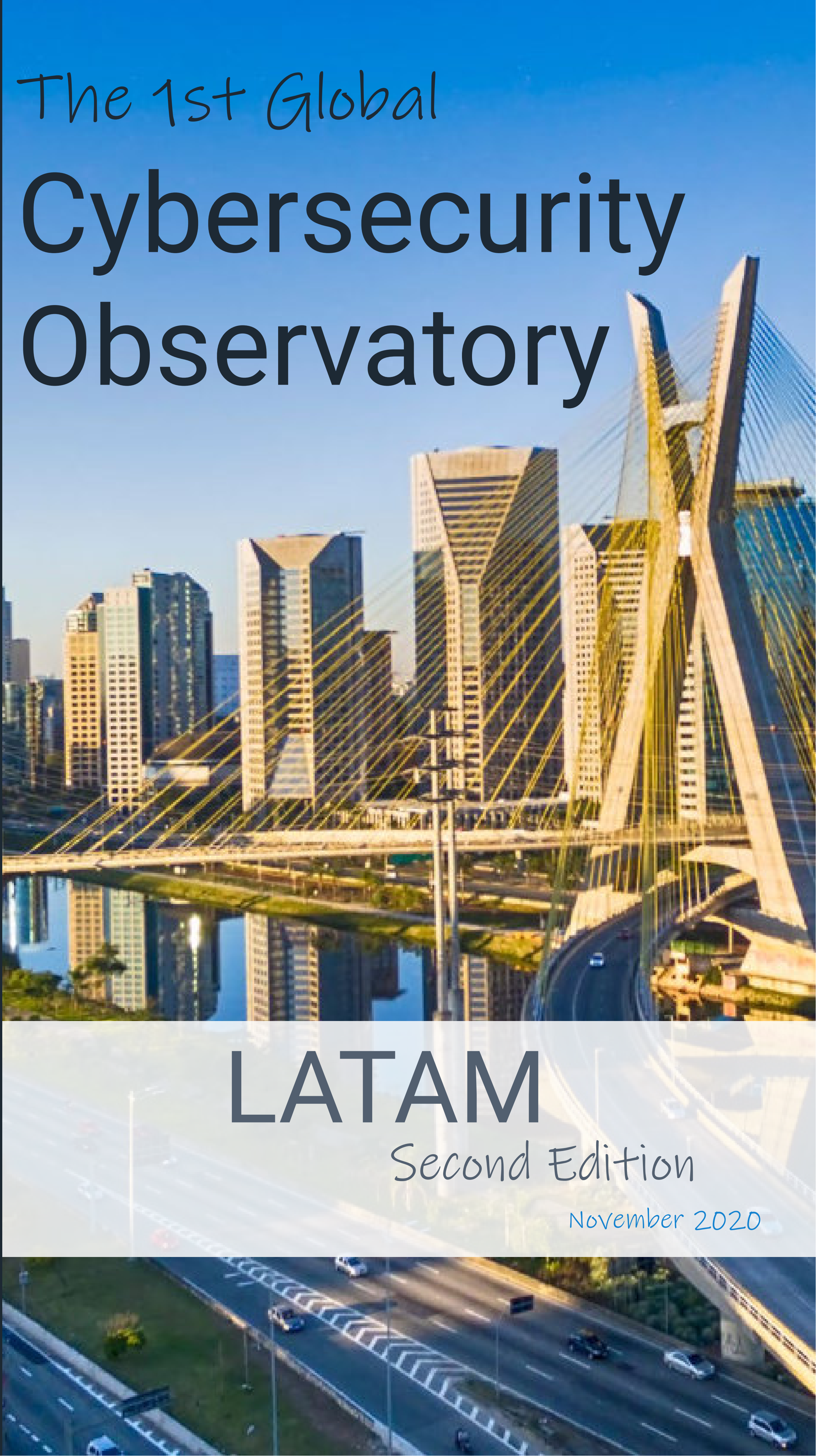
The 1st Global

Cybersecurity Observatory

cyberstartupobservatory.com



LATAM

Second Edition

November 2020

Insight

Blu5

You may need to revise your BYOPC strategy. Here is why!

You may need to revise your BYOPC strategy. Here is why!

At a glance

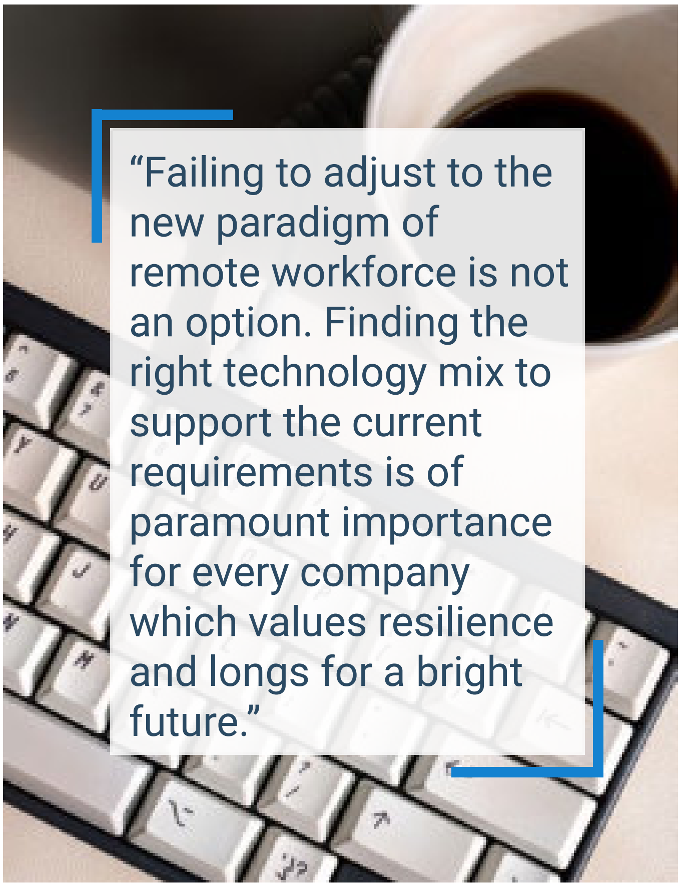
- 4 minute read
- The downsides of remote work
- Bandwidth and connectivity concerns
- The way forward
- The role of secure unified workspace

We were all out there and we all experienced first-hand what happened to our teams and our businesses during these stressful times. Everyone did their best, pouring in resources and incredible energy to keep things going, to allow colleagues to work with what was available. When the peak of the emergency was over, we looked for improvements to get ready for the next round.

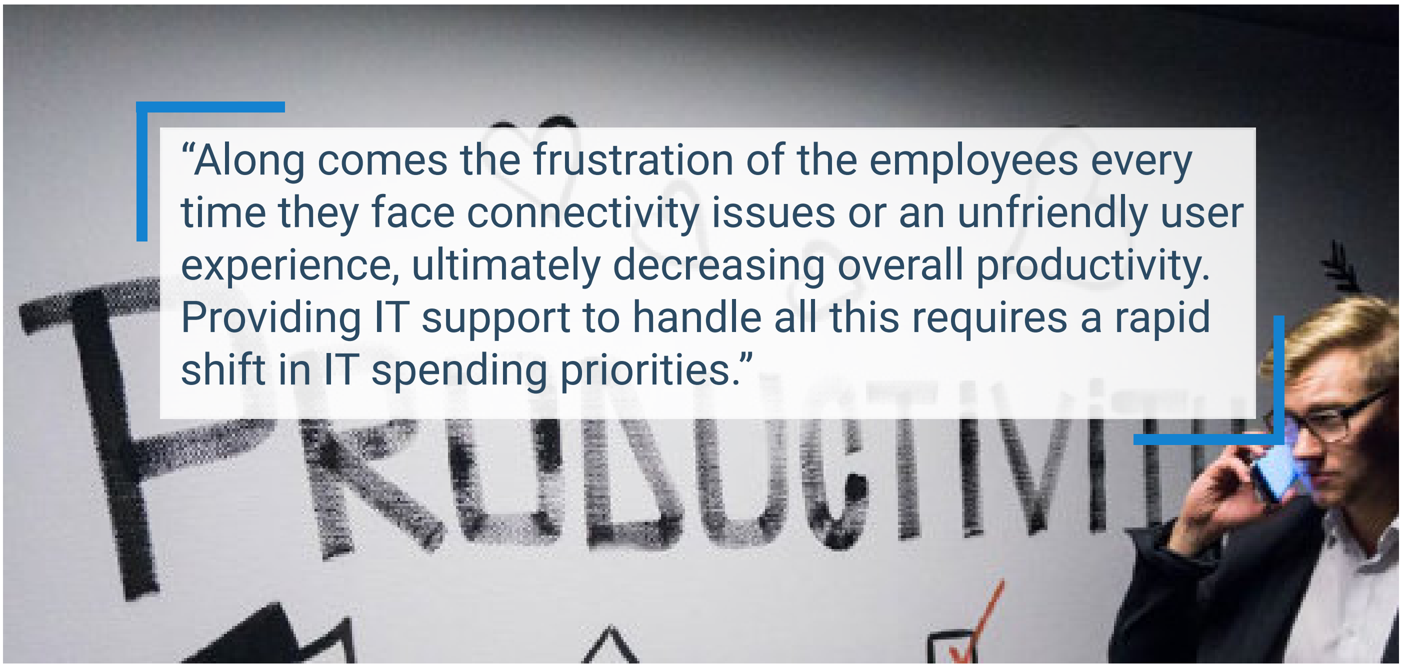
The COVID-19 pandemic has increased the scale of remote work at an unprecedented rate. According to a Eurofound survey conducted in July 2020, more than one in three employees worked exclusively from home, with more respondents engaging in remote work part time. The researchers claim that many companies were not ready to accommodate the sudden increase in remote work: "The transition to working from home was unplanned and ad hoc, based on using the employee's own IT equipment and pre-existing home connectivity".

With less than half of all employees receiving remote work equipment from their employers and companies prioritising business continuity over anything else, employees are using their own devices to work. Bring Your Own PC (BYOPC), is not a new concept.

However, many companies were forced to resort to a dangerously unmanaged form of BYOPC, neglecting security and compromising productivity. Failing to adjust to the new paradigm of remote workforce is not an option. Finding the right technology mix to support the current requirements is of paramount importance for every company which values resilience and longs for a bright future.



"Failing to adjust to the new paradigm of remote workforce is not an option. Finding the right technology mix to support the current requirements is of paramount importance for every company which values resilience and longs for a bright future."



"Along comes the frustration of the employees every time they face connectivity issues or an unfriendly user experience, ultimately decreasing overall productivity. Providing IT support to handle all this requires a rapid shift in IT spending priorities."

The Downsides of Remote Work

Increased risk exposure

Unmanaged BYOPC devices are not aligned with any security policy, which is an obvious threat to company assets and reputation. Malicious actors can take advantage of pre-installed and miscellaneous software present on the machine and which are likely to bring along multiple unknown issues for the integrity and the security of a company.

Such considerations are in line with the "Assumed Breach Model", a strategy where the fundamental assumption is that any given endpoint is already breached. This is always true, but even more in a scenario involving unmanaged PCs. The ultimate goal is to accurately identify and create a strategy to manage risk.

Devices with unrestricted access to the corporate network, typically provided by conventional VPNs, are a big NO-NO! Under ordinary circumstances, companies would at least make sure that devices are configured for security. But, driven by the primary goal of guaranteeing business continuity, companies rushed into BYOPC, to find themselves allowing unsecured devices onto their network, lowering their security guard. Actually, VPNs showed their intrinsic weaknesses while stressing the communication networks to the brink of collapse because of bandwidth requirements.

IT Support and Management Burdens

The lack of visibility of every device often makes IT support a complex task, especially in terms of configuring, managing and securing distributed remote devices. Remote work troubleshooting and endpoint configuration put a huge strain on IT help desks facing a lot of complexities you don't usually run into in the office environment, such as different device setup, network connection and misconfigurations of third-party software.

Along comes the frustration of the employees every time they face connectivity issues or an unfriendly user experience, ultimately decreasing overall productivity. Providing IT support to handle all this requires a rapid shift in IT spending priorities.

Bandwidth and Connectivity Concerns

Companies should take into account that not all employees have high-speed Internet at home; therefore, the connectivity problem becomes worse when there are multiple people working at home, video conferencing to class, watching movies or playing games. Further, many employees use a conventional VPN to access the company's network from home.

These VPNs are known for slowing the connection down due to bandwidth consuming encryption processes affecting the network quality. But the biggest issue is recorded when so many devices are accessing the VPN at once, making VPNs running out of capacity. The lack of constant high bandwidth makes video conferencing and sending big attachments by email difficult.

The Way Forward

1. Implement a Zero-Trust-Network-Access Strategy

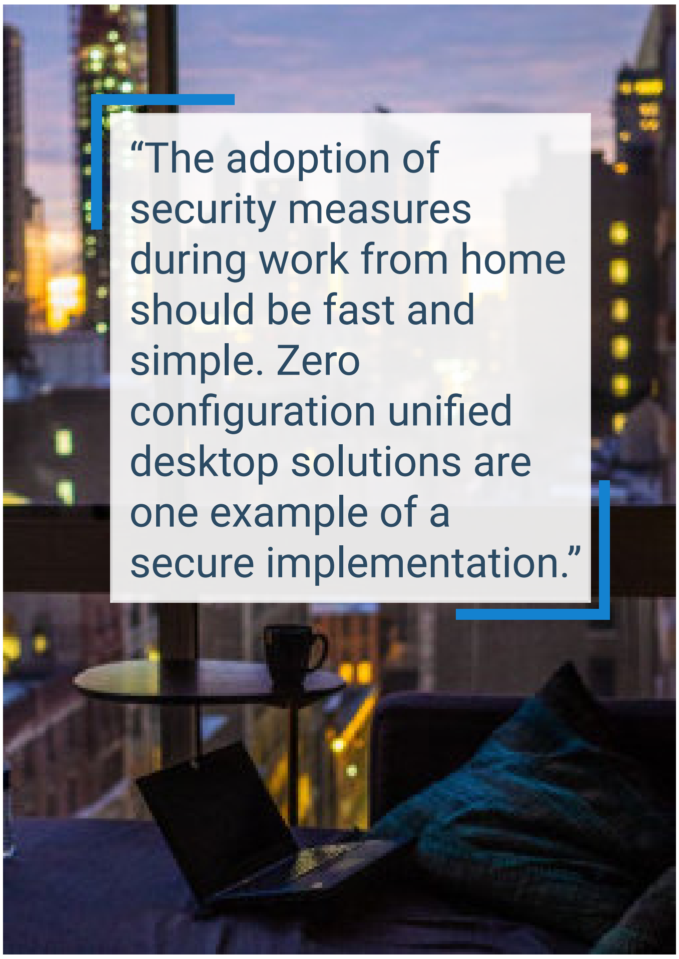
Zero-Trust-Network-Access (ZTNA) refers to "products and services that create an identity-and-context-based, logical access boundary encompassing a user and an application or set of applications" (Gartner).

Under ZTNA, applications are hidden and access is restricted. The administrator grants access by verifying identity, context, and policy adherence of participants. Such an approach reduces the surface of attack, making it more secure.

Moreover, the fine-grained access control allows companies to customise the level of access granted to each role. Excessive privilege is no longer required to access the company's network and security is not compromised. Hence, the company gets the flexibility to work remotely with external partners while sharing critical data with employees that need it. Network communications are encrypted end-to end, adding an extra layer of security. ZTNA does not rely on the device to be completely secure or free of malware.

2. Minimise IT hours and cost adopting a Zero Configuration solution

The adoption of security measures during work from home should be fast and simple. Zero configuration unified desktop solutions are one example of a secure implementation. For such solutions, configuration is carried out centrally by the administrator.



"The adoption of security measures during work from home should be fast and simple. Zero configuration unified desktop solutions are one example of a secure implementation."

Setup is seamless for the employee, which enhances security and increases productivity. This could be as simple as installing software and logging into their account through the unified desktop. It reduces IT support man-hours while protecting the company's assets. In addition, turnaround time for deployment can be as fast as several hours for the entire company.

3. Mitigate Bandwidth Issues with Split-Tunnelling Architecture

The default policy of conventional VPNs is "full tunnel architecture", which means that all traffic is routed through the VPN tunnel. Split-tunnelling, instead, only routes some applications through the VPN tunnel and can be configured to only route company relevant applications and file requests. This in turn, mitigates many of the bandwidth issues associated with conventional VPN architecture, while keeping the company's assets secure.

Critics of split-tunnelling argue that malware could still affect the device because non-corporate internet traffic does not pass through the security stack (European Business Review). However, such drawbacks can be mitigated by choosing an appropriate unified workspace solution. While the unified workspace is connected to the corporate network, the rest of the workspace environment is isolated from the user's desktop, preventing malware from entering the workspace.

The Role of Secure Unified Workspace

Unified workspaces may allow companies to move ahead through the above-mentioned steps, gaining efficiency and security at the same time. The embedded security features can deliver interesting options for an innovative approach, which brings along considerable savings together with a structure ready to embrace the next steps towards a more cloud centric infrastructure.

References

Eurofound: Living, working and COVID-19, Updated 6th November 2020

Gartner Glossary: Zero Trust Network Access, 2020

European Business Review: The Use of Split-Tunnel VPNs for Scalability Jeopardizes Enterprise Security. Accessed Oct 30, 2020

Gartner: Hype Cycle for Digital Workplace Infrastructure and Operations, 2020

"Unified workspaces may allow companies to move ahead through the above-mentioned steps, gaining efficiency and security at the same time."

The
Cybersecurity
Observatory

LATAM - Second Edition