

# FINANCIAL SERVICES VS. CYBER ATTACKS: A DATA-DRIVEN ANALYSIS



Financial Services Organizations are prime targets for cybercriminals due to the vast amounts of valuable data they handle, including sensitive customer information, financial transactions, and intellectual property. A successful cyber attack can not only result in financial loss but can also damage trust and reputation.

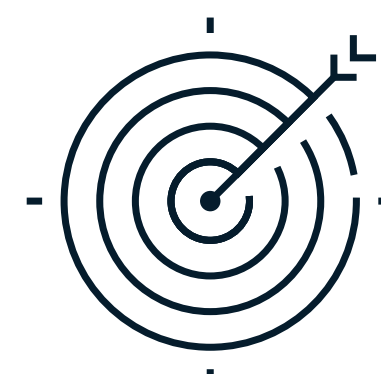


**FINANCIAL SERVICES SPEND MORE THAN ANY OTHER INDUSTRY FIGHTING CYBERATTACKS.**

and for good reason...



**FINANCIAL SERVICES FIRMS ARE AMONG THE TOP 5 INDUSTRIES TARGETED BY CYBER ATTACKS.**



Financial Services Organizations are

**300X**

as likely to experience an attack or breach as other industries.

Financial Services Organizations need to review their risk posture continuously, stay current on new threats and legal requirements, and cultivate a culture of cybersecurity awareness throughout the company. They also need to invest in strong security measures.

By adopting a proactive and comprehensive approach to cybersecurity, Financial Services Organizations can protect their assets, maintain customer trust, and safeguard the stability of the financial ecosystem.

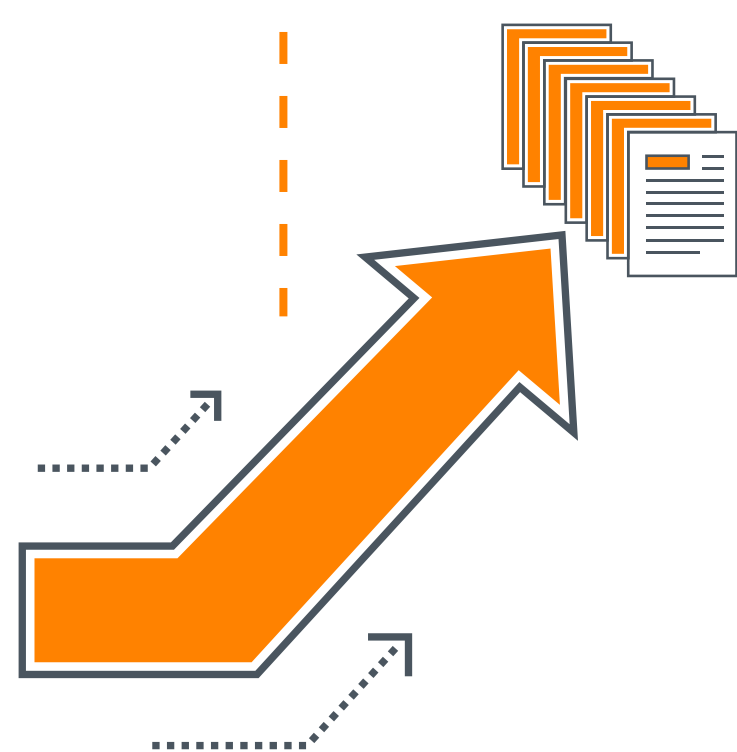


**FINANCIAL FIRMS REPORT 703 CYBERATTACK ATTEMPTS PER WEEK.**

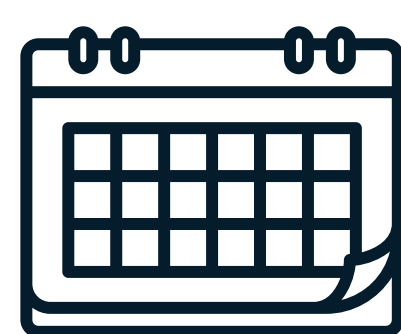


A financial services employee, on average, has access to nearly **11 MILLION FILES** the day they start work.

**DESPITE INVESTMENTS...**



Financial Services Organizations have **449,855 exposed sensitive files** and **36,004 open to everyone in the organization**. This is the highest when comparing industries.



On average, financial services businesses take an average of **233 DAYS TO DETECT** and contain a data breach.



The average data breach cost in financial services is

**\$5.72 MILLION PER INCIDENT.**

**MEANWHILE, THE FINANCIAL INDUSTRY EXPERIENCES THE SECOND-HIGHEST DATA BREACH COSTS.**

## MIXMODE FOR FINANCIAL SERVICES ORGANIZATIONS

The MixMode Platform helps financial services organizations detect and respond to threats in real-time, and at scale, safeguarding their valuable assets and maintaining the trust of their customers.

**The MixMode Platform is the only generative AI cybersecurity solution built on patented Third Wave AI for threat detection and response, delivering:**



**Continuous Monitoring:** Continuously monitors cloud, network, and hybrid environments



**Real-time Detection:** Detects known and unknown attacks, including ransomware in real time.



**Guided Response:** Takes immediate action on detected threats with remediation recommendations.