What did COVID-19 do to your security?

Jisc, October 2020

COVID-19

COVID-19

Before

- Four large offices around the UK: Harwell, London, Manchester and Bristol
- Most colleagues are office based, with 13% home-based workers (120)
- In theory: a flexible working policy exists
- In practice: flexible working practices varied across the company

COVID-19

Since March 17th

- Offices are closed unless you are unable to work from home
- All colleagues are effectively home-based
- The impact of switching to working from home has been different for everyone
- More colleagues are taking advantage of flexible working practices

COVID-19

Impact

- The office LAN has all but disappeared
- Support colleagues can’t easily ask a colleague to bring a laptop to them
- Infrastructure colleagues are not near the equipment they manage
- No colleagues sitting next to you

Suppliers

COVID-19

Impact

- Had to perform a quick analysis of weaknesses in the supply-chain
- Significant concerns about smaller suppliers that were dependent on our business

- Main impact on service delivery has been delay to infrastructure projects due to changes in telco working practices
- Some IaaS/SaaS providers were a bit wobbly for a few days as demand increased

Awareness

Awareness

Impact

- Colleagues can’t ask the person sitting next to you if something looks like phishing
- We can’t check that the home working environment is secure
- No one sees our awareness posters any more
- Induction process for new starters is a bit lonely

However:

- People aren’t printing as much
- All company meetings are more frequent and engaging

Awareness

During the outbreak we've sent regular updates to all staff. Daily at first, now weekly.

These contained reminders about how to stay secure:

- Looking out for scams
- Instructions for VPN
- Updates on how to report phishing

Our internal alerting service is now mandatory, and many staff chose to subscribe to optional messages and alerts.

Endpoints

Endpoints

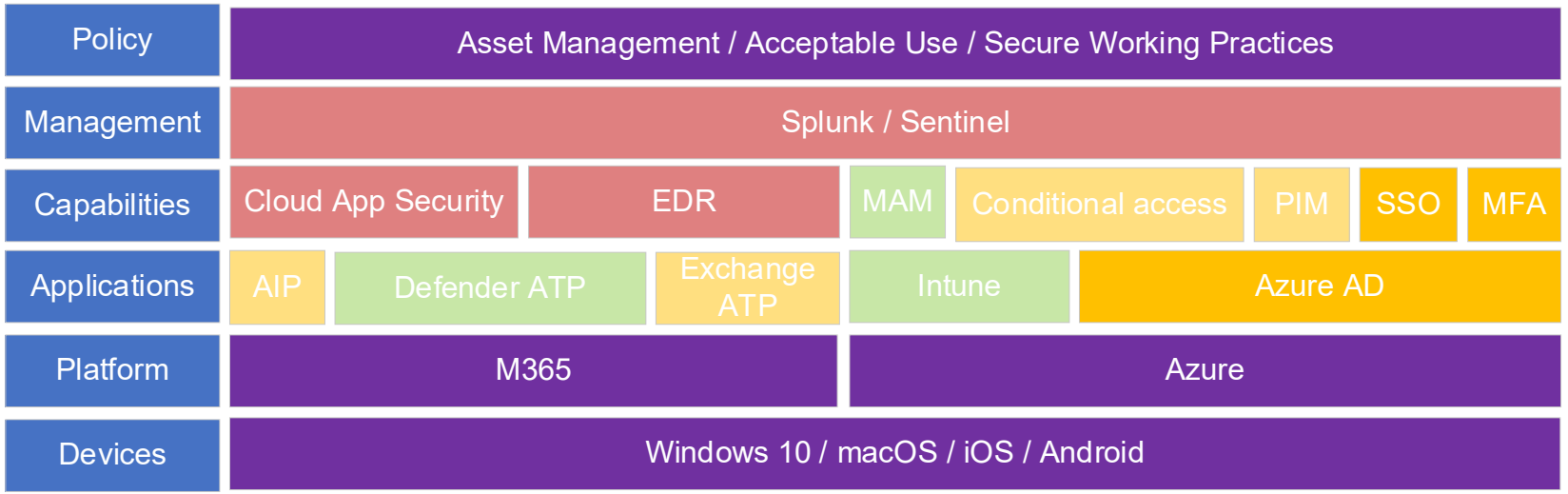
Endpoint devices are no longer sitting on our networks we control, and so the controls at the edge of the office network are becoming increasingly pointless.

This accelerated planned changes to the management of our endpoints. Switching:

- AV software to Microsoft Defender for Endpoint
- Asset management software to Microsoft Intune

This provides us: integration between endpoint protection and M365, EDR capabilities, vulnerability intelligence for endpoints, CASB, c conditional access for M365 and our IdP.

Endpoints



Jisc

Endpoints

Some early wins

Beyond just blocking malware, Defender spotted:

- Some poorly written deployment scripts
- An unauthorised storage device
- Laptops that weren’t consistent with the corporate build
- A Windows 10 device that was failing to update

VPN

VPN

Increased demand

We thought most people who needed VPN access had it. Turns out many of them had never worked from home before.

- Users required proprietary hardware/software tokens for 2FA
- £££££££££…….. and then you've got to get them to users

Solution:

- **Carefully** build some new VPN infrastructure
- Use TOTP instead. Users can authenticate with the Microsoft/Google authenticator app they're already using

After we migrate users to the new VPN infrastructure, we can stop paying the vendor

Jisc

Collaboration

Collaboration

Colleagues use several tools in Jisc depending on their needs and audience

- Microsoft Teams
- Zoom
- Slack

Collaboration

Zoomaggedon

I spent a lot of April reassuring others that:

- Zoom doesn’t have E2E encryption, but neither do our other corporate tools
- Zoom has software vulnerabilities, so does all software we use
- Zoom are fixing vulnerabilities quickly in comparison to their competition
- Passwords really are a good idea. Posting it on a website or public mailing list is a bad idea.

Certification activities

Certification activities

Our ISO 27001 surveillance audit took place entirely remotely

- Made the scheduling easy, no travel between offices
- Sadly couldn’t visit our newly refurbished Bristol office

Also conducted a successful Change To Approval meeting remotely

I also helped a second organisation with their annual surveillance audit

- Their certification body decided to as much as possible offline
- Mostly focused on reviews of documentation, didn’t feel as in-depth