

# ALWAYS LEADING

## Bank Invests in Fortis Security Services for AWS Cloud

### HIGHLIGHTS

---

#### Customer

- Financial services that include banking, lending, mortgages, and more

#### Industry

- Banking/Finance

#### Customer Environment

- Cisco and Dell Technologies products for on premise, AWS for cloud and applications
- Customer was shifting a majority of its IT environment into the cloud

#### Key Challenges

- Fortis by Sentinel now handles the security monitoring, detection, and response of all primary cloud elements for the customer
- Customer has increased visibility into their cloud environment and plans to make further cloud investments with the confidence they will remain secure

### CUSTOMER

A financial services provider with locations throughout the United States, Latin America, and the Caribbean, this customer leverages expertise from more than 125 years of success in banking to help businesses, retail customers, and individuals with their fiscal needs.

### ENVIRONMENT

The customer's data center and infrastructure were primarily comprised of Cisco and Dell Technologies hardware and software. This included top security solutions to ensure protection of client data, servers, and critical desktop components. As part of a modernization project, the customer had also begun to migrate a significant portion of its IT infrastructure into the AWS cloud.

### CHALLENGE

As the customer started to shift most of their environment from on-premise into the cloud, one of their primary concerns was the safety and security of highly sensitive bank data. This included private information from their clients that required the highest levels of protection. They engaged with long-time partners Sentinel and its security arm Fortis by Sentinel to develop a comprehensive package of protection for their AWS cloud investments.

### SOLUTION

The Fortis by Sentinel team deployed an extensive array of security solutions and services designed to satisfy the customer's most rigorous regulatory requirements. Fortis ran routine scans of the customer's AWS environment searching for known software vulnerabilities, changes or misconfigurations of resources, and potential compliance issues. Full 24x7x365 Fortis Security Operations Center (SOC) monitoring kept a close eye on security events, complete with customer alerting, expert remediation recommendations for incidents, and the mitigation of Distributed Denial of Service (DDoS) attacks. Further layers of security included Fortis management of the customer's Intrusion Prevention System (IPS), Detection and Response (MDR) for AWS endpoints, as well as a Web Application Firewall (WAF). Lastly, Fortis provided Business Continuity and Ransomware solutions to help the customer quickly recover should they experience any sort of mass encryption event.

Confidential Information Property of Sentinel Technologies, Inc.



sentinel.com

ALWAYS LEADING

# ALWAYS LEADING

## RESULTS

The advanced level of protection delivered through Fortis by Sentinel solutions and services gave the customer peace of mind as they transitioned much of their IT environment into the AWS cloud. Not only did these security enhancements go beyond current regulatory requirements for financial institutions, but they also improved the visibility and control of applications, infrastructure, and endpoints within the cloud. This more granular management, along with the constant monitoring and regular scanning, left the customer with increased confidence in their ability to detect, defend against, and recover from an attack with minimal issues or disruption to their business.

Confidential Information Property of Sentinel Technologies, Inc.



[sentinel.com](https://www.sentinel.com)

**ALWAYS LEADING**