

Design Your Network for the Way Tomorrow Moves

Your business must adapt to change. Ensure that your network is agile and confidently secure.

Today's hyper-mobile workforce wants to connect to the enterprise network at will via a variety of devices and get their work done from wherever they happen to be. While the good news is that this level of mobility boosts employee productivity and satisfaction, the flip side is that network access via mobile devices—and the devices themselves—if not managed properly can compromise the security of your enterprise network and your data.

While enterprise IT departments are adept at securing and managing computing endpoints such as desktops and laptops, the complexities presented by myriad mobile devices call for concerted attention. Consider these factors to ensure your network, and the devices that connect to it, are keeping your employees productive and your assets safe.

Challenging Your Network

The so-called tsunamis of change have hit IT. The bring-your-own-device trend, a growing mobile work-

force, cloud-based services and IoT devices all present complex challenges when it comes to enabling secure access to the enterprise network. These challenges cause many in IT to rethink just how to design and manage their enterprise networks. Key challenges to consider include:

Security and Access Control: Employees connect to the enterprise network from outside the company's four walls and over hot spots and networks that IT cannot control. IT needs a plan to deal with infected mobile devices connecting to the network.

User ID: The identity of a user is no longer an Ethernet port number. The new mobile context—role of the user in an organization, the type of mobile device he or she is using, the types of apps running on that device and where the device is located—are all useful context points to define policies before allowing network access.

Network Users: Your network has to be designed with the needs of your users in mind. An executive in a Fortune 1000 company will have different requirements than an administrator in a school district or a technician in a healthcare facility. IT must understand its users, how they will connect and which work-related apps they use.



Growing Demand for Access: Organizations must be equipped to address the growing number of devices accessing their networks. As a result, IT's ability to effectively and securely on-board large numbers of devices to the enterprise network is becoming a greater priority.¹

Quality and Security at the Access Level Matters

Just as the days of one wired device per person are long gone, so are the days where AAA (authentication, authorization and accounting) rules are sufficient for network access control. Network access control today is more complex and organizations have to deal with how best to enforce behavioral policies related to mobility, the use of personally owned devices and multiple types of devices per person—all through the prism of security.

Software-defined networking and policy management—software programmability—are key to enforcing secure mobility. Using software programmability that extends across the network allows businesses to adapt in real time to the demands of the mobile generation workforce. A software-defined network understands contextual information such as where the user is, what applications he or she is using, and which devices are connecting. It can also assign and enforce policies based on a complete view of the endpoint (in the case of IoT) or the user.

Aruba ClearPass Policy Manager™ from Hewlett Packard Enterprise is the most advanced policy management platform available and was ranked by Gartner as a leader in the Wired/WLAN access Magic Quadrant. Aruba ClearPass Policy Manager is the only network access control solution that centrally enforces all aspects of enterprise mobility from a single platform. Granular network access privileges are granted based on a user's role, device type, MDM attributes, device health, location and time of day.

Aruba ClearPass provides:

- ✓ Role-based network access enforcement for multivendor Wi-Fi, wired and VPN networks
- ✓ Industry-leading performance, scalability, high availability and load balancing
- ✓ Web-based interface that simplifies policy configuration and troubleshooting
- ✓ Support for NAC, Microsoft NAP posture and health checks, and MDM integration for mobile device posture checks
- ✓ Auto sign-on and single sign-on (SSO) support via SAML v2.0
- ✓ Advanced reporting of all user authentications and failures
- ✓ HTTP/ReSTful APIs for integration with third-party systems such as SIEM, Internet security and MDM
- ✓ Device profiling and self-service on-boarding
- ✓ Guest access with extensive branding and customization and sponsor-based approvals
- ✓ IPv6 administration support

Experience and Expertise Make a Difference

Businesses that are designed for how tomorrow moves are able to adapt. That means their networks must also dynamically adapt to the needs of their users by leveraging the capabilities of software programmability. As a Hewlett Packard Enterprise Platinum Partner, [ConRes](#) understands how mobile devices work with enterprise environments. We can help your organization build and maintain a secure, adaptable enterprise network. We start by assessing your existing network posture, understanding the unique needs of your business and users, and leveraging our extensive expertise and decades of experience in networking, mobility and BYOD security.



Partner with ConRes to benefit from our wealth of resources:

- ✓ 70 engineers with advanced certifications
- ✓ Master ASEs in all HPE categories
- ✓ HPE OEM global partner and integrator
- ✓ 45,000-square-foot integration facility
- ✓ Staging, configuration, implementation and burn-in services
- ✓ Client infrastructure 24/7 monitoring service
- ✓ ISO 9001:2008 certified
- ✓ Certified women-owned enterprise
- ✓ Offices worldwide

Request a consultation with ConRes today.

Call us at 800-937-4688 or visit www.conres.com to see how we can help you optimize your mobile enterprise network for tomorrow.



Continental Resources, Inc. | 800.937.4688 | www.ConRes.com

Corporate Headquarters, 175 Middlesex Turnpike, Suite 1, Bedford, MA 01730-9137. Offices Worldwide

Source: ¹Critical Capabilities for Wired and Wireless LAN Access Infrastructure, Gartner, September 2015

Hewlett Packard Enterprise specializations include Platinum: Converged Infrastructure; Silver: ArcSight

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.

©2008-2016 Continental Resources