

AFR: 'New normal' is a faster pace of change - blueAPACHE

Canonical: <https://www.blueapache.com/blog/afr-new-normal-is-a-faster-pace-of-change>

Details:

Australian Financial Review, 25 November 2020.

As organisations establish or accelerate their cloud strategy in response to COVID-19, a digital workspace offers a more robust and secure way for staff to work remotely — rather than cobbling together make-shift remote access, which can leave a business vulnerable.

The security finding

Remote working during the pandemic significantly increased the risk of a successful ransomware attack , according to KPMG .

Two factors drove the increase:

Weaker controls on home IT networks — consumer-grade routers with default credentials and unpatched firmware, shared with personal devices, on networks with no segmentation and no monitoring

A higher likelihood of users clicking on COVID-themed ransomware lure emails — attackers exploiting genuine anxiety about health information, government support payments and workplace policy

The need to configure access to various business systems and deploy remote-working capabilities within days, rather than weeks or months , also saw some organisations inadvertently compromise on security in their rush to respond.

What "make-shift remote access" actually meant

The AFR's phrasing is diplomatic. The specific compromises made in March and April 2020 are well documented, and they were made by competent teams under impossible time pressure:

RDP exposed directly to the internet , sometimes without multi-factor authentication — the single most reliable ransomware entry vector of the period

VPN concentrators scaled past their design capacity , or brought back from decommissioning with firmware years out of date

Split tunnelling enabled to relieve bandwidth pressure, taking traffic outside inspection

Personal devices admitted to corporate systems with no management, no encryption and no ability to wipe

Conditional access relaxed because it was blocking people trying to work

Local administrator rights granted so users could install what they needed without a helpdesk visit

Each of these was a rational decision on the day. Collectively they described a materially larger attack surface, and much of it stayed in place long after the emergency passed — which is the part that mattered most.

The digital workspace alternative

The AFR's argument is that a properly architected digital workspace is not merely a better remote working experience. It is a more secure one than the improvised alternative, and in several respects more secure than the office it replaced.

The architecture rests on four elements:

Layer	What it changes
Unified identity and SSO	One authentication path, one place to enforce MFA and conditional access, one action to revoke everything
Application delivery and virtualisation	Applications and data are delivered rather than installed — corporate data need not reside on the endpoint at all
Unified endpoint management	Device compliance is evaluated and enforced, across corporate and personal devices
Experience analytics	IT can see how the environment performs for each user, rather than inferring it from ticket volume

The second row is the one that most directly answers the ransomware risk. When data does not live on the endpoint, a compromised home network has considerably less to reach. And when access is mediated through a single identity with conditional access policy, an unmanaged device on an untrusted network does not simply get in because it has the right password.

Why the perimeter argument stopped working

The underlying shift the article describes had been under way for years; 2020 only removed the option of ignoring it.

The traditional security model assumed a defensible boundary: users inside an office, applications inside a data centre, and a firewall between that and everything else. By 2020 every part of that assumption had failed. Users were at home. Applications had moved to SaaS and public cloud. Traffic no longer passed through any single point where inspection could occur.

Identity became the perimeter, because it was the only control point every access request still passed through. That is why identity consolidation is the first step in a digital workspace programme rather than a later one — every other capability depends on it, and retrofitting it afterwards is considerably harder.

The pace-of-change point

The headline claim — that the new normal is a faster pace of change — held up.

Organisations discovered in 2020 that they could execute in days what they had previously scheduled in quarters. The uncomfortable corollary is that they also discovered how much of the previous timeline had been process rather than necessity.

What did not change is that speed executed on the wrong foundation produces debt. The organisations that came out of the period well were those whose platform choices already supported rapid change safely. Our emPOWER consumption-based model was cited specifically in the company's ARN Mid-Market Partner of the Year win for 2020, on the basis of documented examples of clients rapidly scaling services to support remote working — assessed by an independent judging panel rather than asserted.

What to review now

For organisations still carrying decisions made under 2020 time pressure:

Is RDP or any management interface still exposed to the internet?

Is MFA enforced on every remote access path, without exceptions granted during the transition?

Were conditional access policies relaxed, and were they ever restored?

Are personal devices still accessing corporate data without management or compliance evaluation?

Were local administrator rights granted broadly, and have they been revoked?

Is remote access infrastructure patched to current firmware?

Emergency measures become permanent by default. The review is the only thing that stops them.

Frequently asked questions

What did the AFR article say about remote working and ransomware risk? It reported a KPMG finding that remote working during the pandemic significantly increased the risk of a successful ransomware attack. Two factors drove it: weaker controls on home networks — consumer routers with default credentials and unpatched firmware, no segmentation, no monitoring — and a higher likelihood of users clicking COVID-themed lure emails that exploited anxiety about health information, support payments and workplace policy.

What does "make-shift remote access" actually mean? The specific compromises made under time pressure in March and April 2020: RDP exposed directly to the internet, sometimes without MFA; VPN concentrators run past their design capacity or recovered from decommissioning with years-old firmware; split tunnelling enabled to relieve bandwidth, moving traffic outside inspection; unmanaged personal devices admitted to corporate systems; conditional access relaxed; and local administrator rights granted broadly. Each was rational on the day. The problem was that they persisted after the emergency.

What is a digital workspace, and why is it argued to be more secure? It rests on four layers: unified identity with single sign-on, application delivery and virtualisation, unified endpoint management, and experience analytics. The security argument turns on the second: when applications and data are delivered rather than installed, corporate data need not sit on the endpoint at all, so a compromised home network has much less to reach. Access mediated through one identity with conditional access also means an unmanaged device does not get in merely by presenting the right password.

Why did the traditional network perimeter stop working? The model assumed users inside an office, applications inside a data centre, and a firewall between that and everything else. By 2020 every part of that had failed — users were at home, applications had moved to SaaS and public cloud, and traffic no longer passed through any single point where inspection could occur. Identity became the perimeter because it was the only control point every access request still passed through, which is why identity consolidation comes first in a digital workspace programme rather than later.

What should an organisation review if it still carries 2020 decisions? Six things: whether RDP or any management interface remains internet-facing; whether MFA is enforced on every remote access path without leftover exceptions; whether relaxed conditional access policies were ever restored; whether personal devices still reach corporate data without management or compliance evaluation; whether broadly granted local administrator rights have been revoked; and whether remote access infrastructure is patched to current firmware.

What was blueAPACHE's connection to this story? The emPOWER consumption-based model was cited in blueAPACHE's ARN Mid-Market Partner of the Year win for 2020, on the basis of documented examples of clients rapidly scaling services to support remote working. That assessment was made by an independent judging panel rather than asserted by the company.

Is this article still current? It was published on 25 November 2020 and describes the conditions of that year. The architectural argument about identity as the perimeter has held, but the specific pandemic context has passed. For current services see the linked pages rather than this article.

Related

Security services
emPOWER Security
emPOWER SASE — identity-mediated secure access
Human risk management — the phishing-lure layer
Managed detection and response
Microsoft practice — identity, Intune and conditional access
Collaboration
Cloud services
Managed services
Governance, risk and compliance

Source

Original article published by the Australian Financial Review , 25 November 2020. Ransomware risk findings attributed to KPMG.

Knowledge Base

Why did some organisations compromise on security when responding to the pandemic, ?

the need to configure access to various business systems and deploy remote-working capabilities within days, rather than weeks or months, led some organisations to inadvertently compromise on security in their rush to respond to the pandemic.

What call to action do you present at the end of this blog post?

The page invites readers to 'Outpace Change' by partnering with us to improve performance, strengthen security, and simplify complexity through IT Operations Excellence as a Service, with options to speak to the team or get support.