Zero-Trust
Reimagining Security for the Financial Services Industry

Financial executives believe that digital innovations and strategies are key drivers to differentiating customer experience, business performance and growth. Executives attribute 25% growth to digital investments.

Executives see cybersecurity as a key business risk. 67% of executives believe their institutions were effectively managing cybersecurity risk. 50% of executives believe the cost of a breach is going up every year.

For Financial Services (FS) firms the cost and business impact of a breach is consistently higher than other industries.

The real cost of cyber breach per 1K vs 50K vs 100K

The cost of a breach is proportional to the time taken to detect and contain a breach.

Doing more of the same and expecting different results is not a recipe for progress.

Zero-Trust Security is based on the principle that everything has the potential to do harm and handles everything like a potential threat. The Zero-Trust model focuses on reducing the attack surface instead of simply responding to alerts.

BUT what if you could stop attacks BEFORE they have a chance to reach your system.

And surely not success!

Employers report shortage of cybersecurity skills.

7-8 Incidents addressed by average security analyst in a day.

2000 Attacks per min. on each financial services firm.

The real cost of cyber breach per FS firm in 2018

© 2020, Cyberinc.