HPE GreenLake

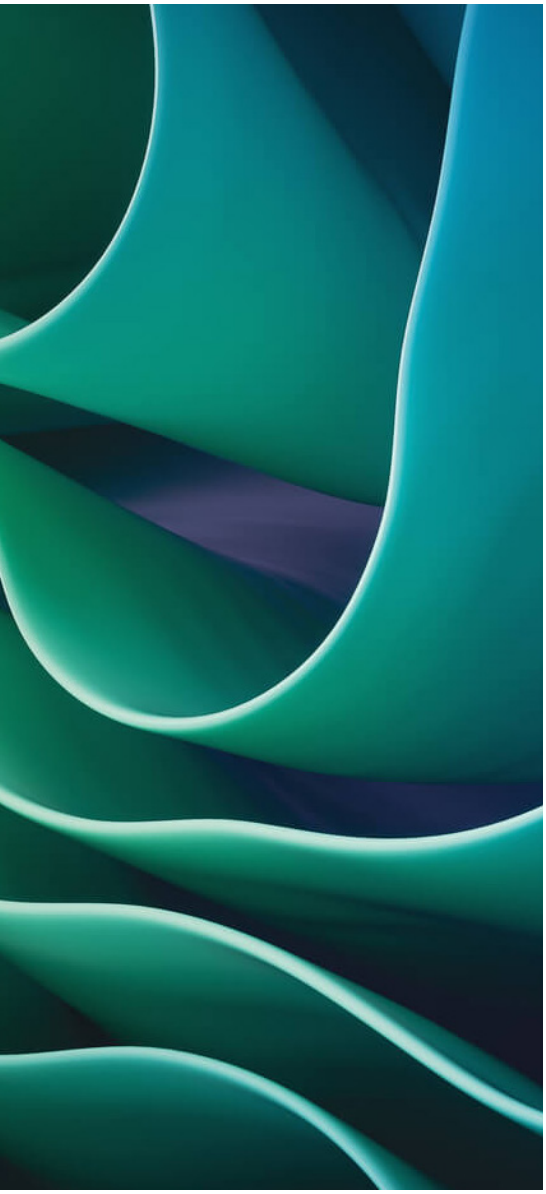
Increase cyber-protection with HPE Networking

Enable new experiences while protecting your organization

New business models focusing on innovative user experiences rely on a highly distributed network—with users, devices, and applications increasingly connecting from edge to cloud. Amid this environment, IT is challenged to predict and prepare for what lies ahead in the ever-evolving threat landscape while often struggling to deal with gaps in existing security capabilities.

If yours is like many organizations, you don't have infinite security resources. Yet because it's so critical to your business, your network must play a critical role in cyber-protection.

Is there a way in which your network infrastructure can increase cyber-protection and work in conjunction with the rest of your security ecosystem?



Keep your organization secure with identity-based access control

Organizations often employ a zero trust approach that relies on the identity of users and devices to secure enterprise data, applications, and infrastructure. Traditionally, zero trust has been implemented by network access control solutions that use the corporate network for policy enforcement. As more access occurs via the cloud, many also use secure access service edge (SASE) for hybrid cloud protection. Zero trust provides the overall security framework. Network access control and SASE are complementary frameworks within a comprehensive security strategy.

Identity-based access control is a core element of zero trust, and the network is key to implementing it. Whether a user or device is connecting to your corporate network or to the cloud, you need to:

- Discover and profile all users and devices on the network
- Validate identity
- Develop and assign access control policies
- Enforce access via the corporate network or cloud services
- Adjust access permissions profiles when threats appear

Incorporating these access control elements into zero trust solutions is an integral part of HPE's approach to modern security. In this way, we enable the control of access to IT resources from edge to cloud, no matter how a user or device connects. This firmly establishes the network and its related security services as an essential partner in a robust cyberdefense architecture.

Get started with Aruba ClearPass Policy Manager and SASE solutions

Aruba ClearPass Policy Manager simplifies identity-based access control for your corporate network. You can set up different levels of secure access for visitors, partners, customers, and employees. Access is holistically enforced when connecting to Wi-Fi, wired, and WAN networks. ClearPass includes built-in features such as preconfigured guest portals and device configuration monitoring.

As you move workloads outside the corporate network and to the cloud, SASE solutions from HPE Aruba Networking provide cloud-based security services that help ensure that the same access policies are consistently enforced across both corporate and public networks.

Use case: Increasing cyber-protection in an academic environment

To help ensure security, a university wanted to separate entertainment and academic traffic in dormitory environments. This would prioritize coursework and research over bandwidth needs from, say, a student's Xbox. Aruba ClearPass Policy Manager was used to segment students' academic and entertainment traffic. It works like this: Students easily connect their devices to the network via a self-service portal, with each device identified and assigned the appropriate access policies. The network automatically enforces these policies, helping ensure that the gaming system cannot access university resources while still providing internet access required to play online games. This is definitely a cybersecurity and user experience win.

Learn more at

HPE.com/ca/en/Aruba-ClearPass-Policy-Manager.html

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise

a50008659ENW