



CASE STUDY:

Providing unparalleled
100% cloud asset
inventory for a global
financial enterprise

INDUSTRY: ESTATE MANAGEMENT

About the client

The client is a global financial services enterprise with a large, distributed technology footprint spanning multi-cloud and on-premises environments. As a data intensive organization operating under strict regulatory oversight, it manages thousands of applications and cloud resources across diverse business units.

Rapid cloud adoption and decentralized development practices accelerated the growth of its asset estate, making real time visibility essential for security and compliance. The organization required a scalable approach to establish a complete and authoritative inventory of its cloud assets without slowing innovation.

Client challenge

Our client faced a foundational obstacle: obtaining a complete and accurate view of its cyber asset estate. The shift from physical data center infrastructure to dynamic cloud architectures had introduced significant complexity. Unlike traditional assets that are procured, installed, and easily tracked, cloud resources are dynamic and ephemeral in nature. Virtual machines, load balancers, storage instances, and serverless components can be provisioned and terminated in minutes, leaving security teams without a reliable, real-time source of truth. This challenge mirrors broader industry patterns, where cloud assets proliferate too quickly for manual or legacy processes to manage effectively.

The organization's existing configuration management database (CMDB) captured only an estimated 70% of assets, reflecting the inherent limitation of periodic, point-in-time updates. While the CIO regarded the CMDB as authoritative, the CISO recognized widening blind spots as developers created cloud resources that never entered formal inventory. As a result, security teams could not depend on the CMDB or on traditional security tools, which often discover only a subset of asset types or focus on the most common services rather than the full cloud asset estate.

The rise of AI and machine learning introduced additional blind spots, as agents, model training infrastructure, MCP servers, and GPU-accelerated compute environments were often deployed rapidly and outside established governance processes. These high-cost, high-risk AI assets frequently lacked consistent tagging and inspection, further widening the visibility gap.

To address this, the enterprise needed a solution capable of discovering 100% of cloud assets and classifying each as managed, unmanaged, or suspicious. This required correlating telemetry from best-of-breed security tools, reconciling inconsistencies across data sources, and accounting for more than 200 distinct cloud asset types on platforms like Google Cloud, far exceeding what most vendors supported.

Benefits



Elimination of security blind spots: Improved hygiene and visibility enabled the identification of unknown assets in the environment, resulting in their reclassification from suspicious to managed in the cyber asset estate. This improved hygiene is vital to ensure security controls are implemented for all assets.



Reduced attack surface: Comprehensive discovery and classification enabled the organization to eliminate unmanaged and suspicious assets including unknown assets and shadow IT, materially shrinking the cloud attack surface.



Stronger regulatory posture: An authoritative, real time asset inventory improved audit readiness and strengthened compliance with financial-sector security and governance requirements.



Higher operational efficiency: Automated reconciliation and enriched context reduced manual investigation cycles, allowing security teams to focus on high-value risk reduction rather than inventory **correction**.



Business-aligned risk prioritization: Tag-driven context ensured that exposures affecting critical customer-facing platforms were elevated immediately, aligning remediation with business impact and reducing service disruption.

Our solution

CyberProof deployed a cybersecurity estate management approach designed to establish a complete and authoritative inventory of the client's cloud assets. The first step focused on comprehensive asset discovery across Google Cloud. While most security tools capture only a subset of common resource types, our solution includes connectors to ingest all ~200 native Google Cloud asset types, ensuring full visibility across the cloud asset estate. This depth of coverage differentiated the solution, overcoming a core industry limitation in cloud-asset inventory accuracy.

The platform then integrated with key security tools to determine the management state of every asset. Using direct plugins for vulnerability management and CSPM tools, the system automatically classified each asset into managed, unmanaged, or suspicious categories. Managed assets had at least one active inspector. Unmanaged assets had no inspection coverage, signaling potential security gaps. Suspicious assets represented discrepancies between primary and secondary sources, such as instances identified by a vulnerability management tool but not present in Google Cloud's authoritative asset inventory, an indicator of shadow IT or misconfigurations that required investigation.

To support meaningful prioritization, the solution overlaid business context onto the asset inventory. By leveraging the cloud provider's tagging structure, assets were enriched with application, ownership, environment (development, test, production), and other metadata such as business unit or geography. This allowed security teams to distinguish between unmanaged assets supporting critical customer-facing platforms and those tied to lower-risk internal applications, aligning remediation efforts with business impact.

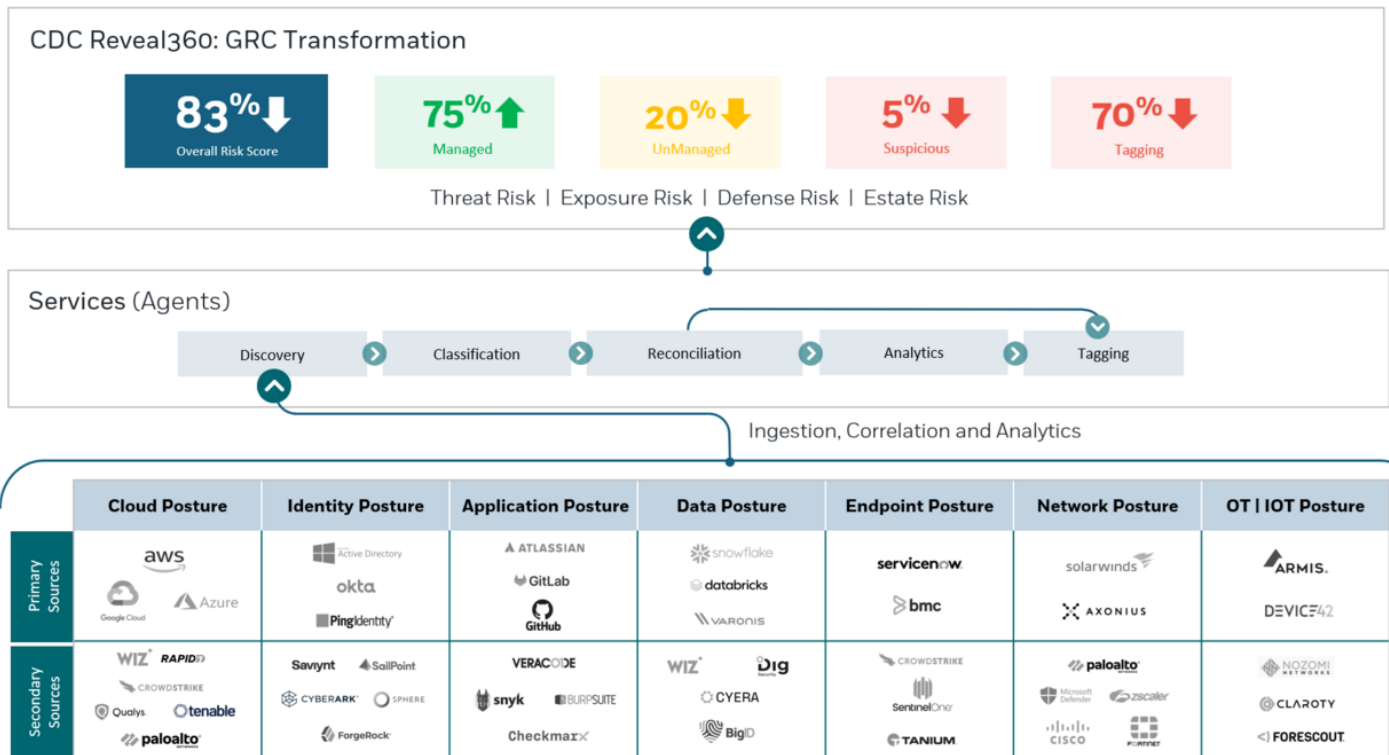
The extensible design of the platform enables rapid onboarding of new asset classes, including AI-related infrastructure such as agents, MCP servers, GPU clusters, and model-serving platforms. This future-focused capability ensures the client can maintain full visibility and control as AI adoption accelerates and new, compute-intensive services enter the environment. While the cybersecurity estate management platform does not replace existing CMDBs, it enriches CMDBs by sitting on top of these platforms to perform full asset discovery and classification.



Results and next steps

The initiative delivered full visibility across the client’s cloud estate, achieving 100% coverage of all ~200 GCP asset types and establishing a complete, authoritative inventory. Integration with Qualys and CSPM brought 95% of assets under active management, with fewer than 1% identified as suspicious and the remaining assets classified as low-risk unmanaged resources. Automated reconciliation between GCP and security

tools eliminated blind spots, surfaced previously unknown assets, and enabled rapid remediation, including agent deployment and decommissioning of unused resources. By enriching assets with business context, the client strengthened risk-based prioritization and improved the speed and accuracy of compliance reporting.



About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: www.cyberproof.com.

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum