

INDUSTRY OVERVIEW

Credit Unions

#1 Cost of Cybercrime

Authorities such as the FDIC have warned credit unions that they are at greater risk for cyber attacks. This concern is echoed by an FFIEC advisory from 2015 indicating they believe attacks on credit unions are increasing in frequency¹.

Why Are Credit Unions a Growing Target?

Stretched IT Resources

Cyber attackers are aware of the struggle that many credit unions have to financially resource and staff a 24/7 security monitoring solution.

Valuable Client Data

A common tactic for a cyber attacker who is seeking financial gain is to go after the most well known repository of money – credit unions.

Automated Defenses

Many credit unions rely on layers of automated security technologies. Today's sophisticated cyber attackers target these organizations as they are skilled in eluding this approach.

Cybersecurity Reimagined for Credit Unions

As banking continues to become a growing target for cyber attackers, you need a solution that constantly evolves with cyber attacks. eSentire Managed Detection and Response™ is designed to see the threats that traditional security defenses aren't able to detect helping you stay ahead of governance requirements.



ELITE

Say good-bye to 1000s of alerts and hello to the intelligence team that manages them for you.



SMART

Moving far beyond IDS/IPS and SIEM to detect the threats that they can't see.



AGILE

Trusted experts protect your network 24X7 and respond instantly to threats.

¹FFIEC Releases Statement on Cyber Attacks Involving Extortion, November 15, 2015.



Meet the compliance and governance needs of your clients

Cybercrime is on the rise across all industries. Many of the industries your clients do business in are experiencing increased governance, compliance and due diligence regarding their security posture. As a result, your clients expect that their banking institutions will protect their assets to the highest possible security standards. Our security experts understand the unique external and internal pressures your clients face. eSentire Managed Detection and Response absorbs the complexities of the evolving cybersecurity landscape to ensure you have the appropriate security practices and policies in place to retain and gain business in the growing digital economy.



Rest assured your privileged data is safe

You have a regulatory, ethical and legal obligation to protect your account holders' financial assets. Cyber attackers target your networks daily because they see credit unions as an easier target than the national and super regional banking brands. Our 24X7 team of security intelligence analysts live inside our technology and know what to look for when it comes to the latest threats. They use sophisticated forensic tools to investigate and respond to suspicious behavior and lock it down - within seconds.



Leverage a virtual team of experts

From forming a team of the appropriate skill sets to budgeting for 24X7 support, resourcing an internal security operations center is not easy. Our team acts as an extension of yours, constantly monitoring, detecting and containing threats so you can focus on your business instead of managing cybersecurity.



Stay out of the headlines

Not all press is good press - especially when it comes to a cyber breach. A cyber breach can cost a bank much more than business disruptions or compromised confidential information. The reputational damage can negatively affect your performance and profitability long after the breach is resolved. In order to stay out of the headlines, you need a solution that evolves as fast as the attackers. With robust threat detection capabilities, industry best threat intelligence, and powerful forensic investigation tools, our skilled security analysts keep your network safe - all day, every day.



Stop the threats traditional technology can't see

Typically, credit unions leverage layers of automated traditional security solutions. However, the unfortunate reality is that as cybercriminals become more sophisticated, these solutions fail because they can't see never-before-seen attacks. To protect you from these threats, we've reimagined the traditional SIEM and IPS by extending their capabilities through a single service. eSentire Managed Detection and Response leverages complex signatures and rules to automatically block threats in real-time. It also uses behavioral-based anomaly detection, log correlation and full-packet capture to provide a richer data set used to confirm unknown threats.