How VRA Built the Security Foundation for Safe AI Adoption: Volta River Authority (VRA) Microsoft Security Implementation Case Study

Before there was a dashboard, a policy, or a protection layer, there was a pressure that Ghana's power utility could no longer ignore.

Volta River Authority has kept Ghana's lights on for decades. VRA is not just an energy company, it is critical national infrastructure, and it carries that weight in everything it does.

But a different kind of vulnerability had quietly grown beyond what workarounds could manage. The grid was resilient. The data estate was not.

VRA faced three converging pressures:

- **Invisible data:** Outside structured ERP systems and databases, the organization's unstructured data, documents, emails, shared files, engineering correspondence, moved freely and invisibly. No classification. No labelling. No monitoring. Nearly 65% of sensitive data existed in a blind spot no tool could see.
- **Compliance drag:** Audit and regulatory reporting consumed up to 10 full working days of manual effort per cycle, pulling records from disconnected systems, reconciling inconsistencies, and submitting reports that leadership could never fully stand behind.
- **A blocked AI roadmap:** VRA had identified Microsoft 365 Copilot as a strategic priority. But every conversation about rolling it out hits the same wall: one cannot safely deploy AI across a data estate you cannot see, classify, or control.

Security as a Foundation, Not an Afterthought

VRA brought this challenge to INFINION with a clear mandate: build the security and governance foundation that the organization needed not just to protect what it had, but to safely adopt what was coming.

INFINION structured a precise, time-bound engagement to assess VRA's current-state posture, validate Zero Trust-aligned controls, and deploy a comprehensive Microsoft security framework across five interconnected domains: Identity, Device and Endpoint, Data and SaaS, Detection and Response, and end-to-end Validation.

The Build

- **Microsoft Entra ID + PIM**

The team configured MFA enforcement for all pilot users and validated successful challenge flows. INFINION designed and deployed Conditional Access baselines to require compliant devices, enforce MFA, and block legacy authentication protocols that had previously left the environment exposed.

INFINION implemented Privileged Identity Management with instant role elevation, approval workflows, time-bound access expiry, and Access Reviews for privileged roles. No standing access. No unchecked privilege. Every sensitive action logged and accountable.

- **Microsoft Intune + Defender for Endpoint**

INFINION onboarded 5–15 pilot Windows devices to Microsoft Intune and Defender for Endpoint and implemented compliance policies across OS version, BitLocker encryption, antivirus, and firewall configuration. Devices that failed to meet the compliance bar automatically lost access to corporate resources.

INFINION enabled EDR in block mode, while Attack Surface Reduction rules protected against credential theft and ransomware. After the team validated automated remediation, VRA moved endpoint security from reactive defense to proactive protection.

- **Microsoft Purview Information Protection**

INFINION defined and deployed a sensitivity label taxonomy across VRA's Microsoft 365 environment: Public, Internal, and Confidential. The team configured labels with both manual and automatic classification rules, so the system identified and tagged data whether or not users remembered to do it. Coverage extended across Exchange Online, SharePoint, and OneDrive.

The impact was immediate. VRA identified, classified, and brought 65% of its previously invisible sensitive data under active governance.

- **Microsoft Defender for Cloud Apps**

VRA had cloud applications in use across the organization that IT had neither approved nor reviewed.

The team enabled Cloud App Discovery to surface every application operating beneath the line of sight. INFINION assessed discovered applications against risk criteria, sanctioned or unsanctioned them, and brought them under governance controls. For the first time, VRA had a complete, enforceable picture of its cloud application estate.

- **Microsoft Sentinel + Defender XDR**

INFINION onboarded logs from Identity, Endpoint, and Microsoft 365 sources into Log Analytics and Microsoft Sentinel. The team deployed analytics rules for key identity and endpoint threats and enabled incident correlation across workloads, so VRA no longer managed a suspicious sign-in, a DLP alert, and an endpoint anomaly as three separate events in three separate consoles. Microsoft Sentinel surfaced them as one incident, and SOAR playbooks guided the response: disable user, isolate device, contain threat.

Unified incident management through Defender XDR gave VRA's security team the consolidated visibility they had never had before.

The Impact (At a Glance):

- Sensitive data visibility: near zero → 65% of previously hidden data now governed
- Compliance reporting time: 10 days (uncertain) → 6 hours (with certainty)
- Sensitive data identification response time: 4–5 working days → under 1 hour
- Data exposure incidents and policy violations: 45% reduction
- IT and compliance team time spent on manual governance tasks: 45% saved
- Annual third-party security vendor spends: $180,000 USD → $300,000 USD in annual savings
- Legacy vendor stack: 100% retired
- Secure AI adoption timeline: accelerated by 45%