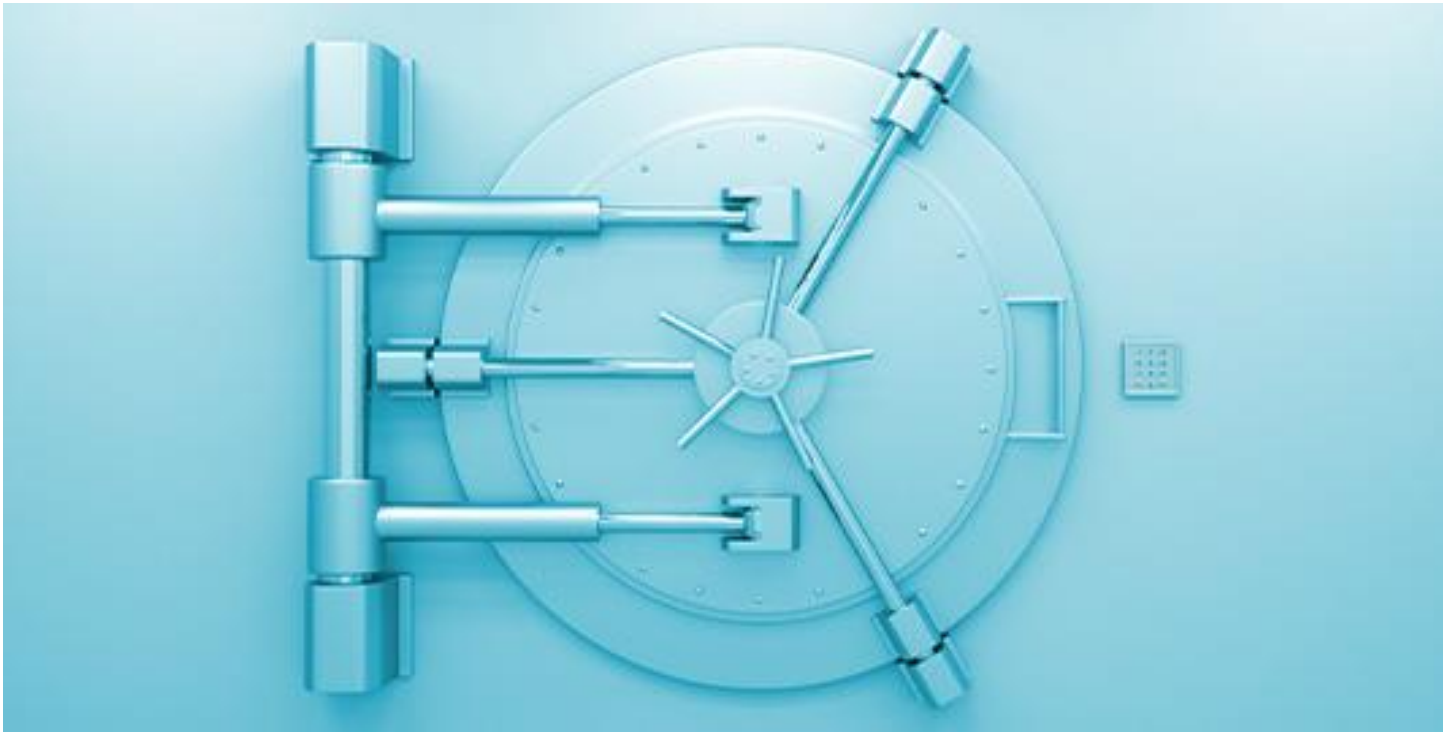
AGILEBLUE

Automation. Visibility. Confidence.

Financial Services

Whitepaper



AgileBlue, 2021

Overview

Information technology (IT) teams at financial institutions such as regional banks, mortgage lenders, credit unions and investment advisory firms are stretched thin. They're expected to meet compliance obligations while simultaneously taking care of cyberthreats. This is particularly true for midsized institutions without resources dedicated to security or compliance, putting them at great risk.

What options do Financial Firms have? The emerging area of SOC-as-a-Service offers financial institutions the opportunity to augment their existing IT staffs and improve their security postures while at the same time simplifying compliance.

This expectation applies to all firms. It includes all aspects of how they store and handle highly confidential information, such as intellectual property, competitive company secrets, financial and payment data, personal client data, etc.

At a Glance: Verizon report – NAICS 52 (2021 Study)

- The US Department of Treasury's Financial Crimes Enforcement Network reports that on average, more than $1 billion is stolen from institutions each month.
- The average cost to remediate a data breach, in the financial sector, is 23% higher than other industries.
- Financial institutions reduced IT personnel by more than 33% in 2021.
- Miscellaneous Errors, Basic Web Application Attacks, and Social Engineering represent 81% of breaches.
- Threat Actors: External (56%), Internal (44%), Multiple (1%), Partner (1%) of breaches in financial services.
- Of the data compromised, 83% was personal information.
- In 2021, 44% of breaches derive from internal actors.

Meeting these diverse cybersecurity requirements is a challenge, and financial firms unable to demonstrate the capabilities of a security operations center (SOC) put their business in jeopardy. Cybercriminals are now capable of exploiting weaknesses at previously unseen speed and scale by rapidly acquiring new cyber weapons and continuously modifying their attack techniques. As threat actors continue to adapt and evolve, paying attention to cybersecurity strategy is paramount to financial firms regardless of size, discipline, or geography.

Beating Hackers and Keeping Regulators Happy

The financial industry has significantly benefited from digital transformation. Paper-based records and communications have long been replaced by email, video conferencing, cloud, API's, VoIP, cloud-based software-as-a-service (SaaS) solutions, and more. Unfortunately, these improvements in operational efficiency also come with increased risks. While financial institutions have been relatively quick to adopt and deploy promising digital technologies, they have yet to appropriately address the related security concerns.

Regional banks, credit unions, mortgage lenders and other mid-size financial institutions can face regulations from both national and state regulatory bodies. Governance, risk management and compliance frameworks, and security guidance developed by NIST, PCI DSS, the FFIEC and state bodies, such as the New York Department of Financial Services and California CPA, all strive to assess risk and minimize security gaps. While such oversight provides useful recommendations for cyber risk management, applying and optimizing a cybersecurity strategy can overwhelm capable but short-handed IT and security staffs.

The [AgileBlue] SOC-as-a service helps financial institutions meet elements of a variety of compliance mandates, including:

- FFIEC/ NCUA guidance
- The New York State Department of Financial Services NYCRR 500
- PCI DSS
- GLBA
- SOX

Not observing compliance mandates can prove costly, and not just from a monetary standpoint. Companies guilty of non-compliance end up spending more in the long run on fines and new resources needed to manage increased regulatory audit scrutiny. They also must endure negative media coverage resulting in customer churn when something goes wrong.

Dangers of Cyberthreats

Extremely sensitive and valuable data resides in the financial services sector—everything from personally identifiable information (PII), to check routing data, to global stock and investment algorithms. The loss of this data and intellectual property has a major impact on a company's brand reputation and customer loyalty. When consumers and business customers place their trust and their money in an institution, its reputation for information security is paramount.

Infrastructure at financial institutions is constantly evolving to support line-of business initiatives. While traditionally this has focused on on-premises assets, cloud services in the form of software-as-a-service (SaaS) and infrastructure-as-a service (IaaS) are becoming more commonplace as cloud providers address the security and compliance concerns of financial institutions. Still, the addition of cloud services increases a financial institution's "attack surface" and adds to their cybersecurity risk equation.
Challenges with Cyber Skills and "Always-On" Monitoring

Gartner found that, "Despite 95 percent of CIOs expecting cyberthreats to increase over the next three years, only 65 percent of their organizations currently have a cybersecurity expert." The shortage of people with security expertise is particularly acute in the financial services industry.

Financial services firms are enhancing their on-premises infrastructure while also embracing the benefits of cloud computing. Such hybrid environments, where information resides both on-premises and in the cloud, require increasing technological sophistication and knowledge to secure.

Lack of 24/7 Coverage

Continuous monitoring is a security best practice and frequent compliance requirement for financial institutions. Such security monitoring demands building and maintaining a security operations center (SOC). A SOC is a combination of cybersecurity personnel, threat detection and incident response processes, as well as supporting security technologies that comprise an organization's security operations. A SOC combines the people, processes, and technology needed to elevate and maintain an institution's security posture.

While a SOC is an industry best practice, smaller financial institutions typically do not have the budget for one. A Gartner report on security for midsized enterprises commented that, "A minimum of eight to 12 security analysts are needed for 24/7 monitoring—an unrealistic objective for most [midsized enterprises]." Justifying the budget to hire a SOC team poses a challenge even for the most persuasive CIO or CISO.

And locating, training, and retaining the necessary security talent is a huge task for small and mid-sized financial institutions. Outsourcing the SOC function, however, provides a viable solution. SOC-as-a-service offerings, like the AgileBlue CyberSOC enables companies to overcome the cybersecurity skills shortage and avoid the costs and difficulties that come with building, deploying, and maintaining an in-house SOC.

AgileBlue's CyberSOC, SOC-as-a-service, delivers the following capabilities at a simple and predictable monthly pricing model- essentially enabling smaller financials to take advantage of security operations. Included are:

- Fully managed, cloudbased SIEM
- Machine Learning Engine
- External threat intelligence
- 24x7 monitoring and alerting
- Compliance reporting
- Cloud monitoring–AWS, Azure, Google Cloud
- Periodic external vulnerability scans

Targeted Attacks on Financial Institutions

While financial institutions of all sizes must comply with federal and state regulations that govern the industry, they face even greater risks and challenges from today's cyberthreats. A single data breach can cause irreparable harm to a firm, including damages that can never be overcome.

Cybercriminals continue to devise new attack methods, here are the top four methods of cyberattacks that banking and financial institutions have recently suffered:

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Firms may install AV or endpoint protection platform (EPP) solutions on employee endpoints, real time threat intelligence, or custom threat detection logic, but without having an expert team to carefully analyze alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls.

Phishing attacks seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such

as a website for a bank, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, firms without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed SaaS applications are left vulnerable.

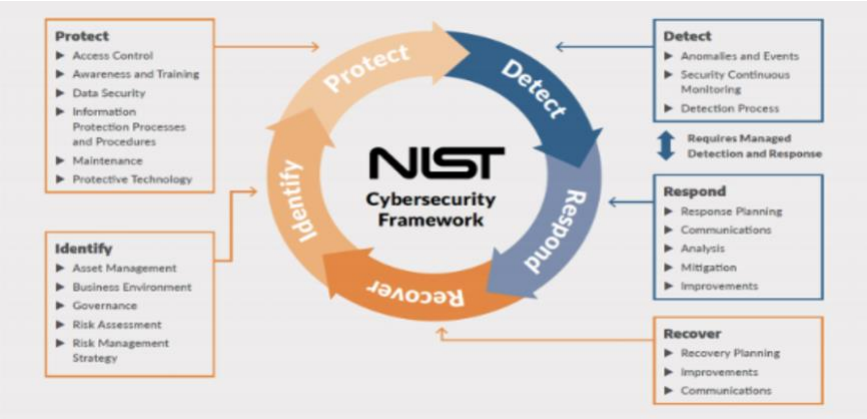
Brute-force login attacks involve threat actors systematically attempting password or passphrase combinations until finding correct combinations and accessing restricted resources protected by passwords. In-depth analysis of Active Directory logs and SaaS application login activity are the primary methods used to detect such attacks. Unfortunately, working with authentication data logs is complex and may require analyzing terabytes of data.

Attacks on unpatched servers and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, financial firms access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities.

Detecting patterns of anomalous activity and potential compromise requires the deep analysis of several critical log sources, including:

- Firewalls
- IDS/IPS
- Endpoint security (AV)
- Active Directory
- Email security gateways
- SaaS applications
- Cloud workloads

NIST Cybersecurity Framework and Managing Risk



A new approach for a secure future: adopting SOC-as-a-Service

A SOC-as-a-service enables banks and financial firms to address the security gaps that result in the cyberattacks from going undetected. Using a managed SOC service gives firms complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access to regular vulnerability assessments and enables firms to establish a detailed and customized incident response plan.

Financial services firms, particularly retail financial firms like regional banks, mortgage lenders and credit unions, are stretched thin as they manage cybersecurity risk and seek to maintain compliance in the face of budget constraints and a cybersecurity skills shortage. The maturing of managed detection and response offerings provides a way forward to solving both issues. SOC-as-a-Service offerings like AgileBlue's CyberSOC offer financial institutions the ability to improve their ability to monitor, detect, and respond to cybersecurity threats while meeting their regulatory obligations around mitigating cybersecurity risk and ensuring resilience.

About AgileBlue

AgileBlue is a managed breach detection company with an Autonomous SOC-as-a-Service for 24x7 monitoring, detection and guided response for cloud, digital infrastructures, and applications. AgileBlue provides their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. The company offers a proprietary risk scoring algorithm including industry comparisons and risk analysis trends. AgileBlue's Silencer technology significantly reduces false positives with a 95% confidence score on incident alerts based on their proprietary machine learning and user behavior analytics.

Ready to protect your company? Contact Us.