INDUSTRY OVERVIEW

Community Banks

The cybersecurity landscape for community banks is setting off some major alarm bells. Not only has the Federal Deposit Insurance Corporation (FDIC) warned community banks they are at a greater risk for cyber attacks, but the Federal Financial Institutions Examination Council (FFIEC) has also released an advisory indicating they believe attacks on banking institutions are increasing in frequency.

Challenges in Meeting Regulatory Requirements

There is no doubt – cybercrime is no longer limited to big banks. As a result, regulators, are driving towards more stringent regulations. For community banks, the pressure to comply with these growing requirements is at an all-time high. This presents a host of new challenges and there is no expectation that requirements will diminish.

Navigating the Complexities

The FFIEC recently released a new resource, the Cybersecurity Assessment Tool, which evaluates your cybersecurity risk profile and maturity. Many community banks struggle to accurately complete this required assessment given the resources and expertise needed to evaluate and understand gaps in your current approach to cybersecurity.

Managing Multiple Vendors

Many community banks have invested in multiple layers of security and other technologies to shore up their defenses against today's sophisticated cybercriminals. Every layer adds to the complexity of understanding and documenting how the layers weave together, and how each vendor satisfies different pieces of the numerous regulatory requirements. It's critical you know where your gaps exist – this can be difficult when working with different vendors with varied support agreements.

Increasing Cost of Compliance

Regulators not only require the appropriate technologies to defend against cyber threats, they also require you to have the appropriate risk management practices and strategies in place, reviewed on a regular basis. Resourcing for these audits, in-house or outsourced to multiple vendors, to ensure you have the expertise required to hunt today's advanced cyber threats while preparing controls like an incident response plan can be both complex and costly.

Simplify Your Approach With a Single End-to-End Solution

eSentire Managed Detection and Response™ is a holistic cybersecurity solution that combines a suite of security technologies and services to keep your bank and customers safe from sophisticated attacks while helping you understand your network's vulnerabilities, assess your unique risk and compliance gaps, and develop a strategic plan to get to where you need to be. This isn't another security technology – it's a security solution that helps protect your bank, discover weakness and strategically grow your security posture overtime – all through a consultative, white-glove approach.

Your Current Approach	Service	The eSentire Difference
VENDOR A	IDS/IPS	**NETWORK INTERCEPTOR™** Protect against known and unknown threats
VENDOR B	SIEM	**LOG SENTRY™** Enhance detection through next-generation log aggregation, correlation
VENDOR C	VULNERABILITY SCANNING	**CONTINUOUS VULNERABILITY SCANNING** Reduce exposure and minimize the exploit window
VENDOR D	MALWARE PREVENTION	**DNS FIREWALL™** Protect every connected device from known malicious internet sites
VENDOR E	INCIDENT RESPONSE PLAN	**INCIDENT RESPONSE PLAN REVIEW AND TESTING** Ensure you are prepared
VENDOR F	FFIEC GAP ANALYSIS	**ADVISORY SERVICES** Identify existing gaps to focus on the most critical compliance areas
VENDOR G / IN-HOUSE	HUMAN SOC	**24x7x265 SECURITY TEAM** Hunt for indicators of compromise and support remediation - *no extra charge*
ADD UP WHAT YOU ARE PAYING FOR THESE SERVICES INDIVIDUALLY	COST	**ONE PACKAGE PRICE FROM eSENTIRE**

esentire

www.esentire.com