Long View

Your multi-cloud deployment isn't as secure as you think.

A guide to securing 'fluid' perimeters and our solution to the cross domain security challenge.

Introduction

In this eBook, we discuss the security challenges of enabling remote work, and the steps organizations must take to protect their employees, customers, and intellectual property. We'll look at some of the tools — and importantly mindset — needed to harden your defenses, and how a comprehensive approach of cross domain security, across identity, access endpoints, data and applications, can secure your investments on cloud providers like Azure and multi cloud environments.

If the last few years have taught us anything, it's that the workplace is no longer a place on a map. Now, enabling hybrid work — combining the ideal mix of remote and in-office work — is the new norm.

Organizations enabling a hybrid workforce must find the delicate balance between the tools that employees enjoy and the vulnerabilities they introduce. While employees accessing company resources from anywhere on just about everything requires fresh mobile device management policies.

Enabling hybrid work also sped up cloud migrations. The scale of which created a whole new world of issues, including increased strain on both cloud and on-premises infrastructures along with a host of security concerns.

The pivot to remote work left security behind

The shift to remote and hybrid work has been a boon to opportunistic cybercriminals — and a costly one for organizations.

According to IBM's Cost of Data Breach Reports conducted by Ponemon Research, the average data breach cost increased from $3.86 million in 2020 to $4.24 million in 2021 to a record-breaking $4.35 million in 2022.

Most organizations aren't focused on security, but on their core business, and many business leaders don't understand the depth and complexity of modern cyber threats, often refusing to act until they are on their doorstep or, to be more precise, inside the business.

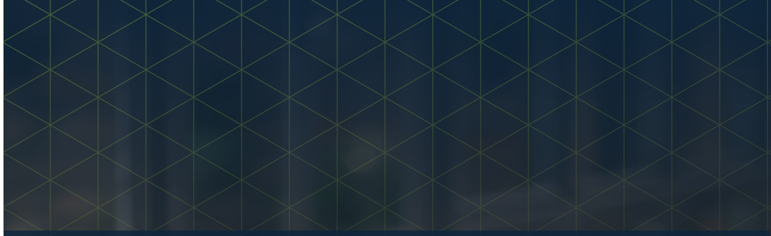
It's a recipe for disaster, as remote employees expect access from anywhere, always, and on any device — regardless of whether they've been recently patched or updated. These employees quickly become the weakest link in the security chain, and prey to the nearly continuous phishing and spoofing attacks.

Hackers prefer employees that sit outside the perimeter

Hackers were fast to take advantage of the speed at which organizations had to make the jump to remote work, deploying phishing campaigns and ransomware to attack employees now sitting outside the enterprise perimeter.

Counting on slower patching from work-from-home employees, large bad actors took advantage of exploits and zero-day vulnerabilities. The haste with which employees' remote systems needed to be deployed increased the likelihood of administrators making mistakes around email credentials.

Of course, not everyone started the move to remote work and their cloud adoption to support it from scratch. Many had already migrated compute, server, or storage workloads to the cloud, or simply more aggressively deployed SaaS solutions already in place like Office 365. Still, the issues around security raised their ugly heads as threats climbed, attack surfaces grew, and they realized their cloud was not as secure as they thought. Add to that attack surface the rise of multi-cloud environments, and fact it's becoming increasingly vital to have more than one cloud environment.



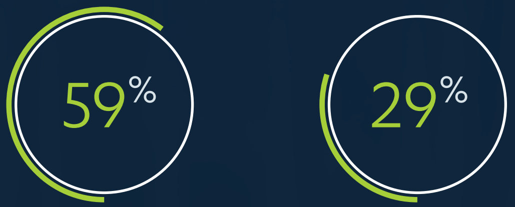
But, most enterprise applications are inherently secure…right?

Compromised accounts can take months to detect, and still more time to contain, meanwhile the bad actors are running rampant inside the organization with their stolen credentials, costing the business more by the day.

And that cost is rising, not just in terms of lost work and revenue from downtime, customer trust and resulting lawsuits or ransom payments - but cyber insurance. As data breaches become more costly and more frequent, the cost of cyber insurance has climbed to keep pace.

Global cyber insurance pricing increased by approximately one-third between 2020 and 2021[1], alongside a greater demand from insurers that organizations have more rigorous attitudes towards cybersecurity. It is now expected that the insured show evidence of preparedness, resilience, and appropriate risk management practice.

The assumption is that the major enterprise applications are secure and, while both have security tools and measures, they aren't inherently secure.



Six in 10 Canadian organizations have cybersecurity insurance coverage as part of their business insurance.

Three in 10 of them have a cybersecurity-specific policy.

Canadian Internet Registration Authority, 2021 Cybersecurity Survey

Do we really need cyber insurance?

Cyber insurance is specialized insurance designed to protect organizations from Internet-based risks, like malware, ransomware, DDoS (distributed denial of service) attacks, and more.

A more robust security solution reduces costs and, in fact, is becoming an expectation. In a period of rising inflation, ongoing supply chain challenges, and heightened competitiveness, many organizations are having a hard enough time just keeping afloat — without the extreme losses associated with a breach or paying high insurance rates because they are at greater risk.

[1] Cyber insurance costs up by a third (computerweekly.com)

Guarding a cross-domain perimeter requires a cross-domain strategy

In the past, securing the enterprise was like defending a castle. You'd build defences — a moat, tall heavy fortifications, a strong gate — around the perimeter and feel confident that no one could get in without an invite.

Once safe behind corporate firewalls and policies, applications, servers, and data living in data centers and accessed either physically at the office or via VPN were backed up offsite and, ideally, disaster recovery was tested periodically.

All of this worked well until the cloud came along and organizations started having to defend themselves across multiple security domains.

Your perimeter is probably leaking

Today, employees work outside the castle walls, and your fortifications may fail to protect them. The area you need to safeguard acts more like water than a container. And as the saying goes, "water finds a way." As such, every endpoint must be secured to prevent leaks.

Now applications and data are residing entirely on the outside of the formerly well-fortified castle, and, truth be told, in multiple cloud fiefdoms. This limits visibility, expands the attack surface, and introduces new compliance risks. The job of protecting your critical apps and valuable data has not gone away with the cloud, it's just become more complex.

Who do you have to fix it?

- A 2018 study found that 94% of IT organizations struggle to find the right talent to build dynamic, flexible, and cost-effective cloud services.
- There are currently an estimated 3.5 million unfilled cybersecurity jobs globally — building a complete team would be costly and unrealistic.

Finding experts who truly understand how to secure multi-cloud environments is an ongoing challenge of epic proportions. Even if the resources are found, reviewing the volume of logs and anomalies that occur in today's threat landscape was humanly impossible, making SIEM (Security Information and Event Management) tools crucial.

Bridging the gap between the versatile skill set common in IT teams and the skills needed for cloud, hybrid cloud and multi-cloud environments remains a huge challenge.

What happens if we do nothing?

As noted, business is booming for hackers. Phishing attacks are on the rise, especially those combining email and social engineering via voice calls (vishing) — which jumped more than 600 percent over just a few months in early 2022.

Phishing itself grew tremendously over the pandemic with the FBI reporting 11 times more phishing attacks reported in 2020 than four years prior, and 91 percent of security breaches started through phishing attacks.

In the past 12 months, almost one in five (17 percent) Canadian organizations have been the victim of a successful ransomware attack. A majority of them (69 percent) paid the ransom, while 59 percent report that data was exfiltrated.

— Canadian Internet Registration Authority, 2021 Cybersecurity Survey

With the addition of ransomware, cybercriminals have figured out how to hit organizations where they hurt. You've invested all this time and money into technology to support the organization and its goals, and now it's locked up. Why even bother investing in technology you are going to lose control or access to it?

Because User Shield is cloud-based, it eliminates security infrastructure setup and maintenance and provides elasticity, reducing costs by as much as 48 percent of traditional SIEMs.

User Shield: Securing on-premises and across the entire cloud ecosystem

User Shield is a cross domain security managed service powered by Microsoft Sentinel and Long View's 24x7 SOC.

SIEMs are a necessity, but they must still be managed, and by a team that has specialized expertise in cloud security, risk assessment, compliance, and other cybersecurity disciplines. With a scarcity of such expertise to be found or trained, there's no denying that managed security services can help.

User Shield pulls it all together connecting, securing and monitoring firewalls, load balancers, access points and switches for end-to-end protection from today's constant threats. Think of it like "managed Sentinel." It hardens your environment, configuring it correctly to close off domains to avoid spoofing or properly enforce the MFA (Multifactor Authentication) needed for a zero-trust security model.

In addition to installing Sentinel in client environments, connections are made to Long View's own multi-tenant version of the SIEM to provide valuable insights into threats and suspicious behaviour being seen across the threat landscape.

Importantly, User Shield opens up and closes off security domains as appropriate, providing a control plane to address mature security needs that simply cannot be handled by a single software or hardware solution or in silos.

All of this is combined with Long View's proven, robust cybersecurity rules and playbook to separate the SIEM alerts that need to be followed up on from the 'noise'. These rules and automated playbooks have been developed over years working with organizations with the strictest regulatory policies, like the big banks. Long View works closely with the client to develop a Security Incident Response Plan (SIRP), outlining the actions to take should an incident occur. Our 24x7x365 Security Operations Center provides ongoing monitoring and expertise to triage, respond, and react to incidents, as well as the monthly reporting needed to measure the cybersecurity system's success.

User shield simplifies security, while providing a modern solution that protects against modern threats and challenges, protecting the enterprise regardless of footprint or platform.

To avoid becoming the next big breach story in the news, you need to rethink security, recognizing that more than the traditional perimeter must be protected and trust — and the credentials that come with it — must be earned.

The Long View

For more than two decades, organizations across North America have been trusting Long View with the expertise to propel their businesses forward, while securing their critical (and valuable) data and assets.

As our name suggests, we "take the long view", building lasting, sustainable solutions that fit precisely fit our clients' needs today and in the future. To meet nuanced industry-specific needs, we've taken a templated approach to implementation based on industry.

And we don't stop at mere implementation. We take an approach to onboarding that allows us to be fast, but also demystifies technology and reduces risks for our customers of all sizes — from SMBs to large enterprises. And it's proven by more than 650 use cases across major national banks, utilities, energy companies that need the most robust and proactive security for identity, access, applications, and data from the data center to their cloud services to the edge.

We know how hard it is to find the talent needed to secure modern IT environments, so we did it for you. We've also sized our team perfectly to provide the top-tier, industry-leading expertise of a large shop with the flexibility, agility and care you get from a small, people-oriented company.

About Long View

Technology is our means, but your empowered workforce is our end. We support the world's dynamic businesses by bringing agility, simplicity and insight to your people, so they can serve your clients. And we can do it because our offices are home to a team of the best and brightest business technologists from across the continent, united by a common mandate -- we're using technology to help the world work.

Learn more

Long View

SOURCES:

[1] Cyber insurance costs up by a third (computerweekly.com)
[2] How To Beat The Cloud Skills Crisis (opsramp.com)
[3] Callback phishing attacks see massive 625% growth since Q1 2021 (bleepingcomputer.com)
[4] Phishing Attacks Growing At Rapid Pace - Patrick Domingues