timus

The $2 Trillion dollar cybersecurity opportunity.

According to McKinsey, the current buyer climate poses a unique moment in time for innovation in the cybersecurity industry. Mckinsey estimates there is a $2 trillion dollar market opportunity waiting to be captured. Vendors who can help underserved segments, improve technology, and reduce the complexity of their solutions are especially well-positioned to reap the rewards in the years ahead. .

In 2021, organizations around the world spent **$150 billion dollars** on cybersecurity. This number is growing by **12.4% annually** and is estimated to only **cover 10%** of the market need, meaning there is a **$2 trillion dollar** market opportunity waiting to be captured.



Source: McKinsey & Company
https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

65%

of executives expect an increase in cybersecurity spending

This trend is supported by a PwC survey who saw 65% of executives expecting to increase their cybersecurity spending in the years ahead.

50%

of executives rank cyber attacks as a catastrophic event

Executives realize the importance of cyber security and the impact a cyber attack could have on their business, so much so that 50% of executives rank cyber attacks as a catastrophic event.

38%

of executives expect more attacks via the cloud.

With the cloud era upon us, 38% of executives expect more attacks via the cloud. This highlights the importance for cybersecurity vendors to cloud-ready solutions.

74%

of breaches include a human element.

74% of all breaches include people being involved either via Error, Privilege Misuse, Use of Stolen Credentials (e.g for VPNs), or Social Engineering.

Source: PwC
https://www.pwc.com/gx/en/issues/cybersecurity.html
Source: Verizon
https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

How can I protect myself against ransomware attacks?

Here are two key steps you can take to protect your organization.

1. Replace your VPN with a Zero Trust solution:

VPNs are subject to credential theft because they tend to give broad access to your network in one swift move. Adopt a Zero Trust Network Access solution like Timus to access data and apps remotely.

2. Augment your hardware-based firewall with an Adaptive Cloud Firewall:

Hardware firewalls were built for a time when data lived inside the walls of the office. Today, apps, data, and people are everywhere. Adaptive cloud firewall solutions like Timus protect company networks and data, no matter where the data lives.



Timus is the network security solution for the cloud era.

Timus helps companies orchestrate secure access while protecting the network against cyberattacks.

Timus combines secure, zero-trust network access with an intelligent cloud firewall that adapts in real time.

Get started in less than 30 minutes
timusnetworks.com