BLUE CONNECTIONS IT

HPE aruba networking

Providing security where the threats are

How to safeguard your dispersed workforce from escalating security threats

Security threats are evolving and expanding constantly. The pandemic has seen cyber criminals exploit the dramatically increased workload on IT and security teams, by launching enterprise-level ransomware, crypto-mining and Denial of Service (DoS) attacks.[1]

For businesses with dispersed workforces, and front-line workers out in the field, the security risks have always been considerable. While employees are generally risk averse, they can unwittingly be one of the greatest security threats to an organisation. In a recent Australian study, 61% of employees admitted they had opened an attachment in an email from an unknown source, and 50% opened a link in an email from an unknown, external contact.[2]

Now, with most Australians working remotely (88% of Australian organisations asked employees to work from home as a result of the COVID-19 pandemic[3]) the cybersecurity risks are greater than ever. In the current climate, exhausted front-line employees, struggling with unprecedented change, simply can't be relied upon to also provide defence against relentless cyber-attacks. The ability for users to connect to a corporate network from anywhere also turns the traditional legacy perimeter security model inside out.

In this eBook, we examine some of the key security challenges for businesses with front-line workers, and outline how a solution based on Aruba's ClearPass technology can help.

> **61%** of Australian workers have opened an attachment in an email from an unknown source, and **50%** have opened a link in an email from an unknown, external contact.[4]

Why does security fail so often?

Different businesses with front-line workers often face the same security challenges. Chief among them:

You can't fix what you can't see

For many modern businesses, network visibility is a major problem. Without granular visibility into who and what's connected to the network, there's no way for IT teams to create policies that meet the needs of specific groups, proactively troubleshoot problems or ensure security compliance.

Connections exploding at the edge

An increasing number of people and things are now connecting at the edge of corporate networks, which is making it very hard for IT teams to maintain control, especially if they are relying on traditional perimeter-based security. IDC predicts that in total there will be 41.6 billion connected IoT devices by 2025.[5]

Consequently, huge amounts of data are now being generated and processed at the edge of the network rather than in traditional, centralised data centre or cloud environments. Gartner predicts that by 2025, this amount of data will grow from 10% to 75%[6] and many traditional networks simply won't be able to easily support this scale and volume of data.

Systems are stuck in the Stone Age

In many instances, the legacy systems of businesses are simply too primitive for secure mobility. IT teams are left using static business rules that can't keep up with the demands of the increasingly mobile generation. Flexible work habits require dynamic policies that are based on contextual data like user roles, device types, ownership, location, and app usage – but many businesses simply don't have this in place.

The rise of shadow IT

In a recent study, 80% of organisations noted that they found IoT devices on their networks that they did not actually install, secure or manage.[7] In a recent Australian survey, 29% of employees admitted to downloading an app or software from a third-party website without their employer's permission.[8]

At the same time, modern IT helpdesks are often overwhelmed by requests from employees and guests to configure and onboard their personal devices for Wi-Fi access. At times, a lack of self-service workflows leaves users standing on the sidelines or taking matters into their own hands.

> **80% of organisations have found IoT devices on their networks that they did not actually install, secure or manage.[9]**

VLANs aren't delivering

The notion of VLANs as a solution breaks down in the face of an increasingly mobile generation that expect to be able to connect to the corporate network from anywhere, and uses work apps on their mobile devices for data, voice and video. In this scenario, IT teams have no choice but to deny services or create complicated enforcement rules. Instead of static VLANs, businesses need to start using role-based policy enforcement.

Employees themselves can be risky

In many instances, employees can be one of the greatest risks to an organisation's security. While 87% of small business owners think antivirus software alone means they're safe from cyberattacks, 33% of employees say they have ignored computer notifications and updates on their computers, meaning they are not protected. 22% also admitted to sharing emails from friends or other contacts, even when the original source was unknown.[10]

Cybercriminals see these stats as opportunities, which is why they are switching up their attack methods to target end users. Right now, when employees are exhausted and overwhelmed by the demands of remote working, expecting them to take responsibility for their device security can become a major risk in itself.

How can an Aruba ClearPass solution help?

Today, businesses need to take a fresh approach to network architecture – with a modern architecture supporting diverse endpoints, connected and combined with context to enable and protect devices and staff.

Aruba's ClearPass Access Management System

Is built on exactly this approach. It delivers secure enterprise mobility by integrating AAA with policy management, guest management, guest access, automated onboarding workflows, device health checks and other self-service capabilities. Plus, it delivers everything from one platform, on any multi-vendor network.

Here's what you can expect from ClearPass:

Enhanced visibility

The ability to dynamically profile devices as they connect provides IT with valuable information that can be used within policies and for troubleshooting. Policies based on real-time contextual data allow security and network teams to allow or restrict access to internal resources based on user, device type and their assumed risk level.

Enterprise-ready contextual policies

Built-in policy services within the ClearPass Policy Manager delivers where legacy AAA solutions fail. Secure enterprise mobility can now be managed from a single platform regardless of access method: wired, wireless or VPN. Contextual data such as location, time of day and device type provide flexible policy enforcement attributes for today's mobility-centric #GenMobile environments.

Self-service workflows

ClearPass leverages user and device attributes to offload routine IT tasks through the use of intuitive self-service workflows. Employees and guests are allowed to self-configure personal devices, manage certificates and request guest access, which reduces IT helpdesk tickets while increasing IT and user productivity.

Enforcement built for mobility

Mobility makes it increasingly unworkable to manage separate VLANs to enforce network privileges for different user groups, work-spaces and traffic types. Mobility requires role-based policies that leverage contextual data to automatically direct users to appropriate resources. This is particularly important as users connect from anywhere and particularly when voice, video and data apps all originate from the same device.

Integration with third-party solutions

In today's complex and ever-changing world, relying on a single solution is no longer enough. To provide rigorous and robust security, businesses need to be able to rely on a sophisticated mix of tools and technologies. The ClearPass Security Exchange Program seamlessly connects best-of-breed third-party solutions to provide the level of security that modern businesses need, whether employees are working in the office or remotely.

Zero-trust security

Modern network security must accommodate an ever-changing, diverse set of users and devices, as well as much more prevalent threats targeting previously "trusted" parts of the network infrastructure. "Zero Trust" has become an effective model to better address the changing security requirements of the modern enterprise. It assumes that all users, devices, servers, and network segments are inherently insecure and potentially hostile. Aruba ESP with Zero Trust Security improves your overall network security posture by applying a more rigorous set of security best practices and controls to previously trusted network resources.

Aruba ClearPass means:

Awesome scalability

- Purpose-built to scale up to 1 million endpoints.
- Unique clustering capabilities for high availability.
- Every application license scales across the entire cluster.

Built-in certificate authority

- Eliminates need for costly and complicated PKI.
- Device certificates include domain, user and device-type info.
- IT or users can easily remove or revoke certificates for lost or stolen devices.

Seamless, overarching view

- Manage policies for different domains due to mergers or acquisitions.
- No need to duplicate Active Directory credentials across multiple environments.
- Leverage separate authentication and authorisation sources in a single policy.

Industry-leading guest services

- Only guest portal that can be branded and deliver messaging aimed at any user.
- Unprecedented scale and flexibility to support network access for hundreds of thousands of guests.
- Self-registration and sponsor workflows eliminate the burden on IT staff and improve the guest experience.

Why partner with Blue Connections?

Blue Connections is a provider of best-in-class IT solutions to Australian enterprises as well as local and state government departments. Through our partnership with Aruba, we deliver robust and scalable network solutions that help our clients provide a better experience for both employees and customers.

When you work with us, you benefit from our:

- **Experience –** we provide Aruba security and network solutions to some of Australia's best known and established companies, as well as organisations navigating the challenges of business growth.
- **Customised approach –** we create tailored technology solutions that support your desired business outcomes, to allow you to focus on what you do best.
- **State of the art facilities –** our new, custom built premises allows us to warehouse more customised solutions, and includes a dedicated build area, decommissioning facility, vendor training capabilities and an End User Experience Centre.
- **Range of services –** we design, supply, implement and manage end-to-end technology solutions and services specialising in procurement, professional and managed services, staff augmentation, and lifecycle management.
- **In-house team –** all our work is completed in-house, and we have a dedicated Networking and Security team with a deep understanding of Aruba technology and how it can benefit our clients. Our team of dedicated professionals includes sales specialists, professional services staff, technical consultants and managed services staff. We pride ourselves on not using contractors or offshore engineers in every project and support request the team handles.
- **Managed services –** offering a fixed monthly cost per nominated device, and receive proactive management of their technology needs, with 24/7 support available.
- **Dedicated Networking, Security and Unified Communications team –** which provides support across all our services teams, as well as expert network/security monitoring, wireless design/implementations, telephony systems, outdoor long-range wireless point-to-points, CCTV surveillance, security PEN testing, network cabling, WAN design and deployment, and more.

To learn more about how Blue Connections can help your business implement an Aruba ClearPass solution, get in touch on 1800 659 477 or visit blueconnections.com.au/aruba

BLUE CONNECTIONS IT

HPE aruba networking

1. KPMG: Scaling security for remote working **2. 4. 8. & 10.** MyBusiness, Employees are your biggest security threat **3.** CMO, Most Australian Employees to work from home **5.** ZDNet, What is the IoT? Everything you need to know about the Internet of Things right now **6.** Gartner, What Edge computing means for infrastructure and operations leaders **7. & 9.** Aruba, Top 7 requirements for a next-gen edge-ready network