SoftServe / Fortified HEALTH SECURITY

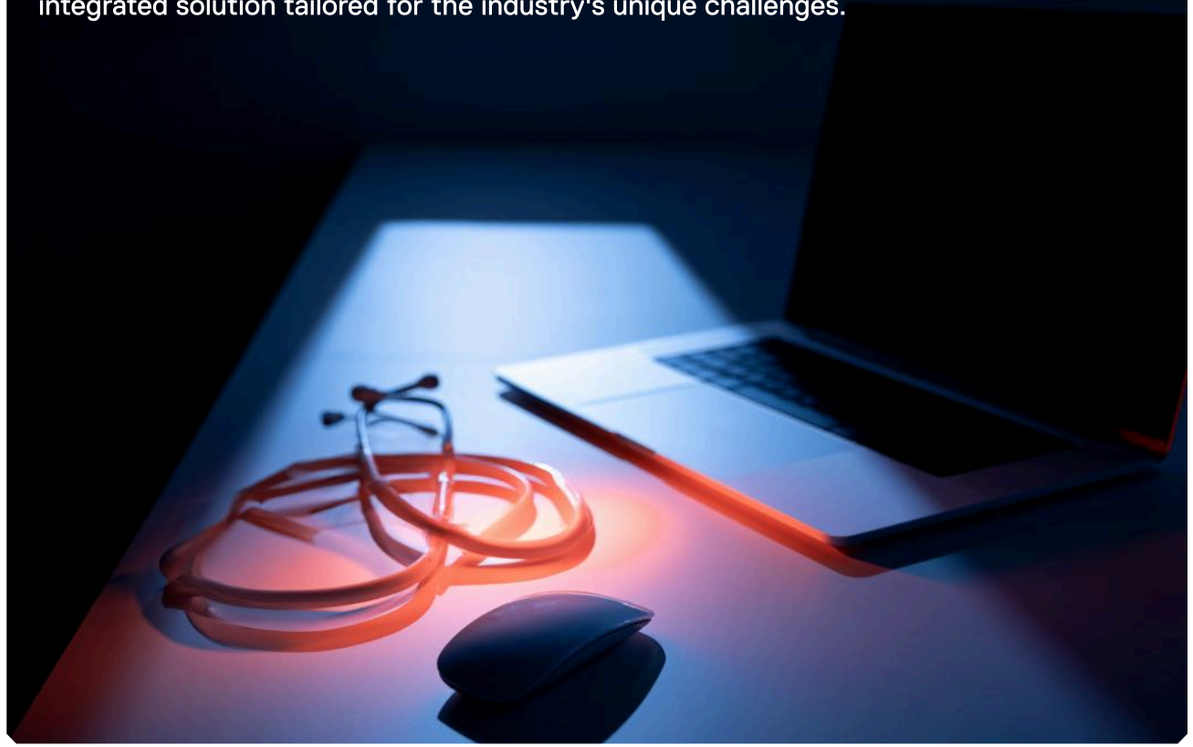
CASE STUDY

BUILDING CENTRAL COMMAND:

How Fortified Health Security Transformed Healthcare Security Operations

At a Glance:

SoftServe partnered with Fortified Health Security to develop Central Command, a unified platform that transformed how healthcare organizations manage and view cybersecurity. This collaboration combined technical expertise with healthcare security knowledge to deliver an integrated solution tailored for the industry's unique challenges.



Fortified Health Security, a top-ranked MSSP specializing in healthcare cybersecurity, recognized a market challenge. Their healthcare clients managed multiple cybersecurity services across various platforms, with data trapped in silos. This fragmentation prevented organizations from gaining comprehensive visibility into their security posture, understanding risk levels across different categories, and tracking progress over time.

Fortified recognized that truly serving their clients and differentiating themselves in the competitive MSSP market required transformation. They envisioned a unified platform where clients could access all cybersecurity services in one place, visualize their security posture across multiple dimensions, conduct comprehensive risk assessments, communicate with security analysts, and track their security journey over time. This platform needed to handle massive data volumes, integrate seamlessly with multiple third-party cybersecurity products, meet the highest security standards, and provide an intuitive user experience for users with varying technical expertise.

For Fortified, a company focused on delivering managed security services rather than building software products, this ambitious initiative required the right development partner who could build technology while implementing industry-leading software development practices.

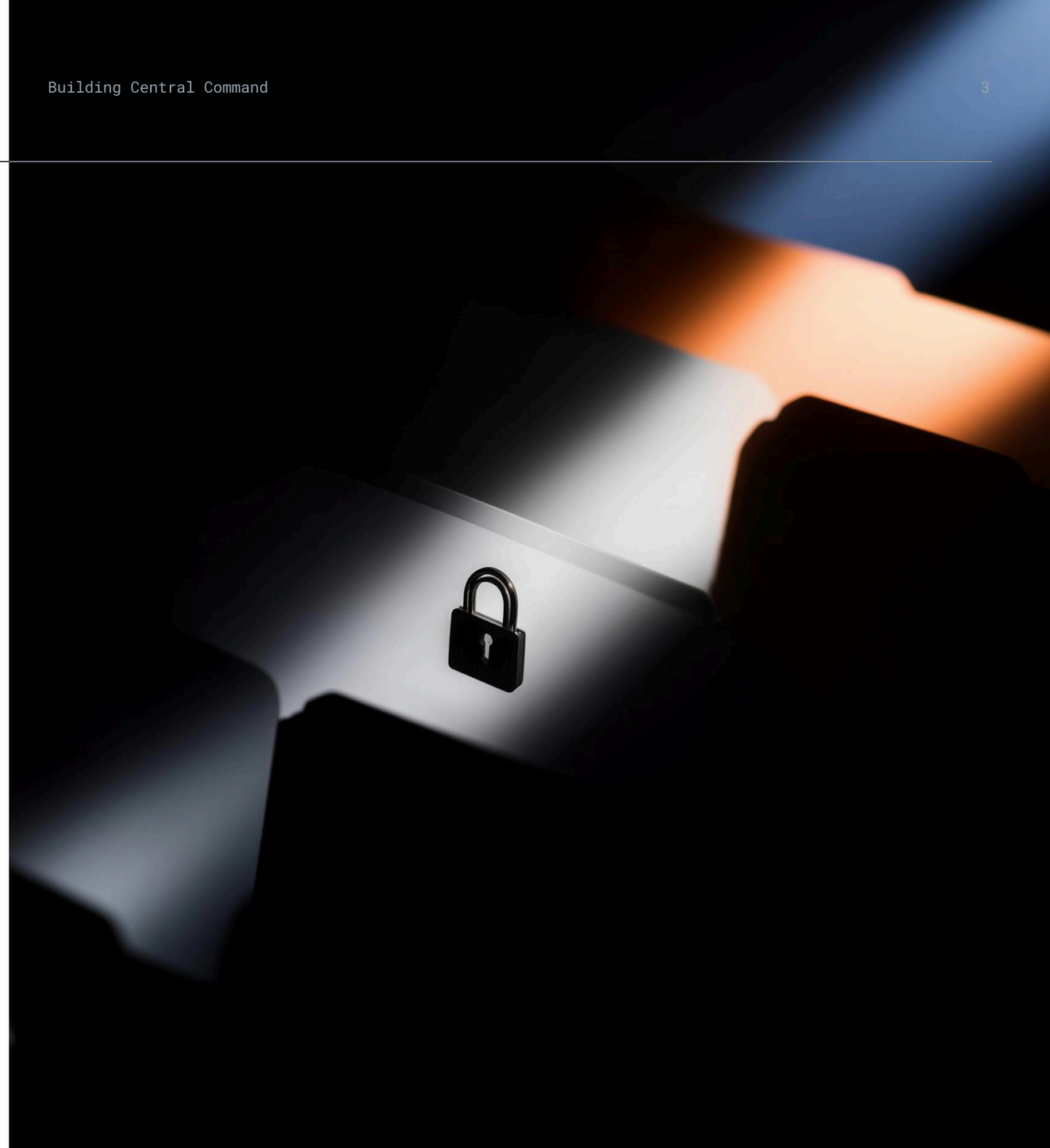
Establish Full Lifecycle Ownership

Fortified made an early decision that shaped everything: before a single line of code was written, they invested two months in Discovery. That choice proved decisive. Working from the inside out — their business model, their clients' needs, the specific pressures of healthcare cybersecurity — Fortified emerged with a clear roadmap, a validated user experience vision, and full alignment on scope and cost.

From there, Fortified stood up a cross-functional team of twelve covering product ownership, development, quality assurance, CI/CD, and project management. Rather than hand off responsibility to a vendor, they structured the engagement for full lifecycle ownership — requirements through architecture, data, DevOps, and specialist integrations including Salesforce — accountable end-to-end from initial charter through deployment and beyond.

Agile delivery with two-week sprints gave Fortified something critical in a competitive market: the ability to respond. New demands, shifting priorities, aggressive timelines — the iterative cadence meant Fortified could act on feedback without losing momentum.

As Central Command grew in scope, so did the team. By beta launch in June 2021, thirty professionals across two Scrum teams were building the platform. Fortified had structured a partnership that could scale with them — and it did.



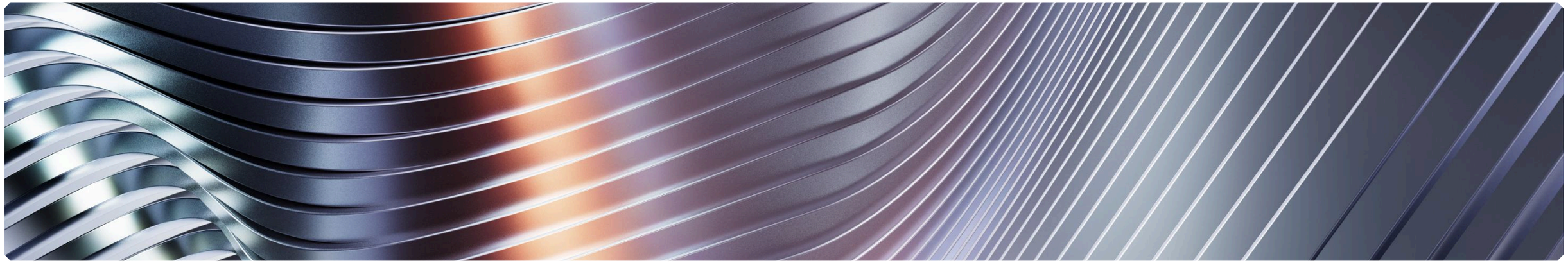
Enterprise-Grade Technology Architecture

Fortified Central Command emerged as a sophisticated web-based platform built on robust AWS cloud infrastructure. The technology stack reflected both current best practices and forward-looking architecture decisions that would support Fortified's growth for years to come.

The platform leveraged an extensive AWS ecosystem including Lambda for serverless computing, Redshift for data warehousing, RDS for relational database management, and S3 for scalable storage. For real-time data processing, the team implemented AWS Kinesis and Kafka, enabling the platform to handle data pipelines processing up to 500 gigabytes consistently. The infrastructure design emphasized auto-scaling capabilities, ensuring the platform could grow seamlessly with Fortified's expanding client base.

Security architecture received particular attention, befitting a platform designed for cybersecurity professionals. The development team implemented multi-factor authentication through Duo, single sign-on capabilities through AWS Cognito, and robust role-based access control that satisfied the principle of least privilege. The platform's architecture incorporated tenant management, allowing Fortified to serve multiple clients while maintaining strict data separation and security.

The backend infrastructure utilized Python with the Flask framework, incorporating libraries like SQLAlchemy for database interactions, pandas for data analysis, and Plotly for creating dynamic visualizations. The frontend leveraged React with TypeScript, providing a responsive and intuitive user interface built with components from Material-UI and data visualization through Highcharts.

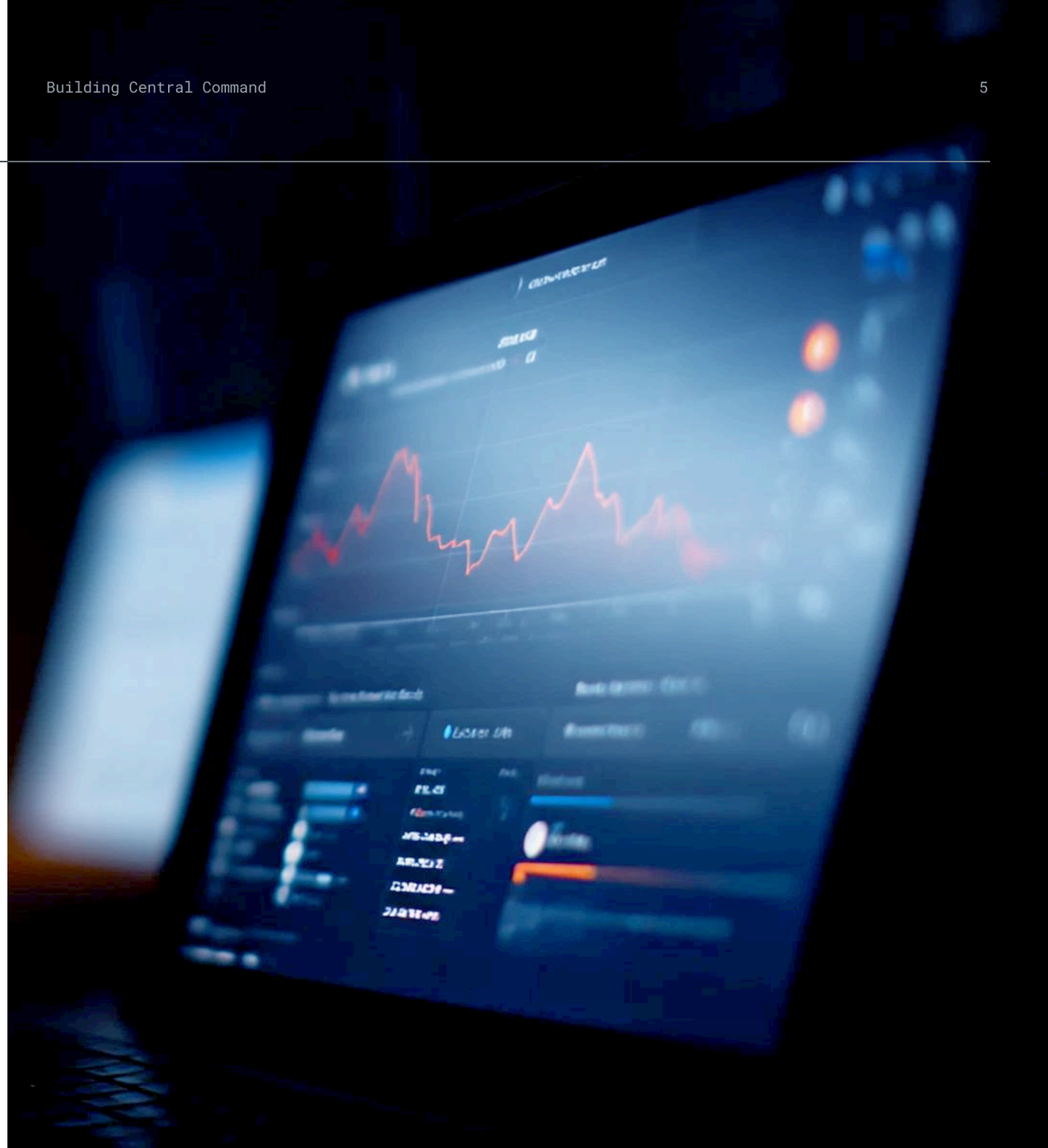


The platform's native data warehouse, purpose-built for analytics, enabled Fortified to provide clients with trending dashboards, comparative analytics showing monthly progression, and detailed views into specific risk areas. Clients could see their security posture across multiple categories, compare their performance against industry benchmarks, and identify the highest-risk action items requiring attention.

The platform transformed Fortified's Risk Assessment process by integrating all communication tools and creating an ongoing Risk Register accessible within a single interface. Clients could participate in comprehensive risk assessments, track findings over time, collaborate with Fortified's analysts through built-in communication tools, and monitor remediation progress.

SoftServe implemented best practices beyond the code itself. The team established a complete DevOps practice with comprehensive continuous integration and deployment pipelines. They built infrastructure with auto-scaling capabilities, implemented business continuity and disaster recovery procedures, and created distinct Software Development Lifecycle environments for development, testing, staging, and production.

The platform underwent an independent AWS Well-Architected Review, validating that the infrastructure met Amazon's highest standards for operational excellence, security, reliability, performance efficiency, and cost optimization. This review provided both Fortified and their clients with confidence that Central Command was built on a solid foundation. The team also integrated SonarQube for continuous code quality monitoring, Google Analytics for data-driven decision making, and developed comprehensive user guides with RoboHelp for seamless navigation.



Recognition and Results

The results extended beyond technology metrics. Central Command fundamentally changed how Fortified engaged with both prospective and existing clients.

For sales and marketing, the platform became a powerful differentiator. Fortified demonstrated their capabilities through a highly functional, modern portal that showcased their commitment to transparency and client empowerment. This capability helped Fortified maintain their position as a Best in KLAS award winner for Security and Privacy Managed Services continuing five straight years from 2022-2026. The company also earned global recognition in MSSP Alert's Top 250 MSSPs, continued to be recognized as one of Modern Healthcare's Best Places to Work. They received Cybersecurity Breakthrough awards for Central Command 2024 Cybersecurity Solution of the Year and 2025 Managed Security Innovation of the Year.

The platform's executive dashboard gave healthcare leaders unprecedented visibility into their cybersecurity posture. Rather than reviewing static reports, executives accessed live data visualizations showing metrics, escalations, and vulnerabilities across all cybersecurity areas. The comparative analytics feature allowed them to track their organization's security maturity over time and benchmark progress against industry standards.

For Fortified's security analysts, Central Command provided tools to increase efficiency and effectiveness. The platform tracked each analyst's interactions within the system, providing visibility into workload distribution and enabling better resource allocation. The integrated communication tools meant analysts could respond to client questions and concerns without switching between multiple systems.

The platform's scalability proved crucial as Fortified continued to grow. The infrastructure expanded to accommodate new clients, additional services, and increasing data volumes without performance degradation. The multitenancy architecture meant each client's data remained isolated and secure while Fortified managed everything through a unified infrastructure.

Cost optimization received ongoing attention throughout the engagement. SoftServe implemented tagging for each AWS service, enabling detailed cost tracking and monthly monitoring. The team continuously optimized the infrastructure to balance performance requirements with cost efficiency, ensuring Fortified could scale economically as their business grew.

Beyond direct platform capabilities, the project helped Fortified build a data-driven culture. The native data warehouse and analytics capabilities allowed Fortified to make strategic decisions based on concrete data rather than intuition, influencing their organizational strategy and informing specific business cases for new services and capabilities.

Building for the Future

From Discovery in September 2019 through the platform's market launch in April 2023 and the continued advancement, Fortified and SoftServe demonstrated sustained excellence across nearly four years of collaboration. The partnership continues today, with ongoing enhancements, optimizations, and new capabilities being added to Central Command.

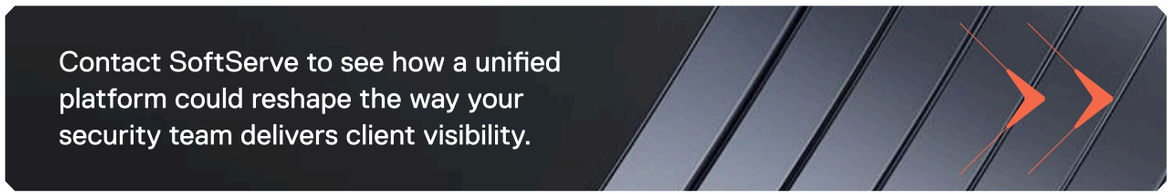
> “The consistent, focused delivery on Central Command was an essential part of our success. Every single team member contributed so much effort and exceeded our expectations. We are truly thankful for the partnership at every touch point.
>
> — Craig Badcock (Vice President, Product Development).

This engagement illustrates key principles that SoftServe brings to strategic partnerships. Full lifecycle ownership means clients have a single partner accountable for outcomes rather than coordinating multiple vendors. Embracing the client's business context ensures technical decisions align with business objectives. Implementing industry-leading practices helps service-focused organizations compete effectively in product markets. Scaling thoughtfully as needs evolve maintains quality while adding capability.

For healthcare organizations working with Fortified Health Security, Central Command represents more than a technology platform. It represents a commitment to transparency, collaboration, and continuous improvement in the cybersecurity ecosystem posture. For Fortified, it is a competitive differentiator that reinforces their position as a leader in healthcare cybersecurity.

Healthcare cybersecurity is constantly changing, with new threats emerging and regulatory requirements becoming more stringent. With Central Command as their foundation and SoftServe as their development partner, Fortified Health Security continues to lead the industry in protecting patient data and strengthening healthcare cybersecurity.

Contact SoftServe to see how a unified platform could reshape the way your security team delivers client visibility.



SoftServe | Fortified HEALTH SECURITY

About SoftServe

SoftServe is a premier IT consulting and digital services provider. We expand the horizon of modern technologies to solve today's complex business challenges and achieve meaningful outcomes for our clients.

Social Links

info@softserveinc.com
www.softserveinc.com

Contact

NORTH AMERICAN HQ

201 W 5th Street, Suite 1550
Austin, TX 78701
+1 866 687 3588 (USA)
+1 647 948 7638 (Canada)

EUROPEAN

30 Cannon Street
London EC4 6XH
United Kingdom
+44 333 006 4341