aruba
a Hewlett Packard Enterprise company

MINIMISE RISK. MAXIMISE EXPERIENCE.

IT security is forever chasing a moving target. So how do you strike the balance between security and user experience?

Cybersecurity threats are everywhere. In many cases it's not 'if', it's 'when' your network will be compromised.

But more than ever before, users need freedom. They need to use cloud services, file transfer services, personal email, work email and much more – blocking domains and services is no longer an option.

Today, mobile working, instant sharing and global collaboration are the new normal, driving the everyday user experience. So how do you get digital transformation right without limiting that experience or jeopardizing security?

Too much security means...

...less user freedom. Unrestricted access leaves you wide open to attack. But they aren't mutually exclusive: you can enhance security without creating risk.

Too little security means...

users going it alone, plunging you into a shadow IT nightmare. Or simply users that toe the line of IT process but are unhappy and unproductive.

The user, location, and device is continually in flux, widening the attack surface of the whole network. Security must constantly adjust to meet these shifting demands – IT is following a moving target.

What can CISO`s do to stay secure while giving users the freedom they need?

Turn over to find out

> "84% of companies with an IoT strategy have suffered an IoT-related security breach"*

*Data from a study of 3,100 IT decision makers across 20 countries in January 2017

aruba
a Hewlett Packard Enterprise company

WHY WE SEE ANALYTICAL SECURITY AS THE FUTURE

How can you deliver robust security while meeting the needs of a young, digitally savvy workforce – a workforce that often values user experience over security?

Manage your network, not your people

The answer is automated Analytical security that takes a user-by-user, behaviour-based security approach to assessing risk, all without compromising personal user data or needing to rip-and-replace your existing network security measures.

It's a move away from traditional perimeter security and user-restrictions approach. New ways of working require new ways of looking at IT security.

Way beyond just perimeter security

You need an ever-evolving security infrastructure that can keep pace with the new technologies entering your business. All without restricting performance or user experience – or accessing a user's personal data.

Analytical security achieves this by understanding context and monitoring for patterns in data without using personal information.

It can spot the difference between a regular task, anomalous activity and malicious intent, ensuring user access permissions are kept continually up to date. The result? Attacks are prevented before they have a chance to develop.

Why it must be a multi-vendor solution

Most effective security needs a multi-vendor approach. This means an Analytical security solution based on open standards, letting it play ball with a huge range of third-party security software and hardware. Like any good team, communication is key.

Rip and replace isn't good enough

It's not good enough to ask you to 'rip and replace' your existing tools, spending millions on a new IT environment, when it's possible to overlay new technology.

Automated analytical security should be available to all, and it should be embedded within the network – the point of access for all company information.

> "The future is Analytical security"

LET'S GET ANALYTICAL

WANT TO KNOW MORE ABOUT MULTI-VENDOR ANALYTICAL SECURITY SOLUTIONS?

Contact Aruba today.

Visit arubanetworks.com/security to discover how to make it happen on your network.