BlackFog in Banking and Finance

BLACKFOG™

3.9m
Average cost of a data breach

983
Average number of bank attacks per day

300x
More likely to be attacked than other industries

Cybercriminals are increasingly targeting the financial industry

Cybercrime is a lucrative business and the financial industry is under relentless attack from hackers. Cybersecurity attacks continue to grow in both sophistication and frequency as financial services firms become increasingly reliant on customer data and technology to run their businesses. Staying one step ahead of cyber criminals is critical.

Ransomware remains the tactic of choice

With more than 90% of financial institutions targeted by a ransomware attack in 2017, it's clear that ransomware is still the tactic of choice for cybercriminals. With financial gain being the primary motivation for cybercriminals, it's not surprising that banks and other financial services organizations are a regular target.

Cybersecurity challenges in financial services

- Banks remain a top target for ransomware and malware. Verizon reported that 76% of all data breaches in 2017 were financially motivated.
- Customers are reliant on electronic banking to complete transactions so financial institutions have developed more mobile apps and web portals. This has increased their exposure and risk to cyberattack.
- Mobile banking threats include mobile malware, third-party apps, unsecured Wi-Fi networks, and risky consumer behaviour.
- The financial institution owns the risk, whether or not the institution uses a proprietary or third-party mobile banking application.
- Security breaches can lead to lost revenue, reputational damage, regulatory fines and interruption to operations.
- Maintaining GDPR compliance and mitigating the risk of regulatory fines.

Cybersecurity in the Financial Sector

Banks are attacked **983x** per day

48% of incidents involved a malicious or criminal attack

Average cost of a data breach is **3.86 M** (increase of 6.4%) Ponemon Cost of a data breach report 2018

Financial Organizations fall victim to cyber security attacks **300x** more frequently than other industries

90% of all financial institutions have experienced ransomware in the past year

Average cost per record from a malicious attack is **$157**

The financial services industry takes in the highest cost from cyber-crime at an average of **$18M**

76% of all data breaches in 2018 were financially motivated

Data breaches reported by UK financial services firms to the Financial Conduct Authority (FCA) increased **480%** in 2018

Ransomware growing by **350%** Annually

92% of malware delivered by email

Cybercriminals are Following the Money

BLACKFOG

www.blackfog.com

Sources:

- Positive Technologies
- GeneraliGlobalAssistance-IDP.com
- Accenture
- Ponemon Institute
- RPC
- Betanews.com
- Verizon
- Cisco

So, how do banking/security leaders mitigate the risk?

Lots of cyber security solutions can tell you when a breach or attack has taken place and data has been lost. BlackFog stops it from happening in the first place.

BlackFog fills the gap between security solutions that focus on preventing access through intrusion detection systems, such as Firewalls and Anti-Virus/ Malware solutions that remove known infections after they have been discovered. Consisting of 12 layers of defense, BlackFog protects against ransomware, spyware, malware, phishing, unauthorized data collection and profiling.

Prevention is the best form of defense

Cyberattacks and data breaches are inevitable, and hackers will find their way in, but with a preventative approach to cybersecurity these threats can be eliminated before the damage is done. Gartner estimates that companies globally could incur $5.2 trillion in additional costs and lost revenue over the next five years due to cyberattacks, so all businesses, particularly those in the financial sector simply must prioritize cyber defense.

> 'It's inevitable that attackers will find their way in, so we spot, in real-time when an attacker has infiltrated your system and is trying to remove unauthorized data from your device and shut them down before they get the chance to.'

Benefits for financial services

- Prevents cyberattacks before they happen
- Data protection
- GDPR / regulatory compliance
- Privacy
- Cyberattack prevention
- Data breach protection

BlackFog prevents

- Data leaks
- Ransomware
- Hacking
- Identity theft
- Dark Web
- Data profiling
- Phishing

About BlackFog

Founded in 2015, BlackFog was born to combat the growing number of online threats targeting your personal and corporate data. Hackers will get into your network; BlackFog stops them getting out. Through a layered approach to security, BlackFog stops attacks in real-time and prevents the unauthorized removal of data from your device.

Consisting of multiple layers of defense against ransomware, spyware, malware, phishing, unauthorized data collection and profiling, BlackFog blocks over 24 million threats across mobile and desktop endpoints around the world, protecting organizations' data and privacy, and strengthening their GDPR compliance.