

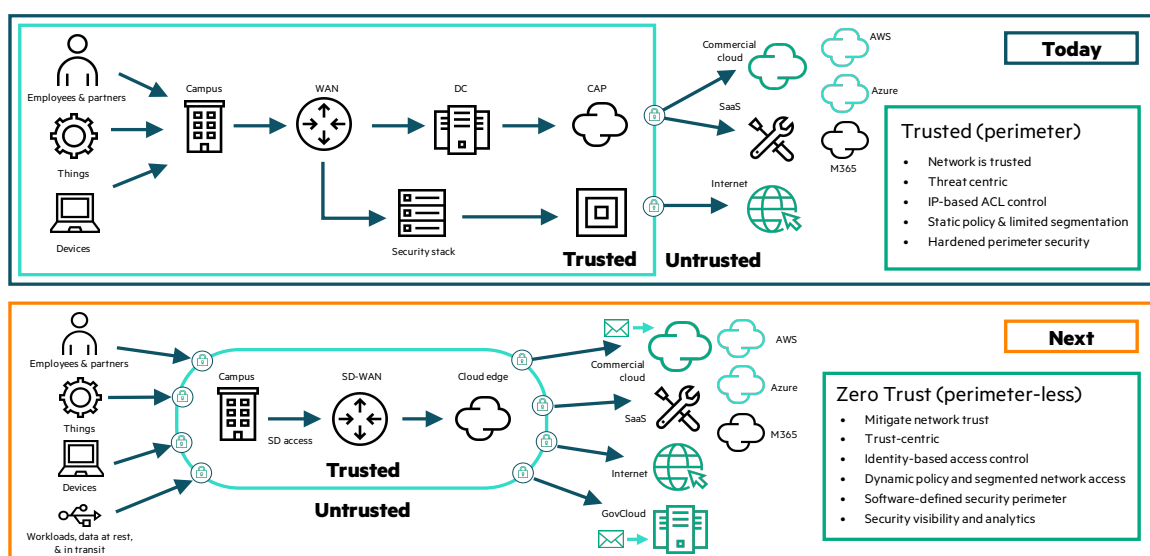
# Zero trust security

A new approach to security architecture

## “Zero trust is not about implementing one or another security or networking technology. It’s a completely new approach to the way you do security architecture.”

– Simon Leech, Senior Advisor for the Worldwide Security and Risk Management Practice, HPE Pointnext Services, HPE

Zero trust security is a philosophical approach to protecting your data and focuses on identity and access management. Compared to perimeter security approaches, zero trust assumes everything is compromised, applying the principle of least privilege to pieces of your architecture that were once considered safe. For example, employees and partners, end devices, and software-as-a-service (SaaS) products must authenticate themselves every time they try to access your systems.



**Figure 1.** See the difference between a “trusted” model vs. a zero trust model where virtually all devices are untrusted.

As new mobile apps, artificial intelligence (AI), and machine learning (ML) drive innovation in nearly every industry, more robust security practices must adapt to keep up. In fact, digital transformation can create vulnerabilities from the core to the edge, as cloud services and microservices architectures work in tandem with legacy systems, and Internet of Things (IoT) devices collect and send high-value data from insecure locations at the edge. Organizations must pay more attention to which systems and people can access different data streams.

With zero trust, all users, devices, and application instances must prove who they are and that they are authorized to access each resource. An efficient and properly run zero trust architecture continuously assesses and authorizes access on a case-by-case basis.





## Our zero trust approach

The complexity of today's cyberattacks, expansive attack vectors, and constant threats can often paralyze even the nimblest enterprises. Zero trust helps simplify your approach to security, to make managing your environment easier.

Essentially, the zero trust security model replaces faith in the integrity of secure network perimeters (such as private networks, firewalls, and VPN/VPC) with that of the individual software systems which are managing critical data.


Hewlett Packard Enterprise has recognized that, for customers and partners to be able to deliver a robust and agile zero trust security solution for their most critical data systems, trust must be built into everything they use—from the silicon that runs the software to the software itself.

## Learn more at

[greenlake.hpe.com/security](https://greenlake.hpe.com/security)

Explore **HPE GreenLake** 

**Make the right purchase decision.  
Contact our presales specialists.**

 **Chat now (sales)**

 **Call now**



**Get updates**

© Copyright 2022 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Azure is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a50006571ENW

**HPE**   
**GreenLake**