Managed Security Featuring Extended Detection and Response:

Financial Services

Background:

Financial institutions face an ever-expanding array of cyber threats coupled with increasingly stringent regulatory requirements for data privacy and security. For organizations in this sector, the risk is two-fold — losing customer trust due to a security breach coupled with the potential for large fines for noncompliance. Many financial institutions have partnered with a managed services provider (MSP) to handle high-level security tasks such as monitoring and vulnerability management. In today's threat climate, more financial institutions are turning to providers who can deliver extended detection and response (XDR) across the IT environment.

Project Summary:

A large regional credit union with nine service centers was growing rapidly. The organization was using an MSP to manage its network, but had become dissatisfied with the level of service and concerned about the MSP's ability to scale.

The credit union felt it needed a more integrated management and security model. The organizations began looking for an MSP with deeper expertise, more sophisticated technology tools and a stronger understanding of regulatory requirements. SirviS was asked to conduct a technical discovery meeting with key executives and present a solution that would meet the organization's objectives.

SirviS provided a deep dive into its core network monitoring infrastructure and the AI-based tools it uses for XDR capabilities. The SirviS team utilizes these tools, coupled with well-defined methodologies, to provide a unified approach to managed services. SirviS can deliver highly responsive services remotely, and has highly skilled field services technicians who provide onsite "smart hands" capabilities as needed. The credit union was satisfied that SirviS could meet its demanding requirements even though the SirviS Network Operations Center (NOC) was in a distant state.

Additionally, SirviS showed how it could utilize the logging and audit trail features of its monitoring tools to assist the credit union with its compliance requirements. The SirviS team would also be available throughout the annual audit to answer regulators' questions as needed.

Project Specifics:

SirviS began by refreshing all of the network hardware in the credit union’s corporate headquarters and every branch location. This included new servers, routers, firewalls and wireless access points, and integrating the SirviS monitoring and management tools into the environment.

Once the network refresh was complete, SirviS began a five-year, 24x7 fully managed security contract. SirviS monitors the network infrastructure to ensure the highest levels of availability and performance. Continuous security monitoring detects not only attempts to breach the network, but threats that are able to make it past perimeter security controls. These tools alert the SirviS team and take automated action to isolate and remediate the threat.

In addition to monitoring the credit union’s core infrastructure, SirviS deployed managed detection and response (MDR) tools to every user device — desktops, laptops, tablets and employee smartphones. The MDR tools enforce corporate security policies across the devices, and alert the SirviS team of any suspicious behavior. Because the MDR tools are part of a unified monitoring and management solution, the SirviS team has the context needed to quickly identify and respond to threats.

Additionally, the SirviS tools monitor and manage the credit union’s Microsoft 365 accounts and Google Workspace, as well as mobile apps. SirviS also performs threat hunting, proactively searching for threats that might go undetected in order to minimize risk. The SirviS team stays abreast of threats that specifically target the financial services sector.

Results:

SirviS has the people, processes and technology to deliver advanced managed services from the desktop to the data center. Although many organizations gravitate toward a local MSP, SirviS proved that it has the resources and scale to meet the stringent requirements of a growing credit union. SirviS is able to deliver an XDR solution that maximizes availability and performance and bolsters the credit union’s security posture. The SirviS team also has the expertise to assist with the credit union’s regulatory compliance requirements.