HPE

Tech article

BRINGING ZERO TRUST TO IOT

Whether they're used for run-of-the-mill office tasks like printing, or advanced activities like fingerprint access control, IoT devices are becoming a staple in every organization's digital environment. Even outside of traditional office settings, IoT has also proven useful. For instance, in the industrial space, IoT-powered sensors are used to monitor temperatures, resources, and even safety.

But while this technology has helped to powerfully transform organizations and their operations, IoT has also become an increasing cybersecurity concern for IT teams. Because they're often unmanaged, IoT devices aren't always on IT's radar, essentially left operating "invisibly" outside of security controls. Only 16%[1] of surveyed IT practitioners can say, with complete confidence, that they know all the users and devices connected to their network all the time. Another concern is that many IoT devices don't support the software agents required by standard security solutions, so can't be monitored — and different firmware and protocols across different types of IoT can make consistent identification and policy enforcement tricky.

The bottom line is that every time one of these devices connects to the enterprise network, a new vulnerable entry point is created for hackers to exploit. And the sheer volume of connected IoT devices means that an organization's attack surface is expanding at an alarming rate.

The risky nature of these devices goes beyond providing cybercriminals with a doorway into IT infrastructure. IoT devices have also become incredibly effective tools for collecting valuable data about an organization's operations that can then be sold on or exploited directly. A topical concern, given IoT's evolving role in supplying data for a growing number of AI use cases, is that these devices could also provide bad actors with the opportunity to mess with the data itself, i.e., via the data poisoning and corruption of AI models.

With the proliferation of IoT devices showing no sign of slowing, organizations cannot allow these network entry points to remain unsecured. This pressing security issue is one that IT must tackle with a zero trust approach.

Applying zero trust principles to IoT

A universal zero trust network access (universal ZTNA) solution helps organizations activate zero trust principes from edge to cloud, giving users and devices the least amount of access to network resources. Access moves from traditional network-level to application- or resource-level, which gives IT more control. In fact, IT practitioners rank the ability to secure IoT devices and users as one of the top three benefits of universal ZTNA.[2]

[1,2] Ponemon Institute Research Report sponsored by Hewlett Packard Enterprise, The 2025 Global Study on Closing the IT Security Gap, February 2025. Available at: paths.ext.hpe.com/c/a00145793enw?x=tJG359&xs=494974

Key ingredients for applying zero trust to IoT

To effectively apply zero trust to IoT, there are a couple of key requirements you need to meet:

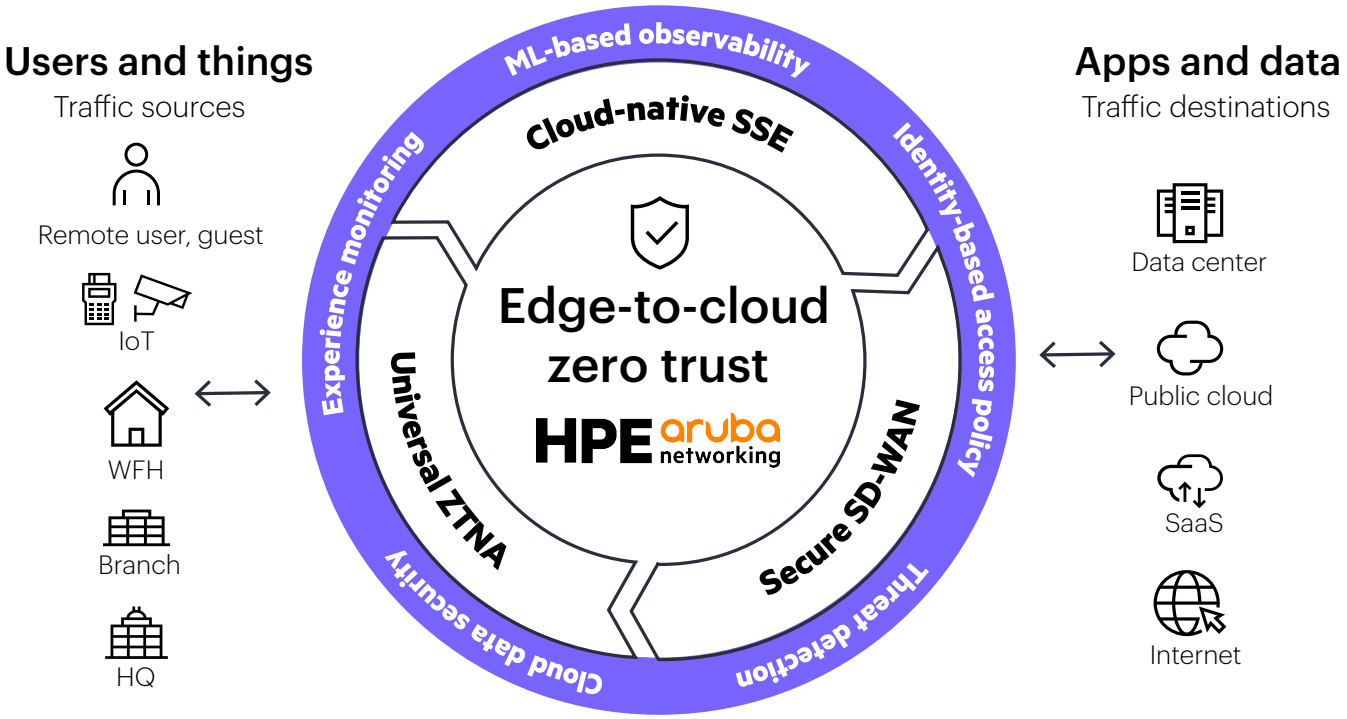
- **Visibility and profiling:** Can you see every device connected to your network, even if you do not manage it?
- **Authentication and authorization:** Do you have a high level of confidence in the identity of devices connected to your network? Do you have consistent methods for assigning access privileges to devices?
- **Enforcement:** Can you apply access control policies consistently throughout your network, regardless of how, where, and to what devices are connected?
- **Continuous monitoring:** Can you monitor the behavior of devices connected to your network? Do you have a means of determining whether behavior is typical, consistent, and expected?
- **Response:** Based on available security data, can you take action to adjust trust, address issues, and thwart attacks?

IoT security begins with the right partner

HPE Aruba Networking provides organizations with a comprehensive edge-to-cloud zero trust platform that ensures all of these requirements are satisfied.

With a universal ZTNA framework from HPE, you can enable:

- **AI-powered visibility** to help you quickly identify connecting devices with greater accuracy.
- **AI-powered profiling** to help you understand typical and expected behavior from any type of device, including IoT sensors, cameras, and printers. With behavioral baselines at a per-device level, you are better equipped to spot anomalies that can indicate compromise or attack.
- **Cloud-based network access control** that makes it easier to define and apply appropriate security controls for every device connecting to your network.
- **Role-based access, consistently enforced**, via a global policy engine that you can apply to both on-premises and remote devices.
- **Continuous trust adjustments in real time**, adapting to risk thresholds and access control policies you've defined.



Components of the edge-to-cloud zero trust platform:

HPE Aruba Networking Security Service Edge (SSE) provides seamless and secure access for users, devices, and applications from anywhere, offering ZTNA, SWG, CASB, and DEM functionalities in a cloud-native solution. With private edge, the solution ensures that on-premises ZTNA traffic remains local, while eliminating the need for inefficient hairpin routing to the cloud.

HPE Aruba Networking EdgeConnect SD-WAN enhances network performance and security by unifying SD-WAN, firewall, routing, and WAN optimization, ensuring high-quality application performance and secure connectivity.

Universal ZTNA with HPE Aruba Networking Central extends zero trust security into branch and campus locations. Additionally, leveraging advanced network access control capabilities, the solution offers deep network observability through machine learning. It can accurately and precisely profile devices, including IoT, and globally enforce access policy and microsegment the network based on role and identity.

IoT innovation without fear

The future of secure enterprise networking won't involve fewer connected devices — but smarter, more adaptive security frameworks that can accommodate the inevitable expansion of IoT.

The shift toward universal ZTNA represents a critical evolution in cybersecurity strategy — one that acknowledges the unique vulnerabilities of unmanaged IoT devices while providing practical solutions to address them. By extending zero trust principles to every device on the network, organizations can maintain robust security without sacrificing the operational benefits that IoT brings.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties 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.

a00148146ENW

HEWLETT PACKARD ENTERPRISE

hpe.com