cloudcover®

Data Security Made Possible for Mid-sized Midwest Bank

CloudCover's CC/B1 Platform™ creates 100% protection from ransomware and blocks over 11,000 viruses and threats in a two-week period

High costs, disruption to business, and reputational damage all effects of financial industry cyberattacks

Banks, credit unions and other financial services companies have long been prime targets for cyberattacks for a simple reason: Where there's money, there's money to be made. For this reason, banking institutions are 300 times more at risk for data security threats than any other industry (Eisenbach, Kovner, and Lee, 2021).

The continued digitization of financial services and the migration to the cloud has caused these threats to increase substantially. According to the ID Theft Resource Center, 12,250 data breaches have been recorded over a 16-year period — from 2005 to 2020 — with half of those occurring within the last five years (Eisenbach, Kovner, and Lee, 2021). And, since the beginning of the COVID-19 pandemic, phishing attacks in particular have increased by over 400% in the banking industry (Knudson, 2021).

While the financial sector has the shortest average timespan of breaches, the breaches also take longer for companies to identify — an average of over six months (Eisenbach, Kovner, and Lee, 2021) — and they're more costly. The cost of cyberattacks is the highest in the banking industry, where the average annualized cost has reached $18.3 million (Dautovic, 2021).

Hand-in-hand with the financial loss is the disruption to business. A data breach impacts the availability of services to a bank's consumers, and it also compromises the integrity and legitimacy of the systems currently in place, as customer account balances or proprietary records can be impaired or exposed. In addition, it can hamper the ability of the bank to service its running creditors.

Then, there's the long-term reputational damage. A 2019 ReputationUs survey says that 84% of consumers trust banks and credit unions over any other industry to protect their personally identifiable information — which means that if a cyberattack is mishandled, these same organizations may face a significant loss of customers ("Study reveals impact of cyberattacks on consumer confidence, corporate reputation," 2019).

> **At a congressional hearing in May 2021, the chief executives of Wall Street's six largest banks were asked to name the greatest threat to their companies and the wider financial system. At the top of the list — above the COVID-19 pandemic, climate change, or the same factors that contributed to the 2008 financial crisis — they answered, "Cybersecurity." (Zetter, 2021)**

The challenge

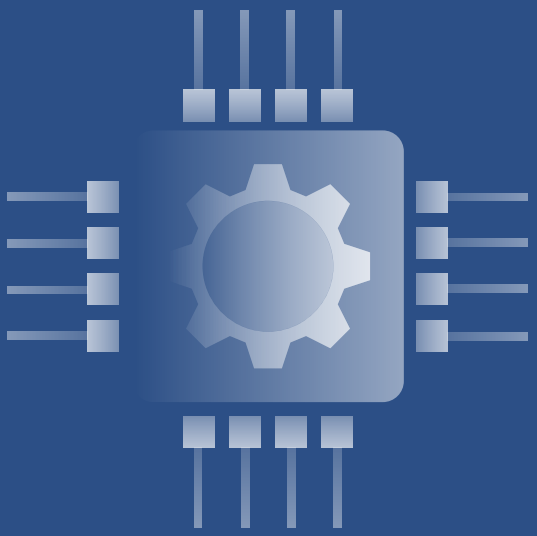
Mid-sized Midwest bank looks to implement comprehensive network security while dealing with lack of staff and budget

Why have cyberattacks increased in the banking industry? There are several related factors:

- **Accelerated transition to digital banking:** As a result of the COVID-19 pandemic, many financial institutions and their consumers had to become comfortable with digital banking very quickly. Some of these customers are not digital natives and therefore aren't familiar with security best practices.
- **Increased sophistication and volume of hacks:** An increase in users — and in new banking technologies — means the number of potential targets and entry points have also increased.
- **Additional third-party risks:** Most financial services providers have a breadth of technology partners, and there's no telling when a third party will have a fourth-party vendor with less-than-ideal security protocols.

Because of these factors, many banks and other financial entities have placed an even higher priority on the security of their administration networks in an effort to further protect a consumer's personally identifiable information. According to the 2020 Deloitte Center for Financial Services Global Outlook Survey, 71% of bank leaders expect their organizations to increase cybersecurity spending — with cloud computing/storage and data privacy being the high-priority areas (Holzhauer, 2021).

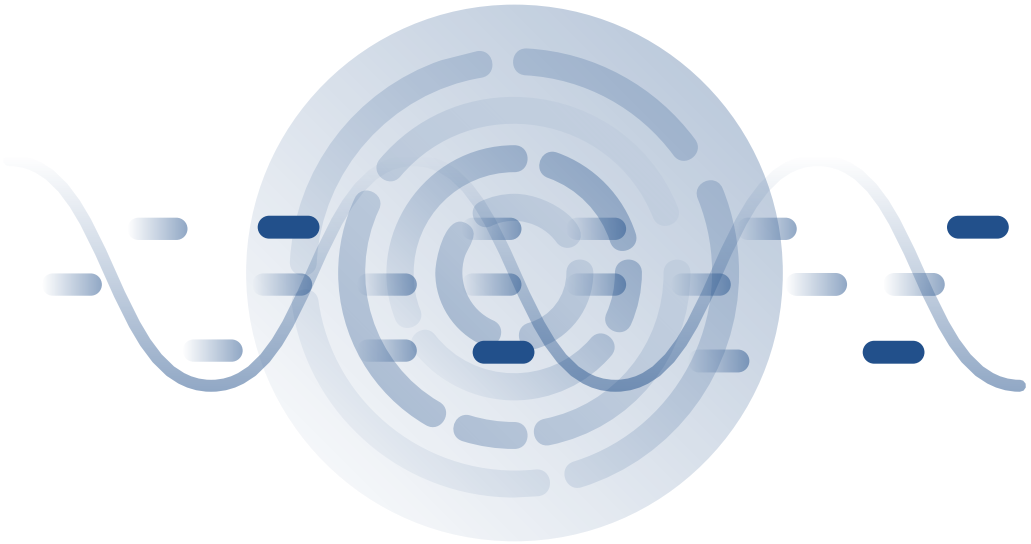
Even before COVID-19, a comprehensive network security strategy was the goal of a mid-sized bank in Minnesota. The bank viewed cybersecurity as a critical element of its network operations, but with a limited IT staff and budget, a proactive approach just wasn't possible. The bank's approach had been a hodgepodge of disparate platforms and systems — firewalls installed to remedy major threats, with a desktop anti-spam program as a sidebar. This isn't an unusual network security method — it's actually common practice, as many organizations don't always understand the extent of their vulnerability or that they might have already been targeted by attackers.



The solution

Automated security without the need for additional staff with CloudCover's CyberSafety CC/B1 Platform™

The bank's staff and budget constraints were a challenge, and hiring consultants that required full-time managed security wasn't an option. To prove the effectiveness of a comprehensive network security approach, CloudCover® approached the bank with an offer to install their CyberSafety CC/B1 Platform™. The goal was to protect the bank's network, log the security events that were taking place, and provide reporting to the IT team on what type of traffic the bank was receiving.

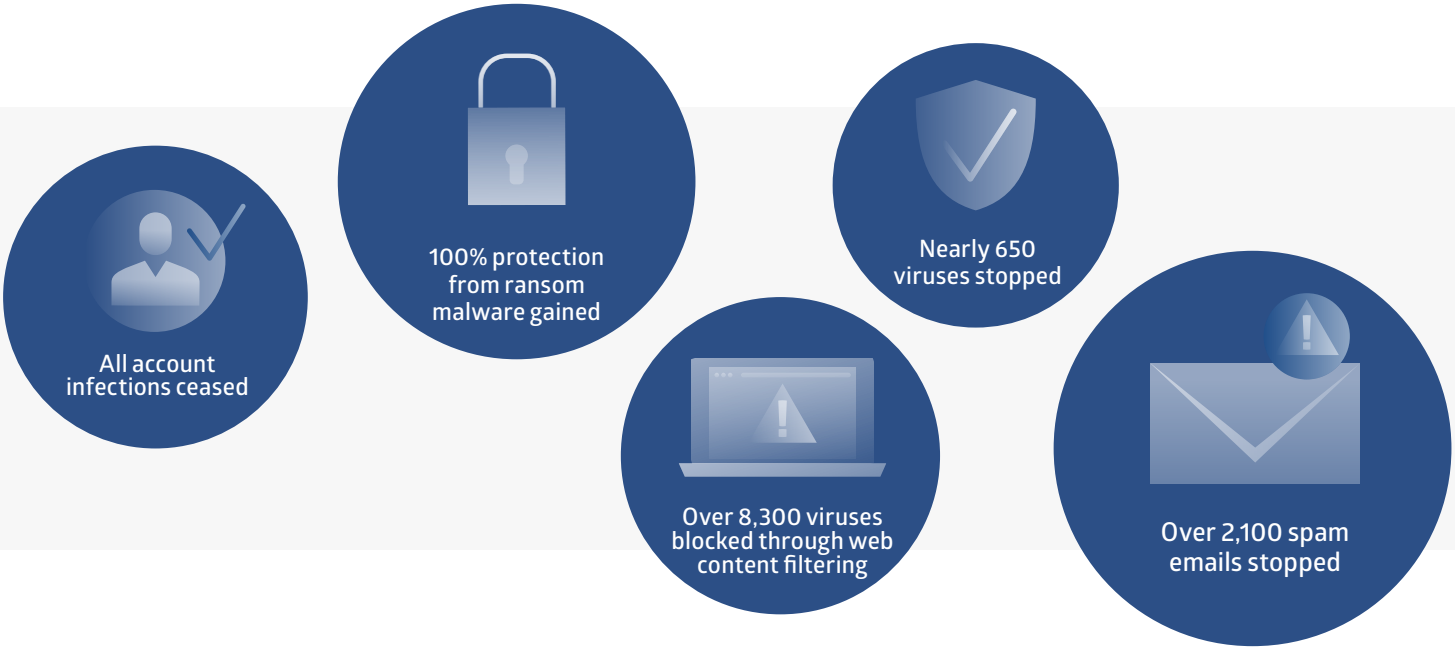


CloudCover's CC/B1 Platform delivers automated security at microsecond speed, with near-zero latency delay. The patented AI-based security orchestration, automation, and response (SOAR) threat management acts as a protective layer that measures, quantifies, and predicts risk of incremental data, in motion, near real time — and with 99.9999999% accuracy. B1 is known as an N-SOC (no security operation center) as it requires no human intervention, making it the ideal platform for organizations that want to focus on proactive CyberSafety and data privacy, but don't have the staff in place to do it.

The results

100% protection from ransom malware within two weeks

Within a two-week period, CloudCover's B1 architecture was protecting all of the bank's data security concerns, utilizing AI-driven, zero-day tolerance criteria:



The CC/B1 Platform enabled this bank to do what they thought couldn't be done: have a holistic cybersecurity strategy that puts them in the driver's seat of being able to proactively detect and deflect attacks without having to hire additional contractors or team members. It also allows them to concentrate on other aspects of the financial industry's digitally focused future.

Ready for a more proactive approach to your financial institution's cybersecurity strategy? Take a look at CloudCover's CyberSafety CC/B1 Platform or contact us directly to learn more.

References

Dautovic, G. (2021). "Top 25 Financial Data Breach Statistics for 2020." Fortunly.
https://fortunly.com/statistics/data-breach-statistics/#gref

Eisenbach, Thomas; Kovner, Anna; and Lee, Michael Junho (2020, Revised 2021). "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis." Federal Reserve Bank of New York. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf

Holzhauer, Brett (2021). "Digital Banking As The New Normal In 2021: What To Expect From Banks." Forbes Advisor.
https://www.forbes.com/advisor/banking/digital-banking-as-new-normal-2021-what-to-expect/

Knudson, Julie (2021). "Top Bank Risks for 2021." ABA Banking Journal. https://bankingjournal.aba.com/2021/01/top-bank-risks-for-2021/

ReputationUs (N/A). "Study reveals impact of cyberattacks on consumer confidence, corporate reputation." ReputationUs CyberSurvey.
https://www.reputationus.com/CyberSurvey/

Zetter, Kim (2021). "Hacking Wall Street." The New York Times Dealbook.
https://www.nytimes.com/2021/07/03/business/dealbook/hacking-wall-street.html

