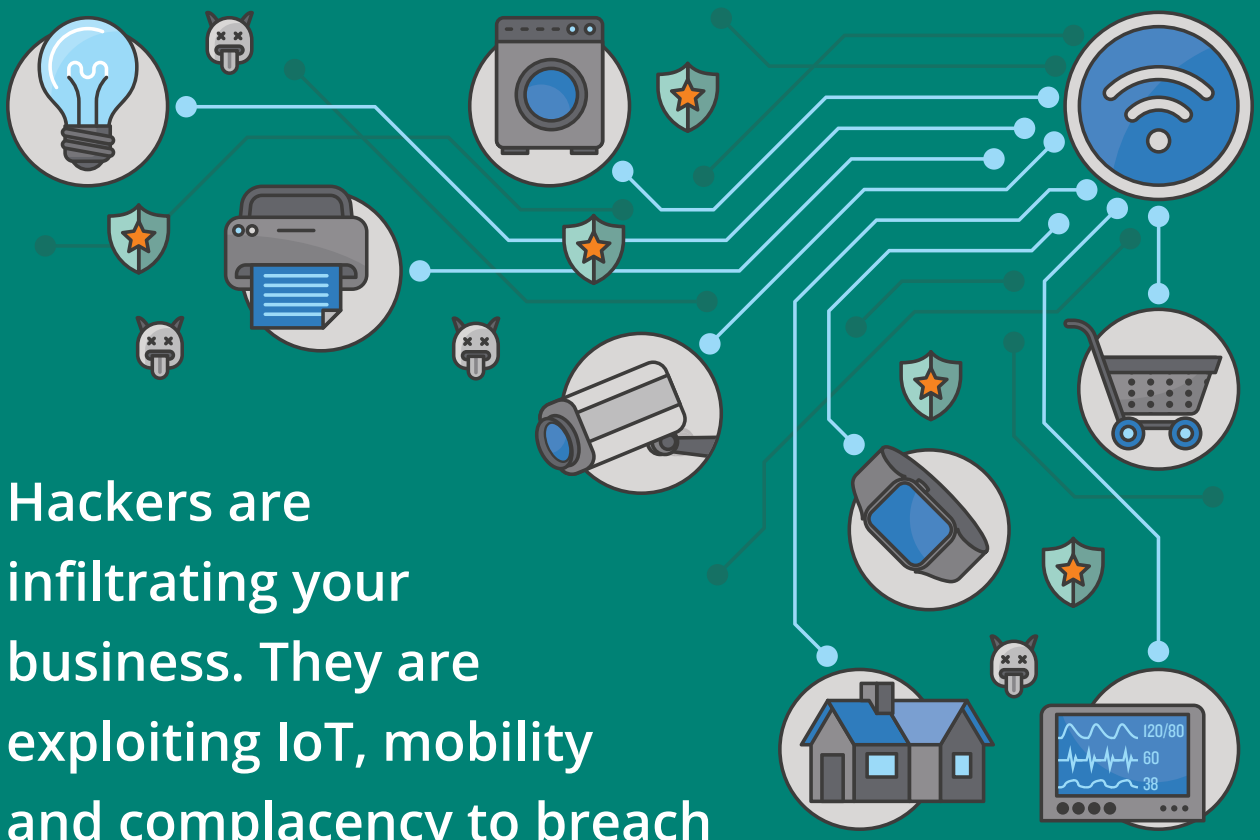


Hackers are infiltrating your business. They are exploiting IoT, mobility and complacency to breach your enterprise.

Aruba ClearPass brings visibility, control and security response to the anywhere, anytime, any-device enterprise

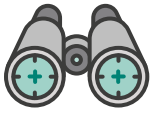
aruba

a Hewlett Packard Enterprise company

According to the **2016 Ponemon Cost of Data Breach study**, malicious insiders continue to represent the most prevalent, costly and effective attack vector, while 76% of businesses remain unprotected from these insider threats.[1] At the same time, the exponential growth of IoT, corporate and BYOD devices has further reduced visibility, yet security resources have not been increased accordingly.

Businesses today embrace the idea of anywhere, anytime connectivity, but have largely ignored the need for secure network access control (NAC). Many employ a *laid-back NAC* "connect now, secure later" philosophy. Others simply choose the same vendor for security that they use for network infrastructure. Both of these approaches give the illusion of security—even compliance—but in reality, leave extensive security gaps.

The need for visibility, control and response



Visibility is a critical issue for under-resourced Operations and Security teams. **Gartner research** shows that each employee uses an average of three mobile devices,[2] and now, internet-connected things must also be considered. Factor in corporate guests, contractors and temporary employees, and the number of wired and wireless devices connecting to the network grows even higher. Without accurate data for all of these connected things, security gaps will appear and be exploited. Visibility is the first step toward closing that gap.



Control of devices is vital for enterprise security. Ensuring that only authorized and/or authenticated devices connect to your wired or wireless network significantly reduces your risk and releases resources.



Response. Your existing security tools—including security information and event management systems (SIEMs), firewalls and antivirus solutions—provide disparate actionable event data. Too many security tools provide too many possible security remedies. When threat data is unified, you can take simple, nuanced actions to suspend or disconnect malicious devices at the network layer and thereby limit loss—without the need for additional processes or resources.







Enforce security across your enterprise

With secure enterprise NAC, you can achieve an assured security posture without additional resources. The right solution empowers your IT team with:

- **Visibility** into all connecting and connected devices, wired and wirelessly
- **Control** of IoT, BYOD and corporate devices, across multiple network vendors
- **Response** with seamless integration of security tools for automated threat detection, escalation and unified policy enforcement

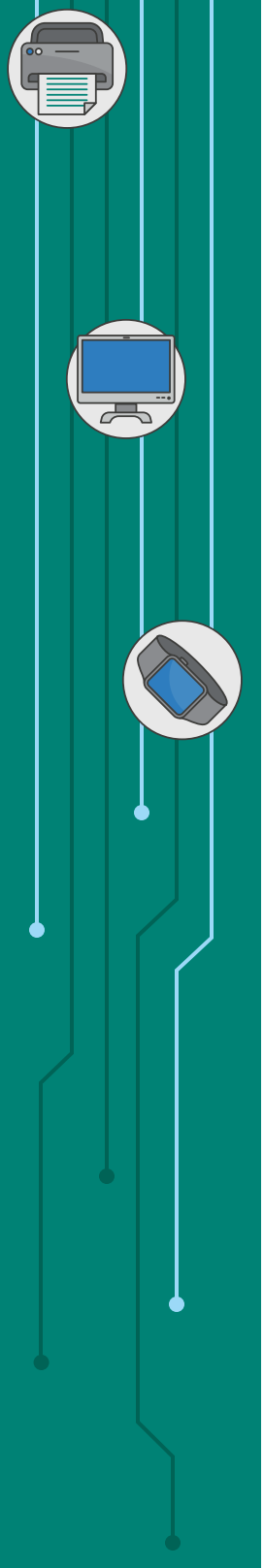
Aruba's NAC solution, ClearPass, provides a single RADIUS-based security and verification point for all your wired and wireless networks, applications, IoT devices, employee, contractor and guest devices. Aruba ClearPass allows organizations to create, define and enforce a consistent access policy of what can connect to which elements of the enterprise, based on the type of device, who is using it, where and when it is being used, the type of connection and its health status.

Only Aruba ClearPass can deliver assured connectivity in a multi-vendor security and infrastructure environment. Today, more than 7,000 enterprise customers worldwide use Aruba ClearPass to ensure a more secure and productive environment.

Why Aruba ClearPass?

Secure all the "things"—corporate, IoT and BYOD—wired and wirelessly

- Identify all devices, secure access and ensure only authenticated, authorized or "healthy" devices can connect—both wired and wirelessly—regardless of network vendor
- Use a trusted solution, deployed in the largest networks, at over 7,000 organizations, in more than 28 different vertical markets
- Ensure your access control can be user and entity behavior analytics (UEBA) ready—secure access, then monitor and secure usage



Enforce wired and wireless policy

- Define what devices can and cannot do, and what infrastructure, applications and data they can access
- Close the gap between encrypted wireless and open-wired ports
- Strengthen BYOD security while simplifying application and device authentication

Streamline network security management

- Unify threat and potential breach response with leading security vendors, all from a single management console
- Re-enforce your perimeter and know and control what connects inside the business
- Automate attack responses and unify threat actions with over 100 third-party security and infrastructure vendors

Improve end-to-end security with Aruba ClearPass

Find out how Aruba ClearPass can enforce security throughout your enterprise.

LEARN MORE

REFERENCES

[1] *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, June 2016.

[2] *Gartner Says Demand for Enterprise Mobile Apps Will Outstrip Available Development Capacity Five to One*, Gartner, 16 June 2015.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM
www.arubanetworks.com

WP_ClearPass_081017