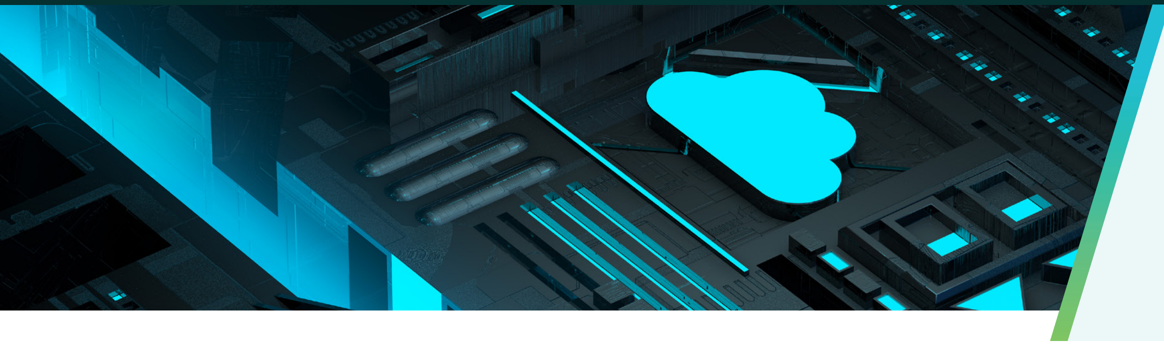
TD SYNNEX
Public Sector
DLT



aws
PARTNER
Managed Service
Provider

Case Study: Securing Compute Infrastructure with WAF and Limited Deployment

In this case study we explore how TD SYNNEX helps a government-funded health and science consortium partner enhance the security of their compute infrastructure by implementing a web application firewall and adopting a limited deployment approach.

The Problem:

The organization faced two key challenges:

1. Security Vulnerabilities: Their web application was being repeatably targeted by offshore bad actors and bad bots and required enhanced protection against unauthorized access.
2. Production Downtime: deployment of configuration changes was causing scheduled and unscheduled outages due to an aging deployment process with limited testing capabilities.

The Solution:

1. Web Application Firewall (WAF)
   - Deployment: TD SYNNEX deployed a WAF in front of application load balancer. The WAF inspected incoming traffic, blocking malicious requests based on predefined rules.
   - Ruleset Customization: TD SYNNEX customized the WAF rules to match the application's specific requirements. Blocking access using Geo-restriction, IP Reputation lists, and Bad Bot rules.
   - Regular Updates: The WAF rules are regularly updated to stay current with emerging threats
2. Limited Deployment
   - Staging Environment: TD SYNNEX maintains a staging environment for testing new features and updates. Only authorized personnel had access to this environment.
   - Limited Deployment: When changes deploy to production, new instances are provisioned in an autoscaling group. Testing procedures ensure that the updated instances are healthy and meeting all requirements. After all testing is completed successfully, additional instances are provisioned in production and instances with prior deployment versions are deprovisioned.
3. Monitoring and Incident Response
   - Real-Time Monitoring: TD SYNNEX set up real-time monitoring for anomalous behavior. They receive alerts for unusual conditions, such as unusually high load.
   - Incident Response Plan: TD SYNNEX developed an incident response plan, including steps for identifying, containing, and mitigating security incidents.

FOR MORE INFORMATION

Visit our website: **tdsynnex.com/na/us/td-synnex-public-sector/**
For questions, email: **publicsector@tdsynnex.com**
Initial Period of Performance: Feb 2024 - Jan 2025

How AWS Solutions Were Leveraged:

AWS WAF was used to create a Web ACL with managed rules protecting an Application Load Balancer.

AWS CodeCommit, EC2 Autoscaling, and S3 storage were used to create a limited deployment strategy.

AWS CloudTrail, CloudWatch, Trusted Advisor, Security Hub, Guard Duty, and Amazon Cognito were used to secure and monitor the cloud infrastructure.

Third Party Tools Used:

CloudCheckr, Automox, Crowdstrike, AppDynamics, Ansible Tower, and Zendesk Support.

The Outcome:

- TD SYNNEX significantly reduced the risk of security breaches.
- The limited deployment approach minimized disruptions during updates.
- Cost savings were achieved by avoiding large-scale redeployments.

Conclusion or Lessons Learned:

By combining WAF protection, limited deployment, and proactive monitoring, TD SYNNEX achieved a secure and cost-efficient compute infrastructure. This case study demonstrates that thoughtful security practices can enhance both safety and affordability.

About TD SYNNEX Public Sector

TD SYNNEX Public Sector is the premier government solutions aggregator that specializes in understanding the IT needs and solving the challenges of the federal, state, local and education markets.

FOR MORE INFORMATION

Visit our website: **tdsynnex.com/na/us/td-synnex-public-sector/**
For questions, email: **publicsector@tdsynnex.com**
Initial Period of Performance: Feb 2024 - Jan 2025