# Strengthening Agency Cybersecurity Using AI-Powered ForeSite360 Platform

Use Case: Enterprise Observability

## Introduction

ForeSite360's AI-powered platform, **ForeSite360®**, is an *Enterprise Intelligence* solution that provides real-time operational insights and automated decision support across government and commercial organizations, enabling faster, more consistent outcomes from enterprise offices to the tactical edge. ForeSite360 serves federal agencies and commercial clients in healthcare, hospitality, food service, national security, logistics, fleet management and information technology.

***This Case Study explores the successful use of the ForeSite360 Enterprise Intelligence Platform deployed at a complex, multi-component federal agency under an enterprise IT observability use care. This case study illustrates how AI-powered enterprise observability, enabled by the ForeSite360 platform, helped the agency transform its cybersecurity posture for a multi-Cloud national ecosystem, achieve measurable mission improvements and drive down the cost of enterprise IT.***


## Executive Summary

A major federal agency responsible for administering a nationally deployed programs, serving more than 180 million Americans, faced escalating cybersecurity challenges as it transitioned to a multi-Cloud operating model. With mission-critical workloads operating across AWS, Azure, Google Cloud, on-prem data centers, and regional field systems, the agency struggled with blind spots, inconsistent controls, rise in breaches and slow incident response.

To address these challenges, the agency implemented a multi-Cloud enterprise observability capability, built around a centralized Security Operations Center (SOC), automated governance, and AI-enabled analytics all made possible by ForeSite360. This Enterprise Intelligence Platform, configured and deployed to support complex observability tasks, became the foundation for strengthening cybersecurity practices across all environments—improving visibility, resilience, and response times at national scale.

Under an "IT observability" use case, ForeSite360's AI powered critical decision making to enhance the organization's ability to secure, observe, and operate complex enterprise- and national-level IT ecosystems. ForeSite360 fuses cyber, Cloud, and operational telemetry into a unified mission picture, turning fragmented data into reliable data for automated decision making and prediction of mission disruption in time to take evasive action -- all while providing actionable insights. ForeSite360 unified data from 60+ sources including commercial and enterprise networks, security events, application data, tactical devices data (including non-IP based), and other technical telemetry data into a shared intelligence layer. ForeSite360 quantified and then visualized mission/business risk in real time, identifying where operational degradation or cyber anomalies threatened readiness. Its AI-driven correlation engine and behavioral analytics detected emerging vulnerabilities, predicted mission impact, and triggered proactive mitigation before users experienced disruption. Its built-in mission-tied dashboards allowed decision-makers to prioritize resources where they matter most. ForeSite360 empowered executive, managers, tactical operations leaders and technical staff to see, predict, and act before business risk became business loss.

This innovative platform unified security operations for multi Cloud, provided centralized real-time visibility, leveraged AI-powered analytics and automated enforcement of security policies, to securely harness multi Cloud innovation without blind spots or compliance gaps. The IT organization realized significant cost savings on three major IT contracts as a result of the AI automation and a reduction in MTTR of 35%. Customer experience was enhanced through AI automation.

## **The Challenges:** Fragmented Visibility, Shadow IT, and Operational Blind Spots

As the agency expanded its Cloud footprint, the cybersecurity team encountered several systemic issues that created numerous vulnerabilities that were exploited under multiple high-impact security breaches:

- **Limited enterprise-wide visibility**: Project teams frequently launched Cloud services independently, leading to "shadow IT" systems invisible to security analysts. Without unified visibility, threat detection was inconsistent and reactive.
- **Siloed logs and incomplete forensic data:** Each Cloud provider used its own logging formats and dashboards. Logs from AWS, Azure, and Google Cloud were stored separately, making it nearly impossible to correlate events or conduct investigations quickly.
- **Slow incident response:** Security teams relied on manual processes, often switching between disparate tools to assess and contain threats. Cross-Cloud investigations could take days.
- **High risk of misconfiguration:** Rapid deployment of Cloud workloads increased the likelihood of human error—such as incorrectly configured storage buckets, open ports, or inconsistent identity policies.
- **Talent shortages:** The cyber workforce was overstretched. Analysts struggled to keep up with the volume of Cloud telemetry and the complexity of multi-Cloud environments.

With these conditions, even minor incidents carried outsized risk. The agency recognized that its Cloud growth and diversity required a fundamentally different approach that included one centered on unified observability and powered by AI -- enter ForeSite360.

## **Intelligent Modernization:** People, Processes, Technology

The ForeSite360 team was consulted to address these challenges in a manner that built on what was working, alleviated pain points, and would be easily adopted by federal staff from the hands-on to the executive level teams, and more than 100 contractors providing various parts of the agency's IT ecosystem. To regain control, modernize and harden the cybersecurity posture, the ForeSite360 team recommended the agency deploy an integrated observability capability. The ForeSite360 platform was selected for the job, with a configuration of dashboards, data ingestion, and AI tooling to create a multi-Cloud Enterprise Observability Platform.

With the ForeSite360 platform configured for an Observability use case, the following key elements of success emerged:

### Centralized Security Operations Across All Clouds

A multi-Cloud Security Operations Center (SOC) was established enabled by the ForeSite360 platform. Immediate efforts focused on creating:

- A single pane-of-glass across all Cloud and on-prem environments
- Real-time visibility into all infrastructure, workloads, identities, and network traffic
- Ability to detect, investigate, and respond through one unified interface

This consolidation eliminated blind spots and standardized security practices across the enterprise. ***Impact:*** *The SOC reduced time spent switching between tools by 60% and improved detection coverage across environments by 40%.*

### Centralized Log Retention & Cross-Cloud Data Correlation

ForeSite360 implemented a unified log pipeline that ingested telemetry from AWS, Azure, Google Cloud, on-prem servers, field systems, and IoT devices (IP and non-IP based), normalizing and storing them in a centralized data platform. This enabled enterprise-wide forensic search, faster investigations, rapid identification of cross-domain activity, and long-term retention for regulatory and threat-hunting needs. ***Impact****: Investigations that previously took 3-5 days were reduced to minutes or hours, dramatically improving containment speed.*

### Automation and AI to Multiply Workforce Capacity

Automation and AI were deployed to establish behavioral baselines, identify anomalies across Clouds, automate initial triage of alerts, normalize multi-Cloud log formats, and suggest likely attack paths and affected systems. The system's AI models flagged unusual activities (anomalous admin access patterns or suspicious configuration changes) before they became incidents. ***Impact:***
*More than 70% of alerts were automatically triaged without human intervention, allowing analysts to focus on complex threats.*

### Automated Governance and Technical Guardrails

The platform enforced governance through pre-configured landing zones, automatic encryption, tagging, network baselines, and IAM guardrails. It maintained continuous compliance with NIST and FedRAMP standards and included automated remediation of

misconfigurations. This approach reduced the risk of human error while standardizing security across all regions and workloads. **Impact:** *Misconfiguration-related security findings dropped by over 50% within the first year of operations.*

## Transforming Cybersecurity at National Scale – The Payoff

- **Full Situational Awareness Across Mission Systems**
  **Impact:** The agency achieved unprecedented visibility across its multi-Cloud and on-prem ecosystem—including real-time detection of vulnerabilities, misconfigurations, and anomalous behavior.

- **Faster Response and Containment**
  **Impact:** *Enterprise-wide incident response improved dramatically. The SOC could isolate workloads across Clouds in minutes instead of hours or days.*

- **Improved Resilience Against Advanced Threats**
  ***Impact:*** *The new observability capability allowed teams to identify lateral movement, privilege escalation, and unusual access patterns far earlier in the kill chain.*

- **Stronger Compliance and Audit Readiness**
  ***Impact:*** *Centralized logs and automated compliance scans positioned the agency for easier audits and reduced the manual burden of reporting.*

- **Sustainable Security Despite Workforce Constraints**
  ***Impact:*** *Automation lightened the load on analysts and allowed a lean cybersecurity team to protect a sprawling ecosystem using AI-driven insights and workflows.*

### ForeSite360 In Action

**Rapid Detection of a Cross-Cloud Credential Abuse Attempt.** *The ForeSite360 platform detected unusual login behavior involving privileged credentials. The account accessed Azure resources for the first time, logins occurred at atypical hours, network flows showed suspicious activity toward an on-prem system, and API calls originated from an unexpected geographic region. Without ForeSite360, these signals would have been scattered across separate dashboards to be synthesized by multiple teams manually, but with ForeSite360 AI as the centralized observability platform, events were correlated without any human intervention, AI classified the activity as high risk, and an automated playbook suspended the account. Security analysts received a real-time alert, and investigators used the unified log store to track activity across all Clouds and on-prem systems. The incident was contained in under 5 minutes, preventing unauthorized access to sensitive data and stopping potential lateral movement – with little to no human involvement required to stop the breach.*

## Conclusions

**Observability as a Strategic Cybersecurity Advantage.** This nationally deployed federal system demonstrates that enterprise observability must be more than a lose collection of best-of-breed monitoring tools to scale to the challenges of multi-Cloud. By fusing data of more than 60 best-of-breed monitoring tools within the ForeSite360 enterprise intelligence platform, this agency not only scaled their multi-Cloud presence but also had dramatic reduction in costs. The holistic approach leveraged AI via ForeSite360, unified visibility, leveraged automation, and enforced governance, allowing the agency to transform its security posture in a complex multi-Cloud ecosystem. In the modern multi-Cloud era, AI-powered observability is not only beneficial, but is also essential to safeguarding federal systems, protecting citizens, and ensuring mission success at national scale.