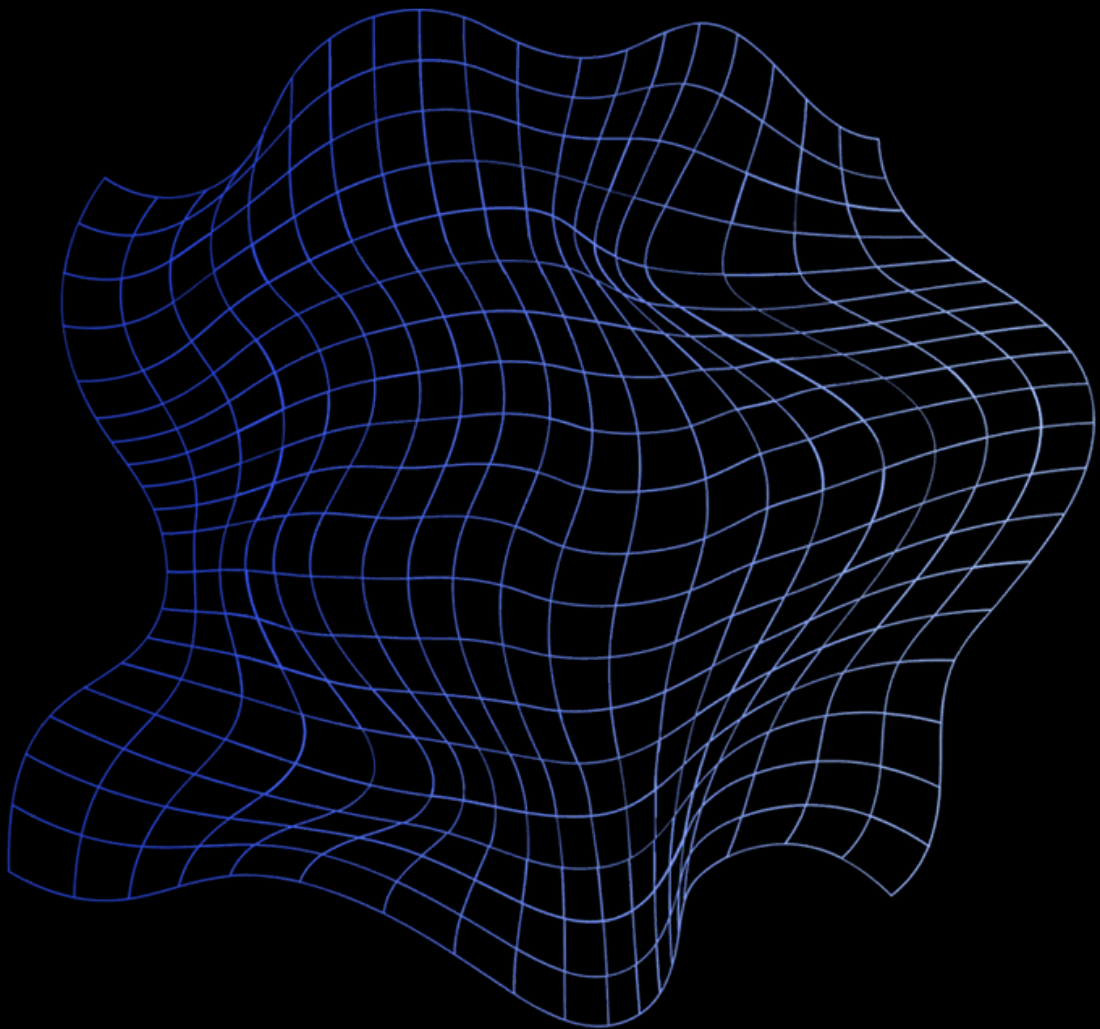
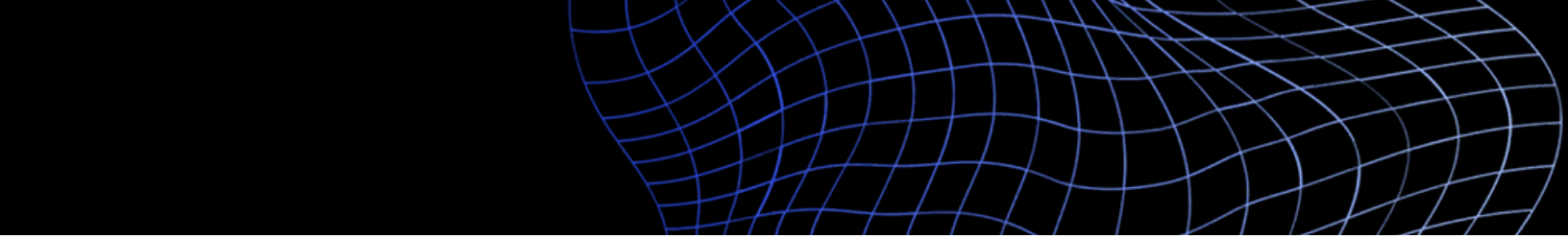
HELIXSTORM

Modernizing a Government Agency's IT Infrastructure from the Ground Up

How Helixstorm turned a third-party audit into a comprehensive engineering redesign for Sunline





Background

Helixstorm was engaged by a Sunline, a government agency, as part of a competitive IT consulting award. The engagement began with a thorough audit of the agency's existing IT ecosystem — a process that quickly revealed not just isolated issues, but systemic gaps spanning security, infrastructure, data protection, and operational efficiency. What started as an assessment became the foundation for a multi-project engineering redesign effort.

The Challenge

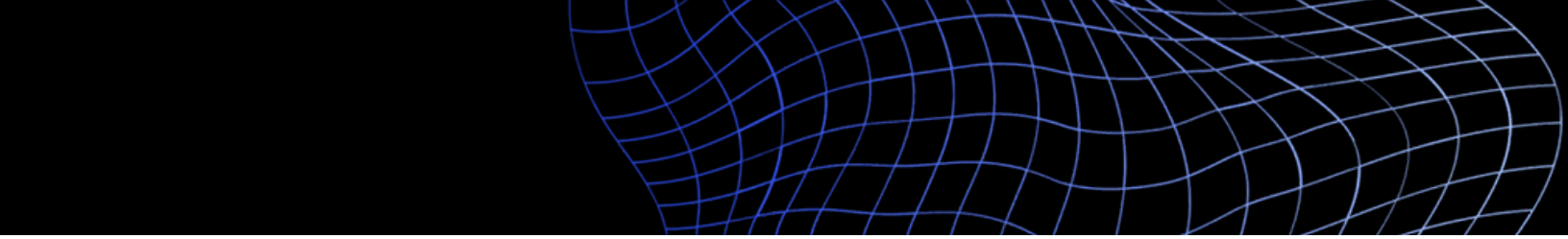
The audit uncovered a wide range of critical vulnerabilities and inefficiencies. The agency's Active Directory environment was poorly designed and running on aging hardware, with no cloud authentication capability to fall back on in the event of a ransomware attack or regional disaster. Multi-factor authentication and conditional access policies had never been implemented. The on-premises Exchange platform was approaching end of Microsoft support. File servers were being used to store end-user data with no modern recovery path. An HPE hyperconverged infrastructure platform that had been acquired as a disaster recovery solution sat in the operations building, never fully deployed.

Sunline was operating with multiple silos of servers and storage running different versions of Hyper-V, creating a fragmented environment with no unified approach to backup or business continuity. These weren't edge cases — they were structural issues that left the agency exposed.

Why Helixstorm

Helixstorm was selected through a formal competitive procurement process, giving the agency confidence that they were working with a vetted partner capable of operating at the scope and complexity the engagement required. But the selection was more than procedural. The audit itself served as a proving ground: Helixstorm's ability to conduct a thorough, credible assessment of a complex IT environment — and to translate those findings into a clear, sequenced remediation plan — demonstrated exactly the kind of technical depth and strategic thinking the agency needed. When the audit recommendations pointed toward a major redesign effort, there was no reason to look elsewhere. Helixstorm’s differentiators also came into play, including:

- Security first to keep your company protected
- White glove dedicated service managed that is hyper-focused on you and your company
- Dugeting and strategy planning with a roadmap on how to achieve your best case scenario
- The company is not owned by a private equity firm - we report to our customers, not shareholders



The Solution

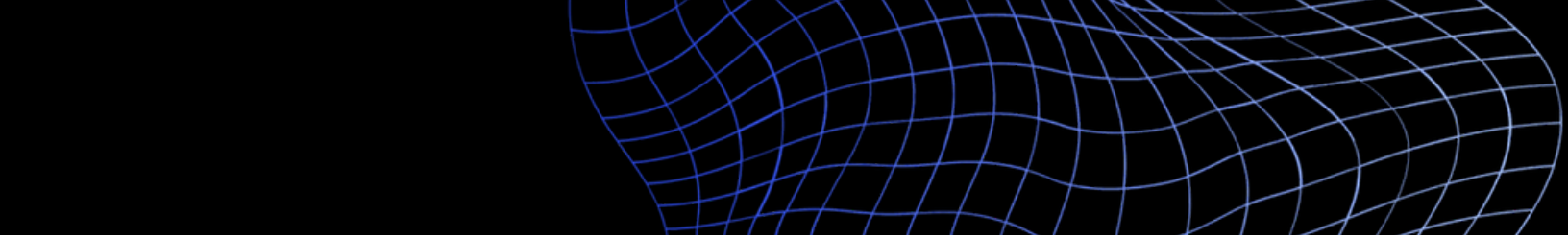
Helixstorm proposed three interconnected engineering redesign projects, sequenced deliberately so each one built on the last.

The first — and foundational — project was a Microsoft Tenant Security overhaul. Before any migration of applications or data could happen, the agency's security posture needed to be rebuilt. This meant upgrading Domain Controllers to Microsoft's latest editions, remediating Active Directory's configuration and design, and integrating with Microsoft Entra to establish cloud authentication capability. This work also created the structure for conditional access policies and MFA deployment, closing one of the most significant gaps identified in the audit.

With the security foundation in place, Helixstorm turned to migrating Exchange, OneDrive, and Teams to Microsoft 365. The agency's on-premises Exchange 2019 platform was approaching end of support — after October 14, 2025, it would receive no further security updates or technical support from Microsoft. Moving to Microsoft 365 not only resolved that risk but eliminated ongoing operational overhead, improved end-user productivity, and removed the need for the agency to manage its own data protection and business continuity requirements for email.

The OneDrive migration addressed a separate but related vulnerability: end-user data was being redirected to file servers on the agency's network — prime targets for ransomware — with no modern recovery path. Moving that data to OneDrive provided automatic syncing, Microsoft's enterprise-grade encryption, and a clean recovery process in the event of a workstation compromise. The Teams migration followed the same logic, replacing exposed network file systems with a governed, structured collaboration environment with channel-based access controls and the ability to use Power Automate to manage file distribution across departments.

The third project tackled the agency's compute and storage environment. Helixstorm proposed leveraging the existing HPE disaggregated hyperconverged infrastructure — the platform that had been purchased but never deployed — as the foundation for a full consolidation of the agency's servers, storage, and applications. Replacing Hyper-V with VMware across a unified HPE platform eliminated the multi-silo complexity, enabled one-click infrastructure upgrades to reduce maintenance windows, and created a significantly more capable foundation for disaster recovery. Backup operations became more efficient, and the consolidated platform opened up a wider range of business continuity solutions that weren't viable in the fragmented prior environment.



Results

The three projects together addressed every major finding from the original audit: security posture, legacy systems, end-user productivity, data protection, and the incomplete prior deployment. Rather than treating each issue in isolation, Helixstorm's sequenced approach meant each project reinforced the next — the security foundation enabled the migrations, and the migrations cleared the way for a cleaner, more resilient infrastructure layer underneath.

The agency moved from a fragmented, reactive IT environment to one with modern authentication controls, cloud-based productivity tools, and a consolidated virtualization platform designed for long-term supportability and recovery.

Looking Ahead

The engineering redesign positions the agency to operate with significantly reduced risk and complexity going forward. With the foundational work complete, future improvements — additional cloud migrations, expanded security policies, enhanced disaster recovery testing — can be implemented on a stable, well-documented platform rather than around legacy constraints.