

# Defending Financial Services from Cyberattacks

Money Matters, Cyber Matters:  
How XTD Protects Financial Services Apps

# Mobile Application Security: An Imperative for Financial Services and How XTD is Making it Easier

Financial institutions are a prime target for cyberattacks. Massive digital transformations of the global financial system and customer demands for ubiquitous transacting create countless vectors for attackers to infiltrate institutional IT environments.

This reality has increased steadily over the last decade. In 2022, more than 60% of global financial institutions with at least \$5 billion in assets were hit by a variety of cyberattacks<sup>1</sup>.

Major attacks are regularly perpetrated by organized crime and state-level actors. For instance, the International Monetary Fund reports that the Carbanak Advanced Persistent Threat (APT) Group stole more than US \$1 billion from financial institutions between 2013 and 2018. They also report that North Korea had stolen at least US \$2 billion from 38 countries as of 2021. But smaller operators are a concern as well. In 2019, a single hacker gained access to the personal information of more than 100 million of Capital One Bank's customers.

Despite investing billions of dollars in cybersecurity measures, financial institutions continue to be vulnerable given multiple threat vectors in a pervasively digitized world.

In 2022, the number of data compromises (breaches, exposure and leakage of private data) in the US financial services industry reached 268, up from 138 in 2020. The financial services sector was the second-most targeted industry by cyber security incidents resulting in data compromise.

Source: Statista

<sup>1</sup> <https://bankingjournal.aba.com/2023/02/larger-financial-institutions-hit-by-variety-of-cyberattacks-in-2022/#:~:text=More%20than%2060%25%20of%20global,new%20survey%20by%20Contrast%20Security>

# Top Cyber Threats to Financial Services

Financial institutions face a growing breadth of cyber risks and threats, like supply chain attacks and negligent or even malicious insiders. Threats have perhaps increased the most due to the pervasive use of mobile banking applications and mobile payments. The numbers are sobering. As just a few examples:

- ▶ IBM's 2022 Cost of a Data Breach Report showed the average cost of a financial services cyber incident at US \$5.97M – up from \$5.72M the year before.
- ▶ The average incident remediation cost in financial services was US\$1.59M, above the global average of US\$1.4M.
- ▶ 60% of financial security leaders saw an increase in island hopping attacks. Application Programming Interface (API) attacks are one of the primary methods for perpetrating island hopping. 94% of institutions experienced an API attack through a financial technology (fintech) application, such as mobile or web apps. Mobile insurtech and cryptocurrency applications are also vulnerable.
- ▶ A whopping 87% said they are concerned about their service providers' security posture. That's especially relevant given major disruptive events like the 2020 SolarWinds supply chain hack.
- ▶ The cost of insider threats to organizations in the financial services industry increased by 47% to \$21.25 million in 2022<sup>2</sup>.
- ▶ 83% of financial services organizations reported having cyber insurance coverage against ransomware, yet this sector has one of the lowest ransom payout rates by insurers: 32% compared to 40% across all sectors

The sensitive information these institutions hold—credit card details, social security numbers, access to funds, credit history, and more—puts the financial sector at greater risk of endpoint attacks than most other industries. This data is a goldmine for cybercriminals. So much so that cybersecurity has become a boardroom-level concern.

All of this underscores the reality that, with the rise of mobile banking, financial institutions need to significantly focus their efforts to safeguard the applications they use and provide to their customers.

<sup>2</sup> <https://www.proofpoint.com/us/blog/insider-threat-management/insider-threats-are-still-rise-2022-ponemon-report>

## 3 Examples of Prevalent Cyberattacks on Financial Apps

**Mobile Screen Overlay:** Attackers trigger an active window over a legitimate mobile app (many banks are being actively targeted on the dark web for this type of threat)

**On-Device Fraud (ODF):** Malware exploits Android's MediaProjection screen-sharing service and Accessibility Service (performs device actions remotely)

**Man in the Middle (MITM) using ARP Poisoning:** Attackers hijack communication flows between an app and an enterprise gateway to intercept/modify communications passing between the app and the server

# Potential Impacts of Cyberattacks on Financial Services Institutions

Most attacks are financially motivated. From virus-infected bots like the [GameOver Zeus Botnet](#) to app-enabled credential theft, there are a breadth of ways for hackers to get actual cash. For example, ransomware has flourished since 2020. A full 74% of financial security leaders experienced one or more ransomware attacks in 2021, and 63% of them paid the ransom<sup>3</sup>. There is another huge penalty for covering losses for fraudulent use of bank customers' credit or debit cards. Organized crime excels at perpetrating these types of attacks on a large scale.



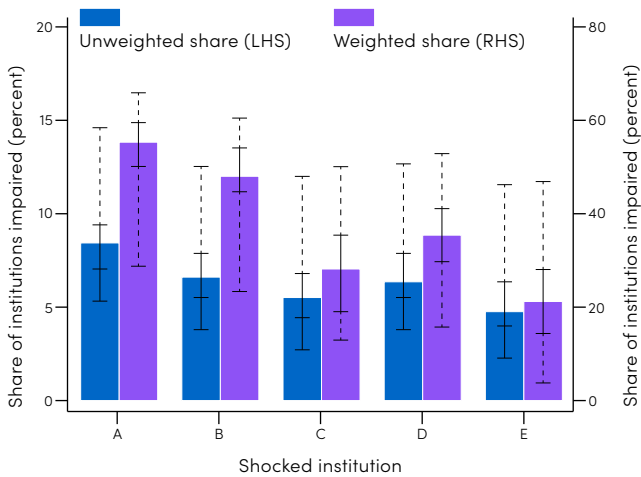
Other attacks are intended to be destructive to critical infrastructure or have systemic effects. One of those could be a shock to the financial system. The interconnectedness of so many financial institutions means that a cyber incident at even one firm could have a domino effect on others. Just a single attack could disrupt a bank's ability to send payments, which could then impact other banks' cash flow and operations. Or, an attack on a market exchange could disrupt trading, such as what happened to the New Zealand Stock Exchange in 2020 when trading in cash, debt, and derivatives had to be stopped for four days.

A cyberattack affecting multiple large financial institutions could even lead to a broad loss of confidence in the security of the entire financial sector. These examples from the Federal Reserve Bank of New York illustrate some potential impacts from a shock-level compromise of a major US financial institution and financial third-party cyber vulnerabilities<sup>4</sup>.

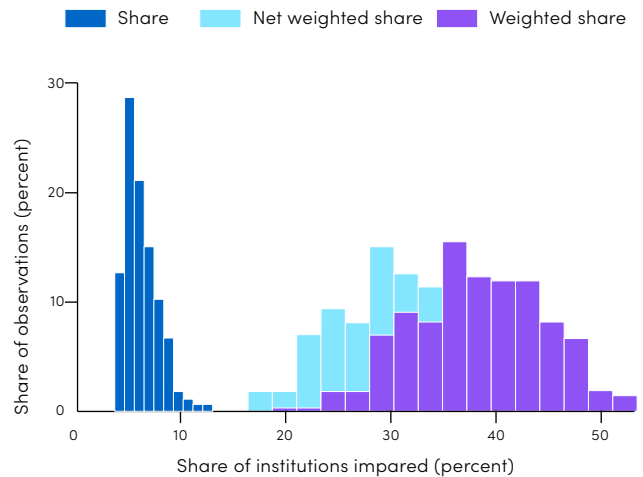
<sup>3</sup> <https://news.vmware.com/security/modern-bank-heists-5-0-the-escalation-from-dwell-to-destruction>

<sup>4</sup> [https://www.newyorkfed.org/medialibrary/media/research/staf\\_reports/sr909.pdf](https://www.newyorkfed.org/medialibrary/media/research/staf_reports/sr909.pdf)





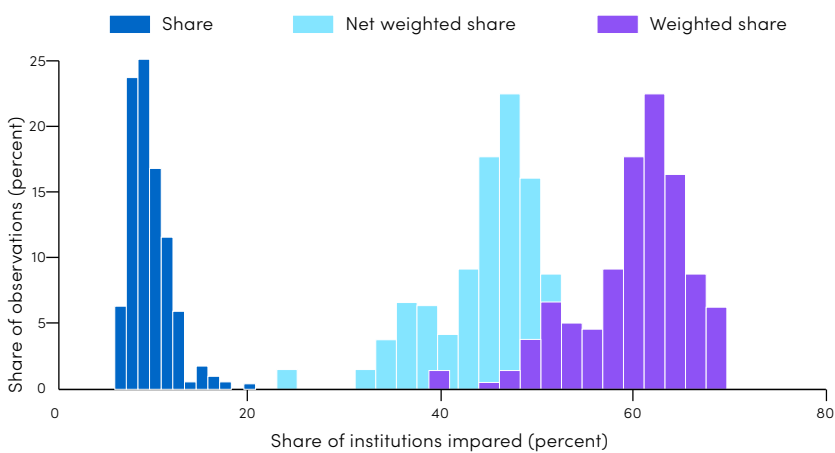
(a) Distribution across the top-5 institutions



(b) Distribution across days

### Impact of a shock to a top-5 institution

The figure shows the distribution of the unweighted share (blue), share weighted by assets (red) and net weighted share (grey) of institutions impaired by a shock to each of the top-5 institutions. Panel (a) shows the distribution across the top-5, averaged across days; bars represent the average impact; solid whiskers represent the p25/p75 range; dashed whiskers the p1/p99 range. Panel (b) shows the distribution across days, averaged across the top-5 institutions. Net weighted share excludes the shocked institution.



### Cyber vulnerability through a third-party service provider


The figure shows the distribution of the network impact for the scenario with a disruption origination from a third-party service provider. "Share" represents the unweighted percent of institutions that become impaired. "Weighted share" represents the percent of institutions that become impaired, weighted by asset size. "Net weighted share" refers to the percent of institutions that become impaired, net of the shocked institutions.



# Growing Cyber Regulations Pressure the Financial Services Industry

In light of the major threats facing the financial sector, it is one of the few industries where cybersecurity is required thanks to legislation.

For instance, as of May 2022, the US Federal Reserve requires that financial institutions disclose cyber incidents to regulators within 36 hours of an incident if it could impact the US banking system. The New York State Department of Financial Services has published the NYCRR 500 Cybersecurity Requirements Regulation for Financial Services Companies Part 500, requiring financial services institutions—including agencies and branches of non-US banks licensed in the state of New York—to assess their cybersecurity risk profile. In fact, 24 US states have passed cybersecurity bills or resolutions. In Europe, financial services firms (as well as all organizations) are subject to the strict terms of the General Data Protection Regulation (GDPR).



**US Federal Reserve requires that financial institutions disclose cyber incidents to regulators within 36 hours of an incident if it could impact the US banking system.**

Government entities are also issuing formal, detailed guidance on structured ways to protect institutions from cyber threats. There is [interpretive cybersecurity guidance](#) from the US Securities and Exchange Commission (SEC), the NIST Cybersecurity Practice Guides [SP 1800-5](#), [SP 1800-9](#), and [SP 1800-18](#), and a new section for financial crimes under the Financial Industry Regulatory Authority (FINRA) [cybersecurity and technology governance](#) policies. While compliance with all of this guidance is voluntary, the attention paid to the problem means that institutions cannot credibly feign ignorance (and therefore lack of liability) when addressing proper cybersecurity protections.

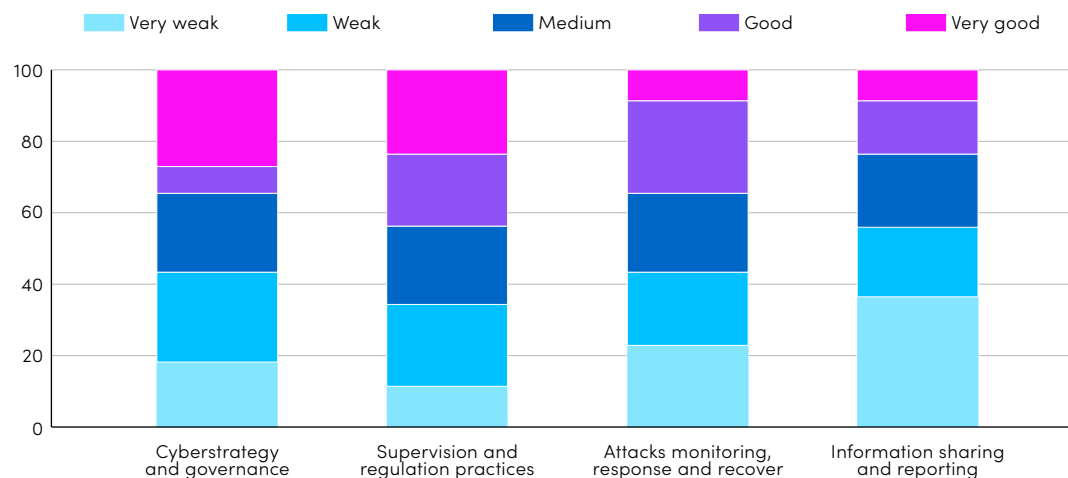
Conversely, a recent [International Monetary Fund \(IMF\) survey of 51 countries](#) revealed that in emerging and developing economies, cyber regulations are seriously lacking.



As institutions in these economies become more integrated into global financial networks, the risks of systemic shocks significantly increase.

### Cyber gaps



Weak defenses against attacks put the financial sector at risk, but collective action could help thwart these costly threats.



Source: IMF staff survey, state of play at supervisory authorities.

# FINRA Cybersecurity-Related Considerations

FINRA offers extensive [guidance](#) for assessing a firm's cybersecurity readiness. Here are a few examples of probing questions to facilitate self-assessment:

 <p><b>What</b> steps has your firm taken to prevent a cybersecurity intrusion, such as a ransomware attack? In the event your firm experiences an intrusion, how will it restore critical data from backups, as well as identify and recover customer information that was exfiltrated?</p>	 <p><b>How</b> does your firm protect sensitive customer information or confidential firm data from being exposed to, or copied by, unauthorized individuals or threat actors, including blocking unauthorized copying and monitoring sensitive data in outbound emails?</p>	 <p><b>How</b> does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives? How does your firm address imposter websites once they are identified?</p>
 <p><b>What</b> process has your firm established to assess the risks associated with third-party vendors during the initial onboarding and on a regular basis thereafter? In the event there is a report of a security breach at a vendor, can your firm identify all components and services third parties provide?</p>	 <p><b>What</b> steps does your firm take to ensure only authorized employees, customers or contractors receive authenticated access to firm systems, such as account management, trading and email?</p>	 <p><b>How</b> does your firm verify the identity of an individual when creating a new account or accessing an existing account?</p>
 <p><b>What</b> kind of security training does your firm conduct, such as email best practices and phishing? Does your firm provide training to all staff, and not just to registered persons?</p>	 <p><b>What</b> are your firm's procedures to communicate cyber events to anti-money laundering (AML) or compliance staff related to meeting regulatory obligations, such as filing of security assessment reports (SARs) and reviewing potentially impacted customer accounts?</p>	 <p><b>Does</b> your firm maintain an Incident Response Plan (IRP) that includes guidance, or playbooks, for common cybersecurity incidents (e.g., data breaches, ransomware infections, account takeovers)?</p>






# The Value of Extended Threat Defense Technology in Combatting Cyberattacks

The multitude of cyber-related challenges facing financial institutions demands an elevated level of security to address the greatly increased risks in the modern environment of ubiquitous transacting. The current reality is that most mobile applications used by banks, fintechs, and others are not well-protected. Since it's becoming more and more difficult for hackers to bypass enterprise-level security solutions deployed by financial organizations, bad actors look for alternative entry vectors and discover the app path.

Extended Threat Defense (XTD) is the leading cybersecurity solution that secures financial services institutions from risks originating from mobile applications to the edge. While many institutions have some form of cybersecurity protection for employer-issued managed devices and personal "bring your own devices" (BYOD), XTD addresses multi-vector threats stemming from unmanaged (consumer) mobile devices like smartphones and tablets.


That specifically includes the range of multi-vector threats that previous cybersecurity solutions like mobile threat defense (MTD) and extended threat detection and response (EDR) miss.

 <b>MTD</b>	 <b>XDR</b>	 <b>XTD</b>
<p>Provides real-time protection against threats and allows organizations to remotely manage and secure their mobile devices.</p>	<p>Provides continuous monitoring of endpoint devices and can detect and respond to a wide range of security threats, including malware, ransomware, and advanced persistent threats.</p>	<p>Helps prevent, detect, respond to and predict cyberattacks originating from the mobile app to the edge, and specifically multi-vector threats</p>
<p>Works on managed smart phones, laptops and tablets</p>	<p>Works on managed endpoint devices</p>	<p>Works on unmanaged devices; any device with an app</p>
<p>Requires an agent to be installed on the device – protects institution employees' mobile devices, but impractical for end customers</p>	<p>May take a more comprehensive security approach (continuous monitoring, incident response, and the ability to identify and remediate vulnerabilities). Lacks integration, limiting visibility into the security posture and slowing response.</p>	<p>Uses behavioral analysis like EDR (for detection), combined with other EDR and MTD elements. Ideal when numerous unmanaged consumer devices are connected to a financial services enterprise via the app</p>

XTD monitors new entry vectors from the fastest-growing attack surface—connected apps, APIs, and unmanaged devices. That makes XTD an essential component of effective cyber defenses for financial institutions.

# Polymorphic Protection: An Important App Security Attribute

An effective XTD platform should include polymorphic protective capabilities. This innovative approach involves constantly changing an application's code and structure to make it more challenging to hack. It's a bit like changing the password of your online accounts every so often to reduce your cyber vulnerability. Some savvy financial firms are already protecting their mobile apps with polymorphic protection.



**Code polymorphism leads to a different result on each compilation, even though the source code did not change. This type of protection makes it difficult for attackers to use information they gathered through experience, forcing them to begin from scratch for every build.**

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. Given the financial sector's particular vulnerability to cyberattacks, this approach is crucial for protecting customer information.

To implement polymorphic protection, financial institutions must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.

# The Verimatrix XTD Approach

Verimatrix XTD offers an affordable and user-friendly solution that utilizes cutting-edge technology to secure mobile apps. With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage. Our military-grade, multi-layered security is very difficult for hackers to penetrate. We also help customers monitor the fastest-growing attack surface: consumer endpoints. By analyzing extensive data, Verimatrix XTD can predict future attacks and provide proactive protection.

## Covering a Wider Attack Surface with Zero-Code Protection

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed to market a reality. This is especially valuable for the mobile transaction environment, where consumer devices with various levels of protection are always in play.

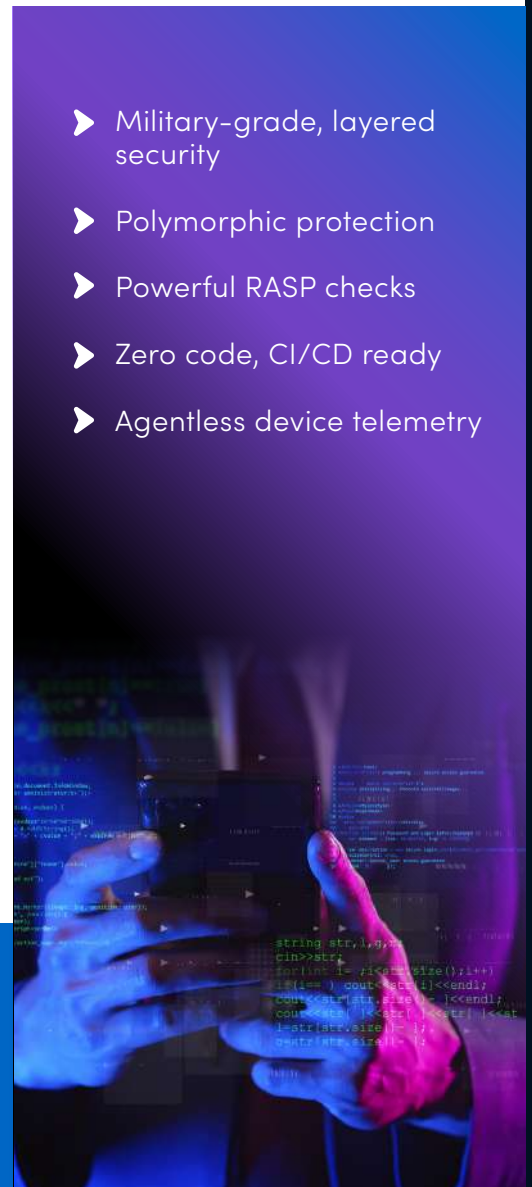
## Addressing Multi-Vector Threats from Consumer Devices

Verimatrix XTD monitors and mitigates cyber threats originating from apps downloaded to unmanaged consumer devices. While many organizations implement cybersecurity measures for managed devices such as BYOD, Verimatrix XTD is one of the few solutions designed to address the multi-vector threats arising from unmanaged mobile devices. XTD can do this because its telemetry is built into its app protection and is automatically passed on to every app instance downloaded. That means any device using the app can be monitored, effectively expanding the coverage of the attack surface into new realms. With Verimatrix XTD, financial institutions can secure a broader range of devices, providing comprehensive protection against potential threats.

## Detecting and Responding to Active Attacks

Verimatrix XTD's proactive defense strategy involves the swift detection of active attacks and an immediate response to neutralize potential damage. By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly. This decisive action safeguards sensitive data and prevents malicious actors from exploiting vulnerabilities.

- ▶ Military-grade, layered security
- ▶ Polymorphic protection
- ▶ Powerful RASP checks
- ▶ Zero code, CI/CD ready
- ▶ Agentless device telemetry



## **Proactive Protection through Predictive Analytics**

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur. This proactive approach empowers financial services institutions to stay one step ahead of attackers, ensuring enhanced security for their mobile applications and connected infrastructure.

## **Understanding Risks and Empowering Security Professionals**

Verimatrix XTD is dedicated to helping security professionals comprehend the risks associated with mobile applications and their connections. Highlighting the existence of blind spots by assigning a risk score to every threat found, Verimatrix XTD prompts financial institutions to acknowledge and address potential vulnerabilities. XTD provides security professionals with a meticulously designed Software-as-a-Service (SaaS) offering. There is also an optional service incorporating the services of human data scientists to review your account and take response actions on your behalf, adding an extra layer of expert assistance to combat evolving app threats effectively.



**Verimatrix XTD Cybersecurity Expert Service extends your security team. Our experienced security professionals provide monitoring reports, risk assessments, and expert guidance to equip your SOC teams with the insights they need to take action.**



# Fight Back with Verimatrix XTD!

As the reliance on mobile applications grows in the financial services sector, so does the need for robust cybersecurity measures. Verimatrix XTD is an exceptional solution, providing affordable and user-friendly mobile app protection. With its agentless, zero-code approach, it allows for easy and painless deployment, allowing customers to monitor a wider attack surface, including unmanaged consumer devices.

Verimatrix XTD effectively detects active attacks and responds promptly, minimizing the potential for damage. By analyzing data and predicting attacks, it enables organizations to proactively protect their mobile applications. Armed with Verimatrix XTD's comprehensive security offerings and expert support, security professionals can effectively mitigate the risks associated with financial app vulnerabilities and secure their digital assets

## Verimatrix — Award-winning Cybersecurity

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered, and frictionless security. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world.

We are proud of the market recognition our innovative solutions have earned:



2023 Global Infosec Award for Hot Company in Mobile App Security – Cyber Defense Magazine



2023 Cybersecurity Excellence Awards – Gold Winner for Artificial Intelligence Security and Biggest Brand Growth



2023 Product of the Year, AI and Machine Learning – National Association of Broadcasters (NAB)



2022 Gartner® Hype Cycle™ for Application Security

[Get A Demo](#) of the Verimatrix XTD cloud-native platform, deployed in minutes to protect your apps!

## Sources

- ▶ <https://www.varonis.com/blog/cybersecurity-statistics>
- ▶ <https://news.sophos.com/en-us/2022/08/10/the-state-of-ransomware-in-financial-services-2022/>
- ▶ <https://www.darkreading.com/risk/cyberthreats-regulations-mount-for-financial-industry>
- ▶ <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20211118a.htm>
- ▶ <https://kirkpatrickprice.com/blog/top-4-cybersecurity-challenges-facing-the-financial-services-industry/#:~:text=Malicious%20hackers%20often%20have%20one,sensitive%20data%20for%20financial%20gain.&text=Because%20the%20financial%20services%20industry,challenges%20they're%20up%20against>
- ▶ <https://www.finra.org/rules-guidance/guidance/reports/2023-finras-examination-and-risk-monitoring-program>
- ▶ <https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards>
- ▶ <https://www.rapid7.com/fundamentals/nydfs-cybersecurity-regulation/#:~:text=Digital%20Risk%20Protection-,What%20is%20the%20NYDFS%20Cybersecurity%20Regulation%3F,assess%20their%20cybersecurity%20risk%20profile.>