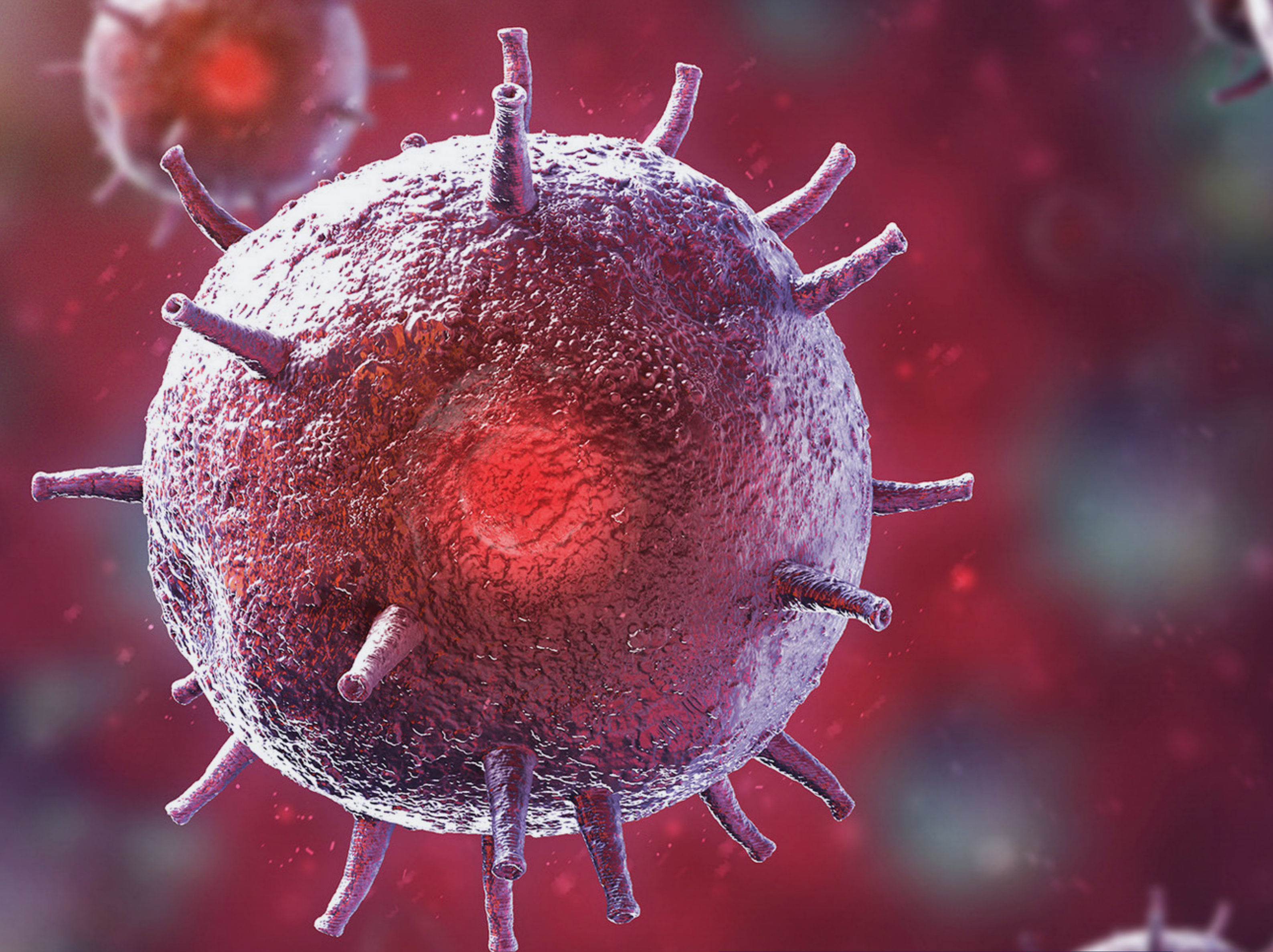
LEARNINGS FROM THE CURVE:

Securing cloud in our new environment

A Secure Agility report based upon a roundtable with multi-industry, IT leaders

SECURE AGILITY



The restrictions put in place in response to the COVID-19 pandemic triggered massive and rapid changes to the ways organisations do business. Some of these changes meant accelerating a process that was already underway, while some of them came out of the blue, and in many cases exposed gaps that might have gone undetected otherwise.

To determine the most prudent steps forward in 2020, Secure Agility hosted a virtual roundtable where customers could share best practices for remaining secure during rapid change. Moderated in conjuction with cloud security experts from Palo Alto Networks, the IT leaders related their insights from various sectors including manufacturing, local government, education, finance, health and disability services.

This report, Learnings from the curve: Securing cloud in our new environment, highlights what these changes have meant, the challenges they have posed, and what the future might look like.

covidlearningcurve.com

Contents

The three-phase rush towards the transformed workplace

Taking us by surprise, COVID-19 showed how many organisations are undergoing three distinct phases of transformation as a result of the pandemic.

1. Rapidly scaling up to a remote workforce

Sean Duca, Vice President and Regional Security Officer APAC and Japan at Palo Alto Networks, said the first phase involves rapidly scaling up to remote working, which most organisations have already done.

This involves finding efficient ways to use collaboration and video-conferencing tools from any location, while staying secure.

This first phase, has exposed limitations in the tools people use to access remote working, thanks to the massively increased workloads with which these tools are suddenly having to cope with.

An IT manager from Local Government pointed out another issue: security.

"Most of our staff traditionally work in the office, so moving 850 users to work from home immediately caused some load balancing issues," he said. "We only have two main sites, where we have our firewalls and VPN access points, so we had to balance that as best we could rather than having everybody coming through the primary site. That worked initially, but we have had lot of performance issues, particularly associated with people doing video conferences on Teams and Skype."

With the rapid rise of video conferencing, companies like WebEx or Zoom have seen sudden mass adoption, and that has exposed some capacity and security issues that people were not concerned about before.

A customer in the Education sector agreed, saying "we did have Zoom-bombing occur, people using random generation of Zoom meeting numbers and just jumping into meetings. That was locked down so we've got things like waiting rooms now, so the host has to let you in, we've got password security on all the meeting numbers."

> "We've been getting heaps of phishing attacks. Most of them just seem to be targeting the users who are willing to click on an email. We had to implement geo-blocking on our OWA in order to mitigate those attacks."
>
> Director of IT
> Healthcare organisation

2. Realigning business continuity plans

Business continuity is difficult at the best of times, but the lesson from COVID-19 is it must change to fit with any accelerated transformation.

Organisations have been fast-tracking projects that would otherwise have taken years, down to months or weeks, and consolidation of spending and technology is an ongoing trend for both customers and the security industry.

This second phase involves going back to business continuity plans and realigning them with the new reality, and automated tools offer help when old habits and processes can't be implemented anymore.

"What's changed in literally every organisation is that five years ago people were running SAP and Exchange on-premises. Fast-forward to today, half that stuff is sitting in AWS or consuming it as a service," according to Duca. "There's a range of things and people need to align what's out, what's in, and what should we start to aggressively push out as well."

Charlie Tannous, Technology Director at Secure Agility said automation can play a key part in business continuity and security, and the opening up of APIs events can trigger an automatic response to pinpoint what's happening in the environment and neutralise it.

"Everyone is talking about automation and it's a big topic in managed services as well. You can be very agile and very effective without having to have a team of five or six people that are continually watching for threats," Tannous said.

> "I've even heard people say 'we were going to go on a transformational journey and it was going to take the next two years, but people are now putting their foot on the accelerator and saying 'we've got to get this done in the next six to nine months'."
>
> Sean Duca
> Vice President and Regional Security Officer APAC and Japan at Palo Alto Networks

> “People will be working from home more regularly, but there’s still the need for the social contact and everything else that comes with working. I think we’re going to define what the new normal is over the next six months.”
>
> Head of IT
> Local government organisation

3. Bringing work to people

Thirdly, the final phase addresses the ‘new normal’ of a distributed and remote workforce.

This ongoing phase will increase the importance of Cloud-based (SaaS and IaaS) products and have lasting consequences for the work environment, from commercial real estate to new perspectives to office layouts and hot-desking.

According to Duca, we’re going to redefine work and re-architect our environments to say “let’s take work to people”.

“That just means doing some things differently, such as consuming things more as a service, will start to become the norm,” he said. “And I’ve spoken to large and small organisations, it’s not one size fits all.”

Taking control of the challenges

With so much change and the associated challenges, Australian organisations need to be proactive managing and securing their new working environments.

The nature of the challenges include fragmentation, obsolete controls and a lack of visibility, which can arise from digital transformation, remote working and cloud adoption. In the case of remote access, there is a demonstrable failure of the traditional VPN.

Organisations have learned that not all VPNs are created equal. A lot of them are not designed to scale, so they fail from the perspectives of both capacity and licensing.

"That's a key drawback of on-premise VPN as opposed to Cloud," observed Riccardo Galbiati from the office of the CSO at Palo Alto Networks.

There are products, such as Palo Alto's Prisma Access that address this challenge at the edge, and at the Cloud. With apps like Zoom, you can play 'traffic cop' and decide who can use it and perform inspections of the application traffic.

> "We recently revamped the firewalls late last year and started rolling out the Global Protect VPN straight to them. And that's certainly made our lives very easy. So, when it came time to move to working remotely, we were able to do it in less than about two weeks."
>
> Digital Strategy Portfolio Manager at an Australian university

> "When I ask 'what do you have in the Cloud' people can tell you the services but they don't actually know the workloads or the type of data that they're hosting and where it is. That type of fragmentation is the source of all problems when it comes to security."
>
> Riccardo Galbiati
> Cyber Advisor with the office of the CSO at Palo Alto Networks

Securing the new distributed workplace

The new workplace will be distributed and bring together a range of business and consumer technologies.

Security is always important, but it has become a more significant issue in the distributed workforce as cyber-criminals are very adaptable and able to exploit technology trends like video-conferencing.

We are already seeing an increase in targeted email phishing, scam and ransomware attacks exploiting the COVID-19 uncertainty.

During this time security education campaigns are more important than ever. In addition to awareness, multi-factor authentication (MFA) is needed as a default component of security tools to prevent the sole reliance on passwords, which can be stolen or cracked.

> "We have several users who received email and they responded, asking 'did you send me a table, or a document' and the attacker actually responded back, from that account, to improve their chances, and said 'ah yes, actually, I need you to review this document'. Obviously, you can't blame the users if, after that, they opened the document."
>
> Security Director
> Education institution

Conclusions and actions to take

With rapid change already forced upon every industry, here are some steps you can take to make the most of the learnings so far:

1. Limits will be stretched

During a rapid workplace transformation all the practical limitations of cloud and collaboration services come to the fore, in addition to their security vulnerabilities. Be prepared to mitigate these limits.

2. Business continuity has changed

With use of cloud apps, organisations need to rethink how they perform business continuity in the event of a problem like COVID-19.

3. Work is coming to people

People will not be working in central offices as much and will work from home or other remote locations. Security must adapt to keep ahead of this change.

4. Network security is paramount

With more cloud apps and remote locations in use, the traditional on-premises VPN is becoming obsolete. Organisations should look to cloud-based VPNs to ensure they are covered regardless of which apps they are using and the location they are at.

5. Education is key

With the changing nature of work and collaboration, attacks are also changing. Secure organisations will keep their staff informed of new and emerging threats and how to prevent them.

Prepared in co-operation with paloalto NETWORKS

About Secure Agility

In a complex world that challenges technology to solve almost everything, Secure Agility provide the answers.

As a leading provider of professional and managed services, we specialise in high availability enterprise-level solutions encompassing market-leading technologies across End User Computing, Network, Storage and Cloud.

secureagility.com

SECURE AGILITY