PRESIDIO® | Case Study

Technology

From blind spots to automated security - vulnerabilities that took weeks to find now remediate in hours

The Outcome

StartingPoint had high-severity vulnerabilities sitting undetected across their AWS infrastructure. After engaging Presidio Adaptive Cloud Services, automated weekly scanning replaced manual guesswork. Detection dropped from weeks to seconds. Remediation dropped from days to hours. StartingPoint now has the security foundation to pursue SOC2, PCI, and other compliance certifications.

How They Got There

Presidio deployed Amazon Inspector with a weekly CVE scanning schedule across StartingPoint's EC2 environment. High-severity findings automatically trigger a Datadog alert and a ServiceNow incident ticket routed to Presidio's managed services team. AWS Systems Manager Patch Manager handles remediation on a monthly maintenance schedule, with out-of-cycle patching triggered automatically for critical findings.

Why It Worked

StartingPoint's main risk was having no way to know where their infrastructure vulnerabilities were. Automating detection and remediation closed that exposure and created an audit trail that now serves as the foundation for future compliance certifications.

The Situation

StartingPoint, a hosted software provider, understood that customer trust depends on the security of the infrastructure running their applications. They had no reliable way to know whether their EC2 instances were exposed. Their security posture was reactive by necessity - there was no systematic process for detecting or remediating vulnerabilities before they became risks.

The Approach

Presidio deployed Amazon Inspector with a scheduled weekly assessment template running the CVE rules package across all of StartingPoint's EC2 instances. High-severity findings automatically generate a Datadog alert and a ServiceNow incident ticket routed to Presidio Adaptive Cloud Services. AWS Systems Manager Patch Manager handles remediation, with a monthly maintenance window for ongoing patching.

The Result

Vulnerability detection dropped from weeks to seconds. Time to remediation for high-severity findings dropped from days to hours. The monthly patching schedule ensures the environment stays hardened. The consistent, documented patching history now serves as the compliance foundation for StartingPoint to pursue SOC2, PCI, and other certifications.

Weeks → Seconds

Vulnerability detection time after automated scanning

Days → Hours

Time to remediation for high-severity findings

Weekly

Automated CVE scanning with zero manual intervention