ISE® AWARDS

EAST

Summit & Awards

20 YEARS

Maximus Cloud Security Governance

Jon Powers

Sr. Manager, Security Architecture

Guy Bridgeman

Sr. Director, Cloud Solutions

Nominee Showcase Presentation

Company Overview

maximus

- A leading strategic partner to governments across the globe delivering public health and human services
- Established in 1975
- 39,500 employees across 9 countries
- $4.25B annual revenue
- Largest provider of call center services to the US government

Presentation Overview

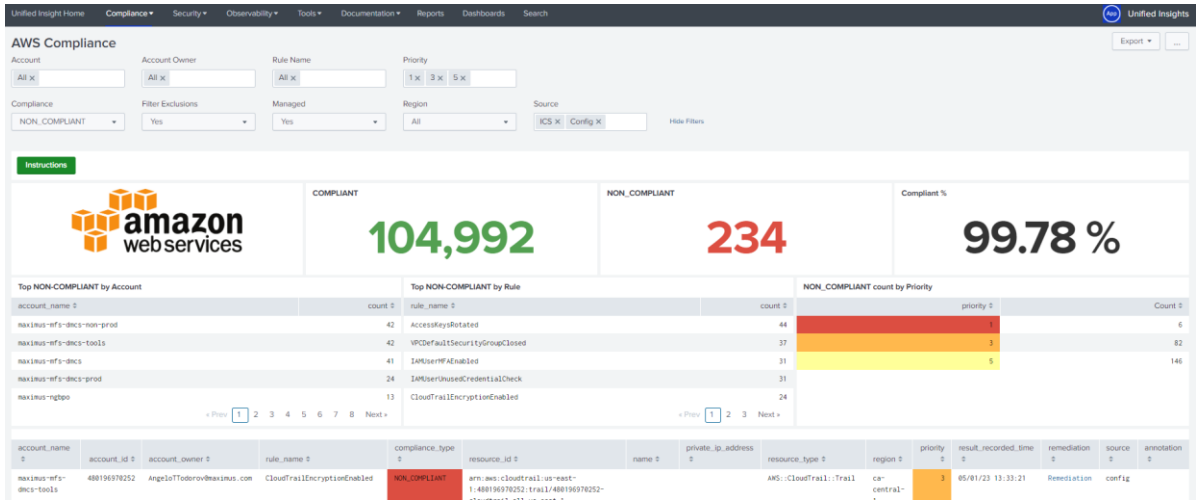
- Cloud Adoption Issues
- Immediate Risk Reduction
- InsightCloudSec Overview
- Visibility, Monitoring, Documentation
- Guardrail Components
- Impact and Lessons Learned
- Questions

Cloud Adoption Issues

- Maximus started migrating from on-prem datacenters to AWS in October 2019
  - “Lift and shift” to get products into the cloud quickly due to time constraints
- 200+ AWS accounts with different application architectures
- Varying levels of AWS maturity across IT, support, and development teams
- Security developed AWS standards based on NIST 800-53, CIS, AWS Foundations
  - Difficult to translate from writing into building infrastructure
- Initially started with AWS Config rules to report on compliance
- No alerting, acknowledgement, or automation to correct issues
- June 2021 discovered AWS resources were only 80% compliant with standards
  - Thousands of non-compliant controls
  - Many were high risk; Org level controls, missing WAF, missing security agents, etc.

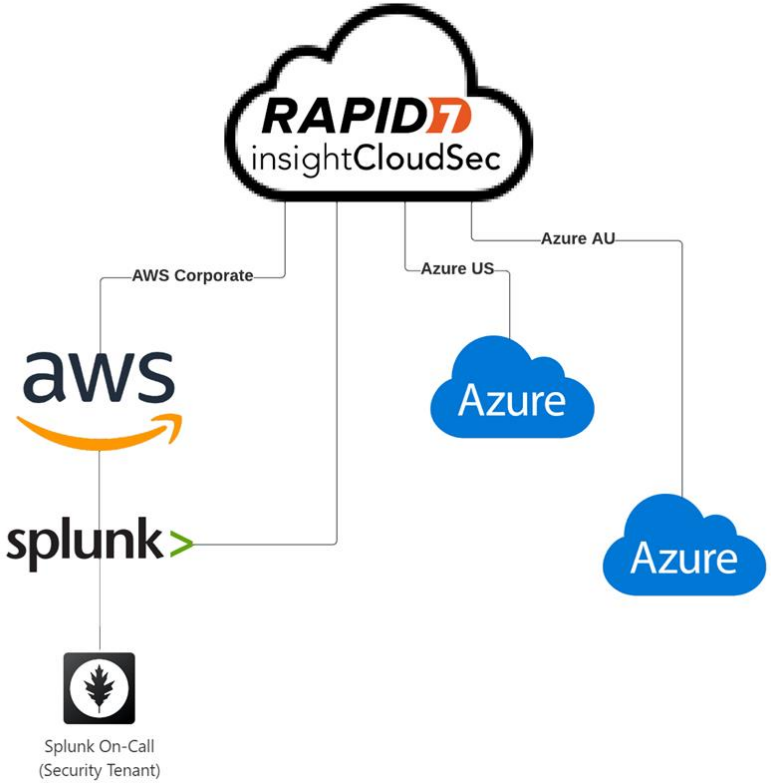
Immediate Risk Reduction

- Monitoring AWS Config compliance in Splunk
- Focused on driving manual remediation
- Prioritized by risk with expected timelines
- Automated where possible
- Educated owners on risk & remediation
- Improved compliance to 95% within a few months
- A long-term solution for automation was needed, especially for complex, multi-cloud future
- Selected Cloud Security Posture Management solution – Rapid7 InsightCloudSec

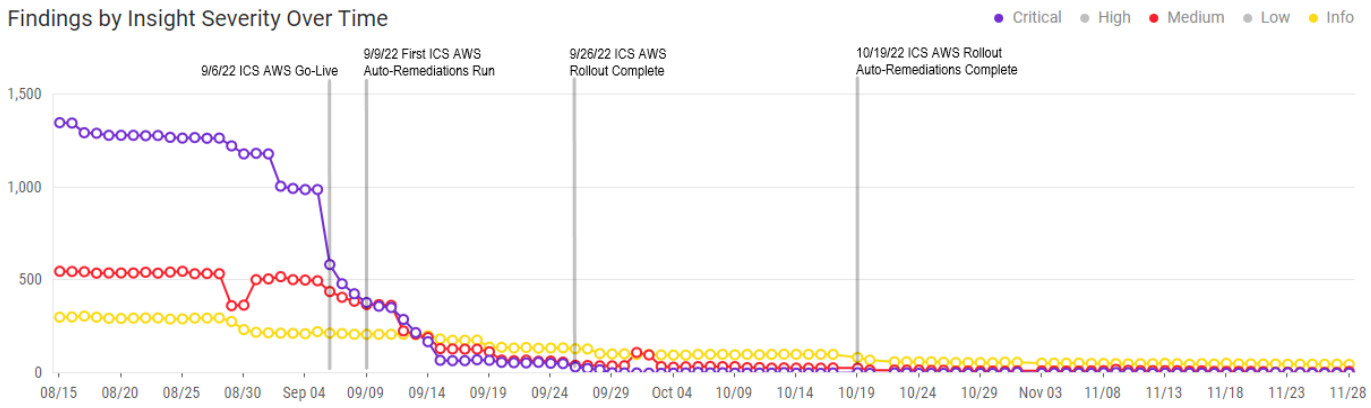


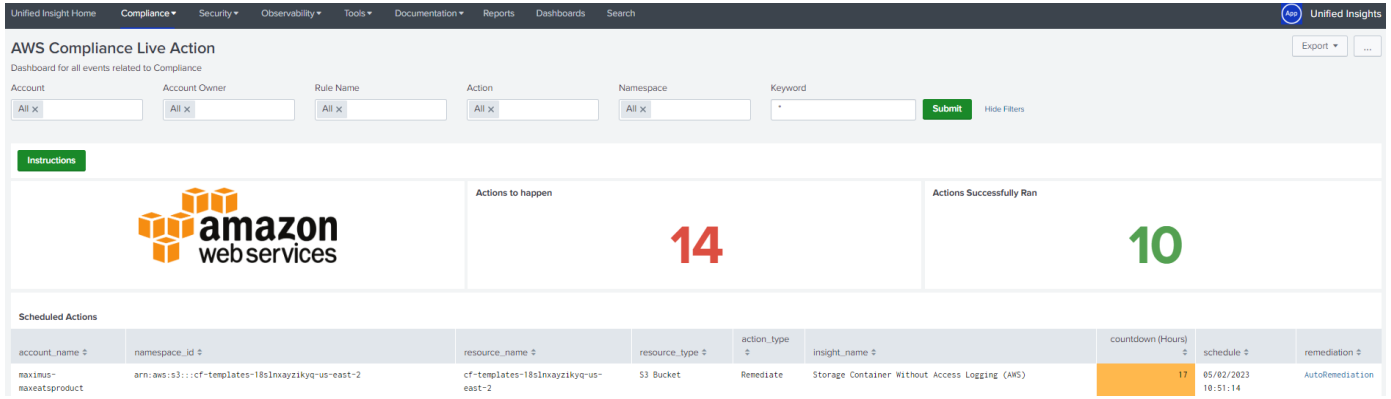
InsightCloudSec

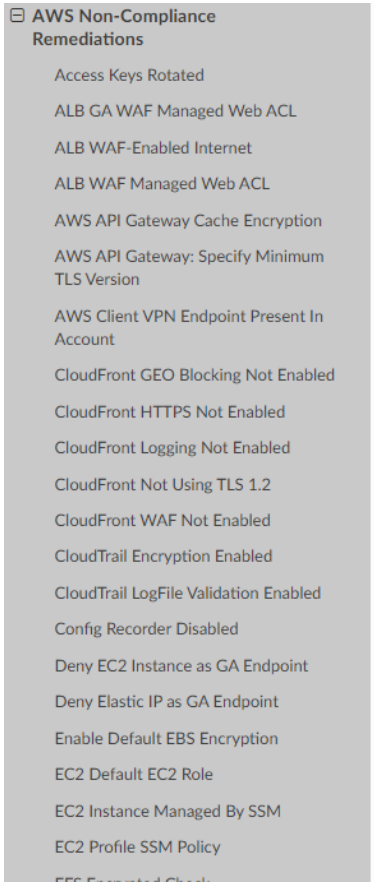
- Centralized multi-cloud visibility – Development to Production
- Custom compliance packs for AWS & Azure
- Continuous monitoring - new and existing resources
- Alerting – Near real-time
- Acknowledgement & Ownership
- Audit Trail
- Automated remediation throughout lifecycle



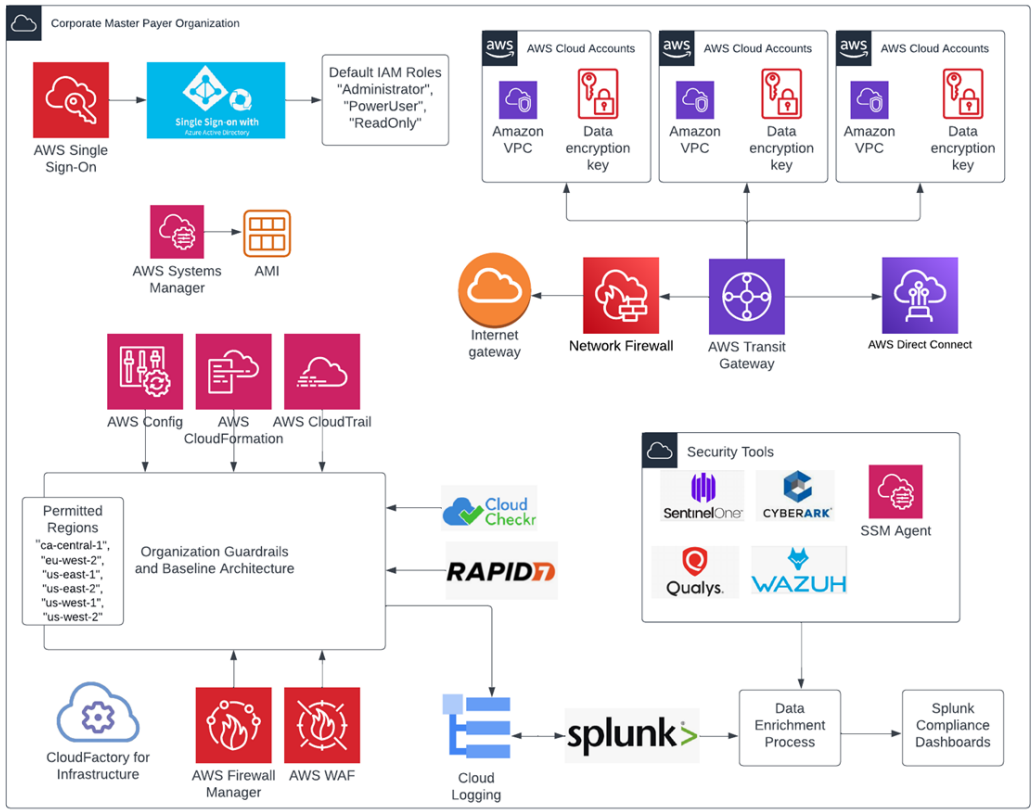
Visibility, Monitoring, Documentation

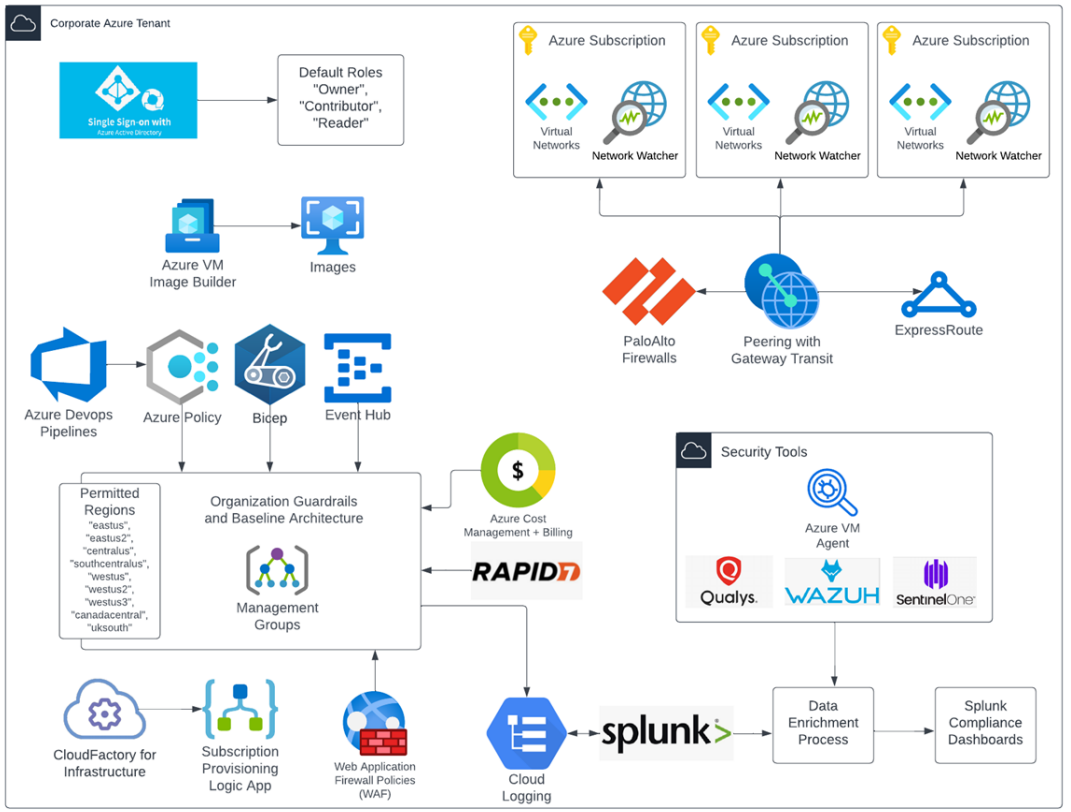






Guardrail Components





Impact and Lessons Learned

Impact

- Maintaining 99.9% compliance
- Environments are more compliant from the start
- Owners are remediating prior to InsightCloudSec taking action
- Extending to our global markets

Lessons Learned

- Establish cloud security standards, governance, and monitoring prior to migrating production workloads to public cloud service providers
- "Lift and shift" does not address complexities in the cloud
- Clearly define ownership and responsibility