DEEPWATCH™
Always Watching. Always Protecting.™

CUSTOMER SUCCESS STORY

# How a High-Growth Financial Services Organization Scaled Cyber Defense Across a Large, Distributed Enterprise

"Deepwatch gives us the 24×7×365 vigilance we simply couldn't achieve on our own. Without it, we'd need to triple our team."

— Director of Cybersecurity, Financial Services

## CHALLENGE

**Unifying a Fragmented Security Landscape**

The security program was rebuilt as the organization transitioned from a smaller MSSP to one capable of supporting enterprise-level complexity. The director inherited an environment with:

- Disparate logging sources across numerous business entities.
- Limited historical tuning or visibility into detection efficacy.
- High alert volume and inconsistent configurations.
- Strict partner and regulatory expectations, including alignment to NIST.
- A team too small to provide continuous monitoring.

The previous vendor lacked the flexibility to support the organization's unique Splunk deployment, and running a fully staffed, in-house SOC was not feasible.

***"We support thousands of users across many independently operated organizations, each with different environments. Bringing all that into a standard is a massive lift."***

—Director of Cybersecurity, Financial Services

## ENTERPRISE DETAILS

**Industry:** Financial Services

**Employees:** 5,000 to 10,000

**Security Team Size:** Lean internal team

## SOLUTION

**A Scalable MDR Platform Built for Complexity**
The organization selected Deepwatch for its adaptability, ability to support a highly customized SIEM environment, and operational maturity. Deepwatch quickly established a standardized foundation for detection and response across the enterprise.

**A Unified, Normalized Security View**
Deepwatch's ingestion and normalization of diverse log sources brought consistency to a previously fragmented environment.

**Tier 1 SOC that Reduces Noise**
Deepwatch's SOC delivers fully enriched, actionable alerts, enabling the internal team to focus on validation and response rather than triage.

**Extensive Tuning & Customization**
During onboarding and expansion, Deepwatch collaborated closely with the customer to tune detection rules and refine data sources, strengthening accuracy and reducing noise across the distributed environment.

**Reliable 24×7×365 Coverage**
The organization relies on Deepwatch for constant monitoring and escalation, enabling sustainable work-life balance for internal staff.

***"Deepwatch allows us to disconnect after hours with confidence. We know our environment is being monitored."***

**Trusted by Auditors and Insurance Partners**
As the organization works with major financial providers and must meet strict controls, MDR coverage from an industry-recognized provider strengthens their compliance posture.

***"Auditors consistently view Deepwatch as a strong MDR solution and a positive answer."***

**Forward-Looking AI Strategy**
The customer is actively exploring Deepwatch NEXA™ as part of their long-term SOC modernization roadmap.

***"The future of SOC operations is AI-driven. We're eager to see how Deepwatch continues integrating natural-language search and intelligent automation into the platform."***

DEEPWATCH™

## OVERVIEW

**Driving Security at Enterprise Scale, Without Enterprise Headcount**

A national financial services organization supporting thousands of users across a broad portfolio of independently operated businesses needed a scalable, unified approach to cyber defense. Years of growth through acquisition created a complex, inconsistent security landscape, each business carrying its own technology stack, legacy systems, and risk.

With a lean cybersecurity team, the organization needed an MDR partner capable of cutting through noise, normalizing log data across disparate environments, and delivering reliable 24×7×365 coverage.

Deepwatch provided the operational scale, stability, and consistency the customer needed to manage overwhelming log volumes, gain unified visibility, and ensure dependable 24×7×365 monitoring across a highly distributed environment.

## CUSTOMER TESTIMONIAL

**“Deepwatch lets a small team operate like an enterprise-grade SOC. The 24×7x365 vigilance, the detailed triage, and the partnership, there’s no vendor more critical to our security posture.”**

—Director of Cybersecurity, Financial Services

## CYBER OUTCOMES

**Avoided Hiring Additional Security Analysts**
To match Deepwatch’s 24×7×365 coverage and triage capabilities, the organization estimates it would need to more than triple its security staff.

**Estimated cost avoidance:**
Avoided hiring multiple additional SOC analysts (~$150K average cost per analyst) equates to approximately **$1.05M annually.**

**Noise Reduction & Faster Triage**
Deepwatch’s detailed investigations and tuning efforts dramatically reduce internal workload, eliminating unnecessary cycles and sharpening focus on true issues.

**Ability to Prioritize Strategic Initiatives**
With Deepwatch managing MDR, the internal team now directs attention to higher-value security improvements, including:

- Enterprise password manager deployment.
- Microsoft Defender tuning.
- Email security enhancements.
- Standardizing and maturing internal security tooling.

***“Deepwatch frees our team to focus on improving the broader security posture of the business.”***

**Strengthened Audit & Partner Confidence**
Deepwatch’s MDR coverage and Splunk integration provide credibility and assurance across audit conversations, reducing friction and strengthening trust with upstream partners.

**A Sustainable Modern SOC Operating Model**
With limited internal staff, the organization emphasizes that Deepwatch is irreplaceable to their security posture.

***“Deepwatch is the most critical vendor we have. No other partner is more important to our security strategy.”***

**Future Plans: AI-Augmented Defense and Expanded Coverage**
Looking ahead, the organization plans to deepen its partnership with Deepwatch as its security program continues to mature. Key priorities include:

- Exploring **Deepwatch NEXA™** to modernize SOC operations with natural-language investigation and AI-enabled decision support.
- **Expanding log ingestion** across additional businesses to strengthen enterprise-wide visibility.
- **Integrating MDR workflows** with the organization’s IT service management platform.
- **Advancing automation** around threat exposure and asset visibility as their environment evolves.

The security director views AI as the next major inflection point in SOC operations and expects Deepwatch to help lead that evolution.

DEEPWATCH™
Always Watching. Always Protecting.

### ABOUT DEEPWATCH

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

### CONTACT US

GET STARTED

250 Cambridge Avenue
Palo Alto, CA 94306

www.deepwatch.com