werklasten

Een benadering met innovatieve nieuwe technologieën en een geïntegreerde architectuur die is gebouwd voor het moderne datacenter. U krijgt:

Context of verkeer **kwaadaardig** is of niet terwijl toepassingen en microtoepassingen zich door het datacenter verplaatsen

Dynamische, flexibele maatregelen voor de consolidatie en automatisering van het netwerk, beveiliging en beleidsregels voor toepassingen

Meerlaagse bedreigingsdetectie en beperking stellen u in staat meer bedreigingen te blokkeren en snel bedreigingen die inbreuk maken op uw datacenter te beperken

## Cisco helpt u gegevens, toepassingen en werklasten te beschermen zodat u beter beveiligd bent en uw bedrijf productiever wordt.

Snellere detectie van incidenten door volledige zichtbaarheid van alle gebruikers en al het netwerkverkeer binnen uw onderneming, cloud en datacenter

Vermindering van het aanvalsgebied door te verhinderen dat ongeautoriseerde gebruikers en geavanceerde bedreigingen **lateraal door uw datacenter bewegen**

Snel identificeren en blokkeren van en reageren op gegevensinbreuken en disruptie van operationele activiteiten

Cisco heeft innovatieve nieuwe technologieën ontwikkeld die samenwerken om het moderne datacenter te beveiligen.

Meer informatie



C05-740358-00 04/18