Hewlett Packard Enterprise

Industry overview

HPE APPROACH TO ZERO TRUST SECURITY

Check if the document is available in the language of your choice.

"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.

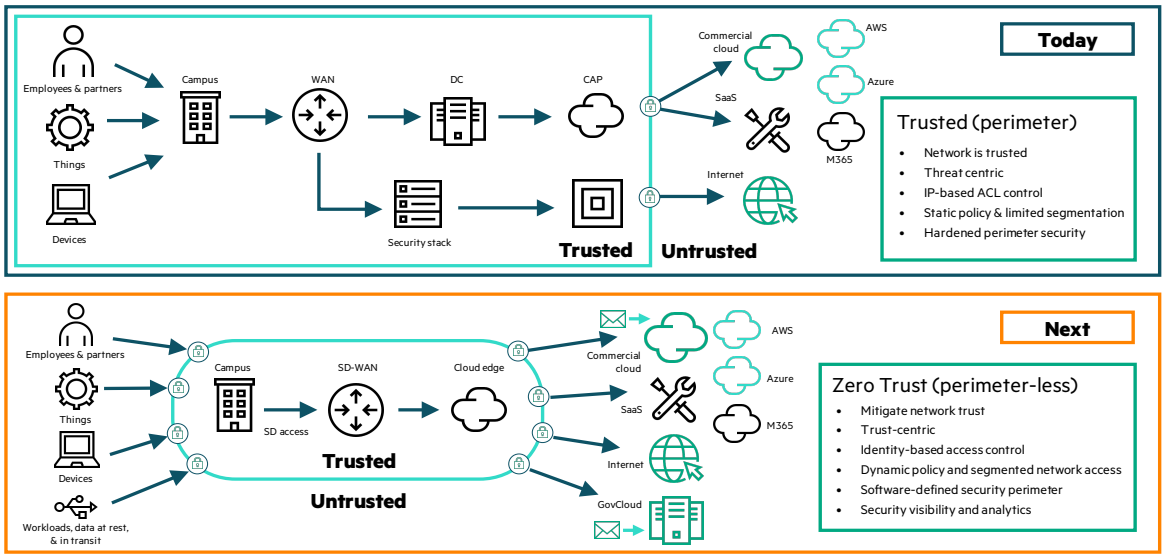

FIGURE 1. See the difference between a "trusted" model vs. a Zero Trust model where virtually all devices are untrusted.

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. This is reflected in a number of deep investments HPE is making in hardware supply chain security (compute), software supply chain security (including SPIFFE [Secure Production Identity Framework For Everyone] and SPIRE [SPIFFE Runtime Environment]), and networking. The culmination of our commitment is our investment in Project Aurora, which aligns and encapsulates much of what is mentioned previously.

ZERO TRUST IN COMPUTE

The compute layer of security is critical to enable Zero Trust architecture across every other layer of your data ecosystem. There are four elements of our Zero Trust compute strategy that work together to fortify your environment.

- Platform certificates detect any tampering and verify that your system is completely unmodified between manufacturing and delivery.
- IDevID is a cryptographic identity that provides secure, zero-touch onboarding without human intervention, enabling automatic provisioning and access management for integrated applications.
- HPE iLO simplifies server setup, health monitoring, power and thermal optimization, and remote server administration, offering administrators a reliable way to integrate HPE servers into existing security environments.
- A trusted supply chain brings together security, processes, and people to deliver protection for your most sensitive applications and data even before your server is built. Only HPE Trusted Supply Chain provides a new first line of defense against cyberattackers with select servers built to the world's toughest security standards in secured facilities.

Sample Zero Trust use case in compute

As the edge expands, so does the attack surface. Perhaps, nowhere is this expansion taking place as rapidly as in the telco industry, where the promise of a vast 5G infrastructure is getting closer every day. 5G has driven companies to integrate and merge their networks, cloud, and communications architecture, connecting everything from mobile base stations, points of presence (POP), and central offices to deliver a virtualized infrastructure that supports new services and applications.

To secure their expanding attack surface, telco companies are adopting a zero-trust edge (ZTE) framework. At the edge, this philosophy requires sophisticated technology to implement without slowing down critical processes and workloads. Here's what a possible universal customer premises equipment (uCPE) for virtualized radio access network (vRAN) reference architecture might look like for a telco customer:

TABLE 1. uCPE for vRAN for small in-building cells

HPE Part #	Description
P39478-B21	HPE DL110 Gen10 Plus Front Telco Cbl CTO Server
P42104-B21	HPE Server Platform Certificate FIO Setting
BD505A	HPE iLO Advanced 1-svr License 3-year Support
P44975-B21	HPE ProLiant DL110 Gen10 Plus 700W Flex Slot Platinum Hot Plug Low Halogen AC Power Supply Kit
P36922-B21	Intel® Xeon® Silver 4314 2.4GHz 16-core 135W Processor for HPE
P06031-B21	HPE 16GB 2Rx8 PC4-3200AA-R Smart Kit
P19888-B21	HPE 240GB SATA 6G Read Intensive M.2 2280 3yr Wty SSD
647594-B21	HPE Ethernet 1Gb 4-Port 331T Adapter

- **For deployment of a single unit in a hostile and untrusted environment (customer premises).**
- **Disks are small because less storage is needed.**
- **For virtualized distributed unit (vDU), you would have 10/25 Gig NICs capable of high-precision timing sync and 128 GB of RAM.**

ZERO TRUST IN SOFTWARE

HPE adds security to the software level through innovative technologies such as SPIFFE and SPIRE.

SPIFFE defines a set of specifications that, among other things, enables an application programming interface (API) to easily establish trust among workloads and system actions. Because it's API-based, unlike manual key generation and distribution processes, SPIFFE attestation and authentication can be fully automated.

"SPIFFE puts in place the underpinnings for enterprises to utilize existing on-premises service authentication protocols (such as Kerberos and OAuth) with workloads running upon increasingly dynamic computing platforms, including cloud and containers."

– Sunil James, Senior Director, HPE (former Scytale CEO)

SPIRE is the first software implementation of SPIFFE. SPIRE's components can be integrated with call providers, middleware layers, and hardware trust mechanisms such as Trusted Platform Modules and hardware security modules. SPIRE is used by workloads across any environment, including Azure, Kubernetes, or an application running in the data center. Ultimately, it creates a finer level of authentication, assessing specific actions that are requested by each user or workload.

ZERO TRUST IN STORAGE

Enterprises are spreading their data from the edge to the cloud and must protect it, wherever the data was generated and wherever it may go. HPE secures the data lifecycle with encryption of data in transit, in memory, and at rest. At the storage layer, HPE follows the Zero Trust model by encrypting data, providing analytics about your data, and even providing an as-a-service storage solution through HPE GreenLake.

Encryption
Encryption happens at nearly every layer of a Zero Trust architecture. Memory encryption powered by Intel® and AMD protects data in use. Silicon root of trust includes state-of-the-art encryption at the firmware. And Trusted Platform Module enables Microsoft BitLocker to drive encryption and create a tamper-resistant environment.

Self-encrypting drives
HPE HDDs and SDDs provide hardware-based data encryption. Compared to software-based encryption, these self-encrypting drives (SEDs) have a performance advantage because they require less processing work for encryption. SEDs also allow devices to be securely erased in seconds.

HPE InfoSight network analytics
Leveraging AI, ML, and predictive analytics, HPE InfoSight coordinates with HPE Active Health System and HPE iLO to help optimize performance and prevent problems. The solution even reacts to behaviors of your install base, helping you improve performance.

HPE GreenLake for storage
HPE GreenLake helps companies with an as-a-service managed security and compliance solution to protect their business at the storage layer. We use trusted processes, tools, and expertise to identify and remediate threats across on-premises and public cloud. You get the performance, scalability, agility, and efficiency your business needs in days, along with a set of workload-optimized, consumption-based solutions built on an Intelligent Data Platform and delivered to you entirely as a service.

ZERO TRUST IN NETWORKING

Although application-level controls have been a focal point within Zero Trust, a comprehensive strategy must also encompass network security and the growing number of connected devices, including the work from home environment. At the network level, HPE provides a comprehensive solution for microsegmentation, granular telemetry between virtual machines (VMs), and such that works in a greenfield or a brownfield.

Distributed Services Cards (DSCs) encrypt data in motion to reinforce Zero Trust in the network. Powered by Pensando, our DSCs allow you to encrypt any to any, meaning nobody can eavesdrop or see what you're doing over the network.

Distributed Services Architecture allows you to isolate every entity on its segment to protect it from everybody else. In other words, you need explicit permission for the server to contact another server. Adding a DSC into your server changes the architecture from a centralized firewall to a distributed architecture that spreads all the way to the edge. In this new model, all decisions are made locally, allowing you to gain visibility into VM-to-VM traffic even when it bypasses the centralized firewall. Ultimately, Distributed Services Architecture improves application response time by breaking through the bottleneck of the firewall.

Aruba
Our new distributed services technology improves latency network utilization, reduces cost, and shrinks your TCO. In Aruba, the five tenants of Zero Trust protection are:

- **Visibility:** Device discovery and profiling, customer fingerprinting
- **Authentication:** One role, one network AAA (Authentication, Authorization, and Accounting) and Non-AAA options
- **Role-based access control:** Context-based access and dynamic segmentation
- **Uninterrupted monitoring**: Real-time threat telemetry from Aruba solutions and more than 150 integrations
- **Enforcement and response:** Attack response and event-triggered actions

Aruba ClearPass Policy Manager allows you to centrally create role-based policies that enable teams to monitor and enforce how devices behave throughout a session, regardless of location or time of day.

Aruba Policy Enforcement Firewall (PEF), Intrusion Protection System, 360 Security Exchange lets you set rules on wireless and wired networks that seamlessly work with our infrastructure and Aruba ClearPass Policy Manager to keep Zero Trust principles in check at the session and traffic level.

Aruba ClearPass Device Insight uses a combination of active and passive discovery and profiling techniques to detect the full spectrum of devices connected or attempting to connect to the network. This includes common user-based devices such as laptops and tablets. Where it differs from traditional tools is its ability to see the increasingly diverse set of IoT devices that have become increasingly pervasive on today's networks.

Aruba Edge Services Platform (ESP) increases protection levels while simplifying operations by applying the principles of edge-to-cloud security, featuring a built-in foundation for Zero Trust and Secure Access Service Edge (SASE) frameworks.

PROJECT AURORA

With Project Aurora, HPE is delivering building blocks to enable a cloud-native Zero Trust architecture from edge to cloud. This innovative technology allows hardware and software to be remotely verifiable and therefore trustworthy.

Leveraging the silicon root of trust from HPE, Project Aurora continuously verifies and asserts a chain of trust from a workload to the HPE hardware it runs on, allowing you to scalably monitor everything, including customer workloads, without signatures. Through continual attestation, which allows a program to authenticate itself, even servers at the edge can prove their integrity and trust worthiness.

Project Aurora will eventually be embedded across HPE GreenLake cloud services and HPE Ezmeral software platforms.

LEARN MORE AT

hpe.com/security/compute

Hewlett Packard Enterprise

a50005219ENW