Securing the workforce in times of uncertainty

Katie Burnell
Specialist Systems Engineer, Absolute Software

22 June 2021
Introduction and overview

• I’m Katie from Absolute Software

Today’s session will cover:

• The problems faced in uncertain times
• Secure working essentials
• Why this matters for the future
Uncertain times

• People had to adapt
• Technology had to adapt
• Disparate workforce
• Timelines unknown and shifting
• “Just make it work”-approach

We did what we had to do.
IT and security teams raced to adopt risk management strategies for environments that would have been unimaginable only two years ago.*

* Absolute’s 2021 Endpoint Risk Report
The result

• Technologies ‘hurried in’
• Shadow IT, siloed practices
• Unreachable, at-risk endpoints
• Missing devices
• Loss of control

30% of devices in the financial services sector contained more than 500 instances of sensitive data — a 15% increase from pre-COVID days.

15% of healthcare endpoints contained more than 500 instances of sensitive data — up 12% from before the pandemic began.
It is the unseen, unmanaged risks that result when organizations lack insight and control over their entire endpoint environment.*

* Absolute’s 2021 Endpoint Risk Report
Consequences

- Updates requiring on-network connectivity delayed/ abandoned
- Vulnerabilities left unaddressed
- Lost/ stolen device count increased
- Sensitive data on unencrypted devices
- Critical apps failed

Temporary became BAU
You can’t know what you don’t know.

- Ignorance isn’t bliss, either.
Questions couldn’t be answered…

1. How many of our devices are using a vulnerable version of Chrome?

2. How many of our missing devices are unencrypted? Where are they?

3. Which devices are unpatched for Windows?

4. Is our AV running and healthy on all devices?

Inaccurate asset intelligence causes incorrect (and often underestimated) risk understanding.
An enterprise’s security posture is only as good as the applications that support it… failing applications continue to undermine the best efforts of many security teams*

* Absolute’s 2021 Endpoint Risk Report
A recent Cybersecurity Insiders report found that:

• **60%** of organizations are aware of fewer than 75% of the devices on their network, and;

• **Only 58%** of organizations say they could identify every vulnerable asset within 24 hours of a critical exploit.

Endpoint complexity issues

- *The more the merrier?* FALSE.
- Causes conflict, friction and exacerbates risk
- Piling on apps to support, secure and serve the remote workforce is not a solution

*Absolute’s 2021 Endpoint Risk Report*
The lights are on… but is anyone home?
## 99 Problems

### Lack of visibility
- Dark devices, off network
- Missing/ stolen
- Location unknown
- ShadowIT, app galore
- Unpatched, vulnerable apps
- Critical apps failing
- Policy noncompliance

### Unsecured devices
- AV, VPN off/ unhealthy
- Compromised security controls
- Sensitive data unprotected

### Loss of control
- Unable to effectively:
  - Offboard staff
  - Lock/ freeze devices
  - Alert on location change
Covid forced our hands

- Prompting organisations to perform tasks and follow practices that will now form BAU.
What’s needed

• Unbreakable tether to the endpoint

• Ability to manage/ reach devices remotely and off network

• Ensure/ persist critical apps are on and healthy

• Accurate asset intelligence

• Control: freeze/ block and locate

Enterprises now have an average of 96 unique applications per device, including 13 mission-critical

* Absolute’s 2021 Endpoint Risk Report
An undeletable connection with your devices, to see:

- Where they are, where they have been
- Who’s using them – or are they even being used?
- If critical apps are running and healthy
- If patches and updates are being applied
- If encryption, AV, VPN are on and healthy
Securing the workforce

- A direct, undeletable line of sight to your devices will enable the 4 key elements
- Persist, monitor and keep your critical applications compliant
- Secure your data and devices
- Control the device when needed
73% of respondents say that the impact of the pandemic will alter the way their business evaluates risk for at least the next 5 years

*Pandemic impact report, CSO Online, 2020*
Why bother?

These ways of working and infrastructure demands are here to stay (for the meantime, at least)

- Data risk is increasing as more employees work off-network and more sensitive information is stored on local machines
- Endpoint complexity is escalating as more applications are installed to support new ways of working
- Compromised security controls are widening a gap already ripe for exploit

Infrastructures and endpoints are expected to adapt, support and secure the business in any situation – now, and going forwards.
Ensuring secure working now, and for the future, arms you to weather the storms ahead.

Thank you
kburnell@absolute.com