CyberRes | TriVir

Case Study

US Department of Defense Contractor

NetIQ Identity Governance accelerated the adoption of a unified review process to address audit findings and improve security and compliance at scale.

The Compliance Conundrum

A US Department of Defense (DoD) contractor had to prepare for compliance with the Cybersecurity Maturity Model Certification (CMMC). This new certification model is the latest development by the DoD to reduce risk in the defense supply chain. A compliant CMMC score is critical as future DoD procurements will require minimum CMMC scoring for suppliers to compete for contracts and task orders. To address specific CMMC security controls, DoD contractors must perform certain identity governance and administration processes. However, application owners were already struggling with the existing audits, access reviews, and compliance of several critical financial applications and other sensitive databases. The DoD contractor chose to leverage a COTS solution to address their governance deficiencies.

"Implementing NetIQ Identity Governance accelerated progress toward meeting CMMC requirements by automating the onboarding of so many applications quickly and simplified the administrative burden of governance across the organization, which was a huge positive paradigm shift."

Jim Montgomery
TriVir Governance Practice Lead

NetIQ Identity Governance to the Rescue

TriVir, a CyberRes partner with nearly 20 years of experience supporting commercial and government clients with complex identity and access requirements, was engaged to improve the existing governance processes and quickly integrate with enterprise systems. After assisting with vendor selection and recommending NetIQ Identity Governance, TriVir piloted a solution to connect Identity Governance with the Identity Vault, Active Directory, and the Card Management System.

NetIQ Identity Governance was ideal for the task of defining and enforcing identity governance controls for access to business applications, as well as enabling system owners to control the security of valuable business assets. This was all done in an automated, web-based fashion instead of spending weeks or months manipulating data in spreadsheets. While the deployment's default review fulfillment mechanism was to use ServiceNow tickets, some changes

At a Glance

Industry

Technology

Location

Global

Challenge

The business must pass a CMMC compliance assessment and improve enterprise governance audit results.

Products and Services

NetIQ Identity Governance
TriVir Identity Governance and Administration

Success Highlights

- Updated enterprise access review capabilities to adhere to CMMC controls
- Facilitated rapid application onboarding for thousands of applications
- Incorporated access reviews for privileged accounts through PAM integration
- Automated reviews and generation of audit evidence to reduce administrative overhead

could be made directly to the Identity Vault or Active Directory. The Internal Audit team reviewed evidence captured and presented by the system to ensure compliance with audit policy which increased the level of trust that the system was successfully collecting all relevant data and remediating access change decisions properly.

System and application owners saw these benefits and requested identity governance onboarding for their systems and applications. After the successful initial deployment, the management team was excited to tackle the next identity governance challenges.

The Database Dilemma

After the successful initial deployment, the next governance challenge was connecting to over 200 applications with accounts and permissions stored in databases with similar schemas. The typical configuration of one IG collector for accounts and one IG collector for permissions to each of these 200 databases wasn't feasible because it would take too long to configure each of these 400 identity governance collectors manually.

Jim Montgomery, TriVir Governance Practice Lead, explains the novel approach to integrating with so many applications: "We created an application integration model to quickly onboard more than 200 applications by leveraging the organization's Enterprise Service Bus (ESB) and two custom-developed NetIQ Identity Governance account and permission collectors for all 200 DBs." In most cases, database owners could onboard themselves with very little assistance–all they had to provide were the connection details and match up their database fields to the collector schema. Building identity governance collectors that use the existing enterprise service bus allowed data to pass securely between systems and enabled automatic onboarding of applications with similar account and permission mapping needs.

The successful connection to 200 databases was still only scratching the surface–hundreds of high-risk applications and thousands of additional in-scope applications were next to meet CMMC compliance. Using this proven design, the work continues to identify application types successfully integrated previously and applications with similar data models for quick onboarding. Shifting this mapping exercise to the application owners focuses on the experts best suited to provide the information. Additionally, sharing the efforts with application teams allows a faster deployment than if the IG team connected one application at a time.

The PAM Imperative

The DoD contractor chose to implement a privileged access management (PAM) solution, CyberArk, to store and track the usage of privileged account credentials. With so many elevated privileges, this system became management's next target for access review and certification.

Although no CyberArk collector is available out of the box, NetIQ Identity Governance contains an SDK for writing custom collectors and fulfillers for any system. TriVir assisted the DoD contractor with creating a custom collector for CyberArk to gather the system's different account and permission types. The organization's CyberArk system contained both internal CyberArk accounts and Active Directory accounts from the local domain. CyberArk uses "safes" to store credentials and access information, and permissions to the safes are configured separately. Both permissions sets needed to be cataloged to understand who had what kind of access to a particular safe and what kind of access to what was stored in the safe.

Once both types of accounts and permissions were imported, reviews of who has access to which safes and who has access to privileged accounts for enterprise apps were configured. This consolidation of administrative and privileged account information both simplified and greatly improved the organization's security.

“We have worked with the NetIQ suite of identity and access management solutions for the last 20 years and felt NetIQ Identity Governance ticked all required boxes. We introduced it in a proof-of-concept (POC) and beat the other vendors in the mix.”

Brent Kynaston
Solutions Architect
TriVir

Contact us at **CyberRes.com**
Follow us on Social Media.

The Sweet Smell of Success

Brent Kynaston, TriVir Solution Architect, describes the success experienced so far: “The system owners tell us emphatically how much better their user experience is with the full automation of identity governance. They no longer need to respond to cumbersome and time-consuming queries about what entitlements are assigned within their applications, who has assigned them, and why. Instead, internal and external auditors log onto a user-friendly enterprise portal where they can run specific reports that provide all the required data.”

Jim Montgomery explains how TriVir helped the DoD contractor meet CMMC compliance regulations: “This particular DoD contractor manages tens of thousands of identities, covering thousands of applications, including financial solutions containing very sensitive data. Implementing NetIQ Identity Governance accelerated progress toward meeting CMMC requirements by automating the onboarding of so many applications quickly and simplified the administrative burden of governance across the organization, which was a huge positive paradigm shift.”

This rapid deployment facilitated the complete audit and access review process for more applications than had ever been reviewed before. More importantly, the first review and access certification removed many erroneous existing accesses, resulting in significant zero trust progress toward least-privilege access. It was estimated more than 3000 hours were saved by eliminating manual data sampling, spreadsheet review, and email communication. The success of this program has enabled CMMC compliance and opened the door to continue adding thousands of additional applications.

About NetIQ

NetIQ provides security solutions that help organizations with workforce and consumer identity and access management at an enterprise scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage to learn more. Watch video demos on our NetIQ Unplugged YouTube channel.

NetIQ is part of CyberRes, a Micro Focus line of business.

TriVir | CyberRes
A Micro Focus Line of Business