FORRESTER®

Managing Distributed Work Environments

Paddy Harrington
Sr. Analyst
Security & Risk

BOLD AT WORK

Paddy Harrington

Forrester Analyst serving Security and Risk Professionals

Background

Paddy is responsible for helping cybersecurity leaders understand the broader endpoint security landscape and guiding them towards the solutions that address their challenges.

Before Forrester, Paddy architected, delivered, trained, and sold solutions across the End User Computing and Application Security market for small, medium, and global businesses.

Coverage Areas

Endpoint Security and Protection

Mobile Device Security

IoT Security

VDI Security

Browser Security

Agenda

The challenges of Anywhere Work

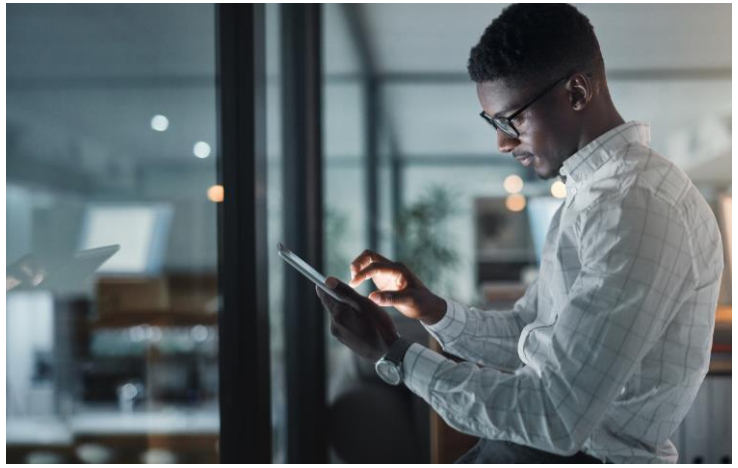
Support from anywhere needs new approaches

IoT/OT Management can be complex when “out of office”

The challenges of Anywhere Work

And not all resources are “in the cloud”

Anywhere Work has many faces



Mobile in the office

Where are your resources?

Are you switching devices?

Are you crossing networks?

Home work

Secure connectivity is needed

Access from non-corporate assets

Is your home network secure?

From anywhere

Open WiFi is a disaster in the making

Turn your back: Where’s your laptop??

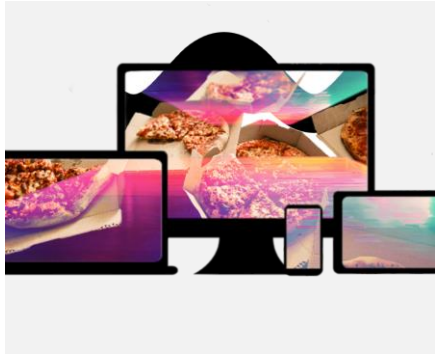
What if your device fails?

Issues with Anywhere Work

What factors contribute to the challenges of Anywhere Work

Endpoint Security

Enterprises with traditionally deployed EPP/ESS have issues maintaining the security of the endpoint when they can't control where it is



Consistent Experience

Users switching between devices and connections can have a disjointed experience because of the different interfaces

BYOD

Anywhere Work often introduces personal devices to the business and IT/SecOps needs to implement controls for devices they don't own

Users work more often

Anywhere Work often leads to people working outside of normal business hours. Issues arise and they need support; how is it delivered?

Secure connectivity

VPN's have inherent security issues because they extend the business network. Controlling user access to resources is imperative.

Not all resources are in “the cloud”

Businesses are adopting cloud, but not for everything

Resources range from apps to desktops

VDI can be costly and a challenge to implement

What is Zero Trust?

- Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: **All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented.**

Source: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

Zero Trust is needed for Anywhere Work

Identify the user

- SSO

Check the device

- Security state, risk level

Limit access

- Apps, data, desktops

Enforce policies

- Control the flow

Monitor the session

- Store analytics

Support from anywhere needs new approaches

Anywhere Work can include IT/SecOps analysts

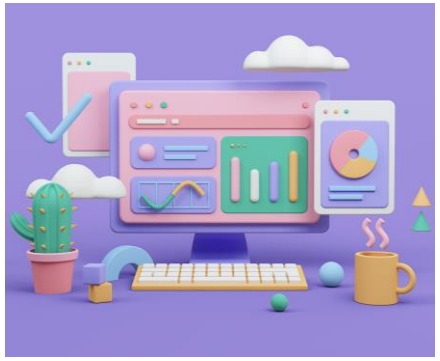
Remote Support complexity

- Assisting users who are anywhere, from anywhere
- Guiding users through issues without seeing their problems
- Users have multiple devices, supporting multiple platforms is critical
- More support needed: Less people to do it

What can help?

The right tools

Support analysts need to have a complete picture of what's happening, including the ability to connect to the remote device to see the problems



Integrate into Mgt stack

Easy integration into the rest of the IT management tools for a seamless experience

SSO

With management tool integration, seamless access for support is needed.

Reduce vulnerabilities

Identifying the vulnerabilities in managed devices and easily patching them from one place is crucial for support analysts

Maintain compliance

Full auditing, secure infrastructure, and deep policy control can ensure your support aligns to standards and regulatory compliance needs

IoT/OT Management can be complex when “out of office”

Management has many faces

IoT/OT Support challenges

Diversity of devices

Often needs rapid changes

Physical access may be needed

Operators have limited external access

Do you need to see the problem?

Simplify IoT/OT Management

Streamlined Management

Ability to guide Operators onsite with equipment is necessary to shorten support times

Assist Operators

Many management systems are costly and complex, beyond what many environments need to support their devices.

From anywhere

Management needs happen when they happen. Solutions need to allow Support teams to implement changes whenever, from wherever, while maintaining security compliance.

Reduce vulnerabilities

Identifying the vulnerabilities in managed devices and easily patching them from one place is crucial for support analysts

May need new tools

Sometimes you can’t just add software to fix remote work issues. You may need to introduce new toolsets to simply things, especially with physical devices

Conclusion

Anywhere Work requires secure connectivity to support zero trust

Support teams need the right tools to work remotely

Managing IoT resources remotely needs new, secure tools

Thank You.

Paddy Harrington