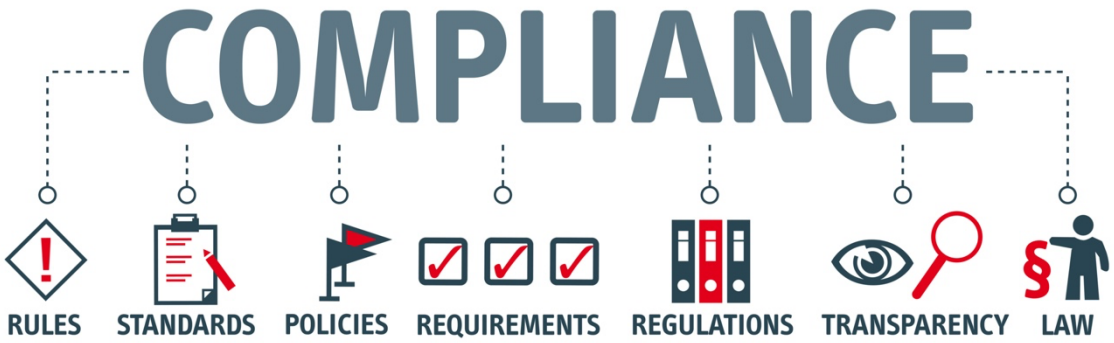

360
SOC

360 SOC Banking Industry Whitepaper

Client Industry: Banking
Client Endpoints: 2350
Client Locations: 42
Client Datacenters: 2
Estimate Revenue Size: 5 Billion

The Use Case

The board set a requirement to shift the overall security methodology to a robust security posture that will require a full transformation of how the business accepts and understands risk. The institution has consumer and business customers. The business has grown faster than technology has grown. Additionally, finding the right personnel with the right skill set has become an increasing challenge for this customer. Compound the personnel issue with an end of life infrastructure issue on the horizon. The institution is regulated by the OCC, PII, HIPAA and PCI. The customer is looking to achieve ISO 27001/27002 by the end of 2023. This additional requirement is being pushed down by the organization as a marketing differentiator.



The Solution

After multiple discussions, compliance planning and assessments, 360 SOC and the institution decided with the client that the 360 SOC secure everything methodology (layered security approach) was the right solution powered by 360 SOC's SOC as a Service (Managed Security) and 360 SOC's SDWAN as a Service (SDWAN). The solution started with the implementation of a Next Generation SIEM (Log and Event Management) solution included User Entity Behavioral Analytics (UEBA) and Network Detection and Response including Full Packet Capture (NDR) in order to create visibility and efficient reporting to the overall environment.

From there, 360 SOC delivered a Next-Generation Endpoint Solution as a managed solution (EDR) to protect against malware. We then coupled that with a managed DNS protection by 360 SOC with log retention in AWS with the intention of these service to protect the institution's web and roaming users. To help prevent phishing and malware via email, 360 SOC implemented a cloud email security appliance, 360 SOC Email Security for

Office 365 for both inbound and outbound emails to provide encryption, spam filtering and phishing prevention.

We then completed another assessment to determine further gaps/posture improvements that can be implemented. We then created the next layer, we added a set of managed firewalls with a separate IDS and IPS with a goal of creating an automation workflow that starts in the cloud, flows to the endpoint, then validates through the Intrusion Detection Solution to address the edge and the segmentation of known and unknown workflows.

Our next step was a transformation of how wireless and wired users will be authenticated and controlled whether a corporate owned device or the ever-challenging BYOD device. We implemented an Identity Services (NAC) tool in order to track the device and apply policy, posture, profiling for authentication.

After this step, we then needed to create an audit trail of users (that access data) by leveraging a DLP (Data Loss Prevention) solution in order to protect data at rest, data in motion and data in use and address compliance requirements such as GDPR.

The last step, we implemented was the ability to audit and track vulnerabilities and compliance gaps present in the environment. We

accomplished this by adding a vulnerability management solution by 360 SOC and Penetration Testing.

The Outcome

360 SOC is now managing the day-to-day security events and alarms, IDS and IPS events, internal and external vulnerabilities, endpoints and the institution's most critical assets. The institution is now able to focus on serving their internal and external customers more efficiently without having to worry about chasing down the next security event.

Additionally, the institution's IT team has been able to cut down their compliance audit time by nearly 57% providing them more time to focus on innovating and servicing the business. After 12 months of management, the institution estimated their cost savings at just over $525,000 per year by outsourcing to 360 SOC.

Solutions and Services currently implemented and managed by 360 SOC for this financial services client:

Managed SIEM (Log and Event Management)
Managed Vulnerability
Managed Compliance
Response and Remediation as a Service
Managed Asset Discovery
Behavioral Analytics and Machine Learning
Managed Endpoint (EDR)
Managed DNS w/Intelligent Proxy
Managed Identity Services
Managed Firewall
Managed Intrusion Detection and Prevention
Managed Email Security and Encryption
Managed Cloud Security (Managed WAF and Load Balancing)
Virtual CISO and Virtual CIO
Vulnerability Scanning
Penetration Testing
Advanced Incident Response (24 Hour Onsite Major Breach)
Resource on Demand (Tier 3 and Beyond Support)
Managed Secure SDWAN as a Service (SDWAN)

Interested in hearing more about 360 SOC?

Our contact information is below and feel free to visit our website at www.360soc.com.

360 SOC
Sales Department
info@360soc.com
1-866-278-5578