Servium

aruba
a Hewlett Packard Enterprise company

OUTNUMBERED, BUT NOT OUTSMARTED

Servium Aruba White Paper

A 2-step solution to protect IoT and mobile devices

+44 (0)303 334 3000 | www.servium.com | hello@servium.com

HOW DO YOU REALLY KNOW WHAT'S ON YOUR NETWORK?

For most organisations, the answer is you don't. The influx of mobile and IoT devices at the network edge – both corporate and privately owned – makes the challenge of really knowing a big one. The attack surface that accompanies them is equally as scary, putting sensitive data at risk and opening up networks to all sorts of vulnerabilities. Sophisticated and persistent attacks zone in to target the weakest links in your infrastructure. As such, the sheer volume of devices now interfacing with your network means that link could literally exist anywhere, especially as so many connections are occurring outside of your IT team's field of view and their control.

To date, any protection achieved against these threats has been the result of multiple point solutions that are intensive to manage and don't offer a real-time view of your security posture. Limited integration between network and security solutions also makes it difficult for IT to get a complete picture, or identify and adapt to the changing needs of a mobile workforce and respond when a threat is encountered. Furthermore, many of the measures you're likely to have in place including firewalls, intrusion protection and URL filtering are outward facing, monitoring a clearly defined perimeter. Increasingly, the most serious threats are emerging from within the enterprise. Once upon a time, IT had the comfort of dealing with fixed endpoints and well-defined locations and data paths. Now 'within the enterprise' could be a user connecting from anywhere - such is the freedom to interface with enterprise resources.

However, there's no question that mobile and IoT technologies deliver significant value and create welcomed efficiencies. The key is to enable this to continue and in unison keep corporate assets safe.

A new world that brings new challenges

It's easy to think of the challenge simply as a wireless issue, but the reality is that the device explosion is the product of both wired and wireless devices. From BYOD initiatives, GenMobile users to operational technologies included in buildings and machines used in manufacturing processes, all of these different devices are connecting to your network.

Whilst there is huge value to be gained from their presence, this can't be at the expense of protection. It's a hugely complex task. You might be outnumbered by devices, but you don't need to be outsmarted.

Start by knowing what you're up against.

Enterprise Mobility

In the realm of mobile, the network perimeter is anywhere and everywhere a user connects, therefore bypassing traditional gateway defences. What makes mobile devices so attractive also makes them a serious security threat. Powerful productivity features including storage, extensive apps and portability also mean a lot could be at risk when they're so easily lost, often without password protection or only basic security at best. Furthermore, mobile devices are always connected and continually seek out available Wi-Fi networks. Inevitably, this leads to sensitive data being exposed to untrusted and unsecure networks.

GenMobile

The idea of a fixed perimeter that can be secured and maintained is a thing of the past. Today's IT environment is open and mobile, shaped by anytime, anywhere access to enterprise resources. A new generation of users – known as GenMobile – use more devices, work with more apps and challenge security measures more than ever before. These users change their devices regularly too. New devices mean a continual re-examination of security controls to try and deal with the mix of devices in user possession. Other factors like whether devices have been jailbroken amplify their risk to security.

BYOD

Whether formally or informally, your users are increasingly bringing their own devices to work and interacting with company systems and data. These unmanaged devices literally walk right through your front door, evading corporate security controls and connecting right into the heart of your infrastructure. Without visibility of onboarding devices it is not sufficient for IT to simply assume the same trust models that have previously governed corporate-owned devices. Likewise, with privately owned devices comes a world of unauthorised apps and use of cloud storage, potentially risking corporate data under the auspice of improved productivity.

Guest Access

It's not just your staff who are bringing foreign devices onto your network. Visitors will be doing the same too. IT teams need a simple way of enabling these devices to get online but kept away from sensitive enterprise traffic. Likewise, guest networks can be used as a 'work-around' by staff trying to avoid corporate BYOD policies to obtain a network connection. In doing so, corporate data is unnecessarily exposed on open guest networks.

Operational Technologies

Everything from the machines used in manufacturing to smart buildings, environmental controls - even smart lightbulbs! There's a whole new category of device connecting to your network outside of the traditional devices your IT team is used to managing. Unmanaged and unsecured they represent vulnerabilities that can, and indeed have been, exploited by attackers.

Wired Devices

In recent years, organisations have become fixated with securing wireless networks, and in doing so have neglected wired networks and devices at their peril. Wired ports in conference rooms, behind IP phones and even printer areas are often the subject of security oversight. What's more, all sorts of new devices are being wired into your network including CCTV cameras, motion sensors, medical equipment and process controllers. And because IoT devices of this kind lack familiar security attributes and often require access from external administration resources, they get ignored as a troublesome exception.

ARUBA: A NEW DEFENSIVE FRAMEWORK

It's time to mount your defence. Aruba Adaptive Trust is a new defensive framework pioneered to offer an end-to-end solution to tackle new patterns of user behaviour and the rise of new devices now connecting with enterprise resources. Leveraging contextual data across wired and wireless network and security systems, Aruba provides protection from traditional and modern security threats as the worlds of mobile and IoT collide.

At the heart of this approach is the ClearPass family of products, which together offer the central control and real-time security enforcement measures. Through powerful features, Aruba ClearPass offers one place to see and manage it all.

Contextual Intelligence

The ClearPass suite uses agentless discovery to identify endpoints quickly and efficiently and then sorts them according to important attributes that determine device category, vendor, operating system, IP address, hostname, owner, and more. Classified into the correct families, users and devices can be more closely tracked in real-time and security appropriately enforced in relation to these attributes. Acting as a centralised gatekeeper ClearPass identifies and authenticates users and devices using trust-based rules that are continually monitored to grant appropriate access privileges that follow accurate policies.

Adaptive Protection

Armed with contextual intelligence, potential security gaps can be plugged by sharing data across all network security solutions to mount a co-ordinated defence without interfering in user productivity. Security controls adapt to the changing nature of user behaviour and device choice, and recognise that threats can literally originate from anywhere. It means IT can shape policies that determine access privileges on a case-by-case basis without risking exposure to new threats.

ClearPass Use Case - BYOD

- Create a central system for network authentication
- Manage, track and grant access to devices accessing the network
- Prioritise and manage traffic across the network
- Successfully manage a user base of known and unknown users
- Quickly and easily adjust levels of access

Automation

Tackling potentially thousands of devices connecting and re-connecting with your network simultaneously on a daily basis is not a task that can be achieved using manually assigned enforcement policies. Only through intuitive automation can IT teams be unburdened from the task, policies strictly enforced and risk minimised. ClearPass uses secure workflows to profile users and devices around the clock, ready to alert against suspicious activity and take action in the event of a possible threat. What's more, ClearPass comes complete with ready-to-go policy templates to meet BYOD, Guest and IoT initiatives. With the hard work done, IT teams can literally enforce new policies in minutes.

Sharing endpoint visibility

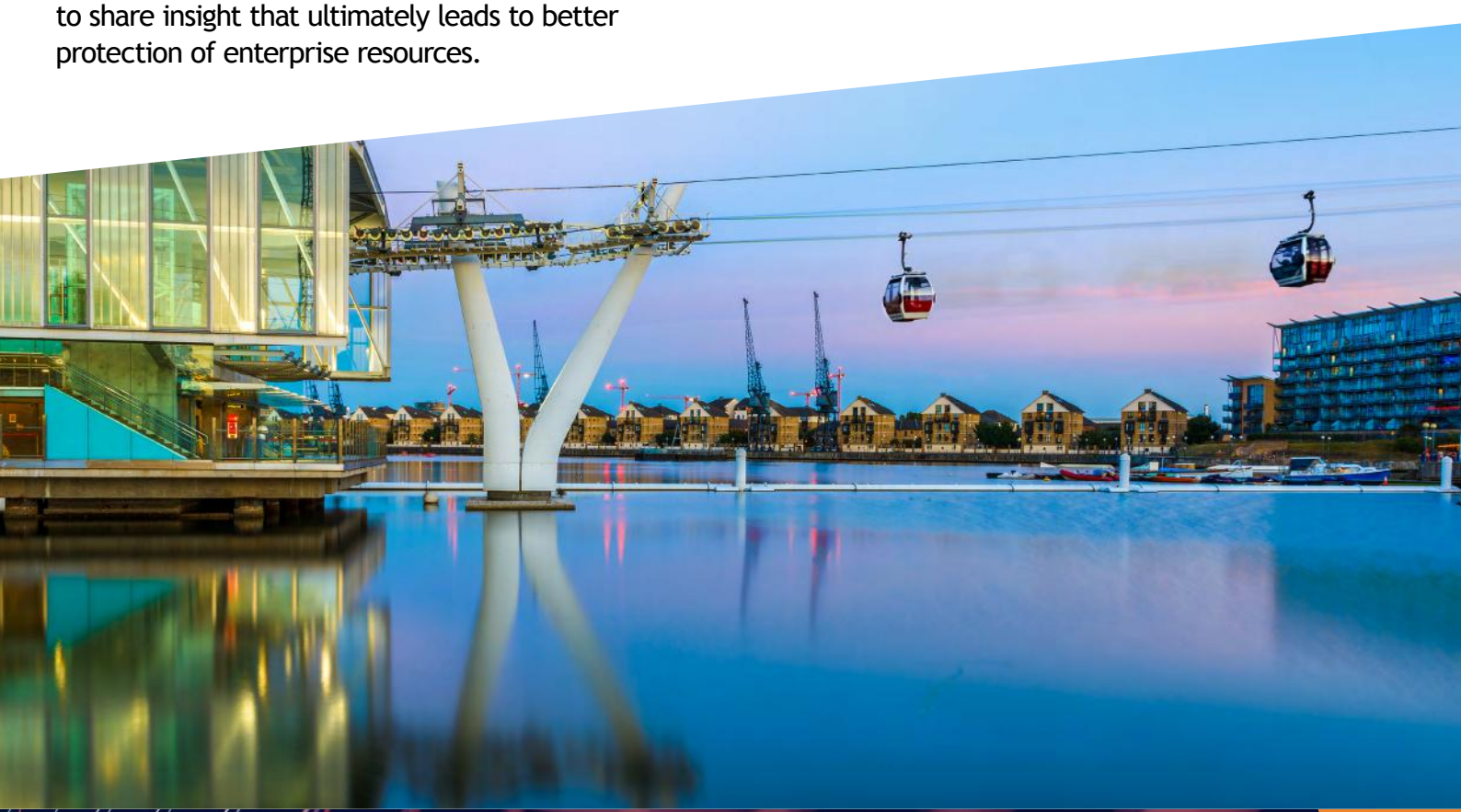
Thanks to ClearPass APIs it is easy to exchange endpoint attributes with many of the different security solutions you already have in place. Tight integration means these solutions can use the data to correlate with traffic patterns specified for each device category, to optimise connections or remediate suspect traffic. Similarly, through unified policy management, ClearPass presents a common way for disparate network and security systems to share insight that ultimately leads to better protection of enterprise resources.

Self-service capabilities

ClearPass is built with IT teams in mind. Wherever possible users are empowered to self-configure devices, revoke security certificates for lost devices and even sponsor guest access. This reduces helpdesk calls and also motivates users to carry out many of the tasks necessary to complete device authorisation. As such, important device healthchecks like virus scans can be undertaken by the user before devices are permitted onto the network.

ClearPass Use Case - Guest Access

- Monitor usage and report on uptake of Wi-Fi services
- Ability to onboard any type of device
- Capabilities for proximity marketing and services augmentation
- Deliver highly tailored interactions based on guest type



WHERE TO BEGIN?

A 2-step solution

Identifying what is on your network is the first step to protecting your data. Then comes a solution to continually monitor devices regardless of type and capable of enforcing your connectivity and security measures based on the policies you set.

Step 1: Identify

ClearPass provides rich profiling visibility and is a great intermediary step to deploying the wider family of ClearPass tools and experiencing the levels of insight that can be obtained from the technology. As a virtual appliance the solution can be live in minutes and is a highly cost effective means of identifying what exactly is on your network.

Step 2: Enforce

With device visibility secured, you're set for automatic policy enforcement. Aruba ClearPass Policy Manager enables you to build automated workflows and enforce smart policies that are right for your business, achieving this across both wired and wireless networks and for every device that connects. With modules covering guest access BYOD onboarding, endpoint assessment, reporting and third-party security integration it offers rich capabilities to deliver enhanced threat protection. Deployed as a physical or virtual appliance it delivers everything to help you keep ahead of the risks your business faces.

TIME TO TRY IT FOR YOURSELF

For a limited time we're offering you the chance to try Aruba ClearPass on a 30 day trial. Essentially a free security audit, we'll tell you everything that has an IP address currently on your network, whilst also giving you first-hand experience of the powerful discovery capabilities of the ClearPass family of technologies.

If you'd like to register for a trial, simply email hello@servium.com or call on +44 (0)303 334 3000.

Servium | aruba a Hewlett Packard Enterprise company