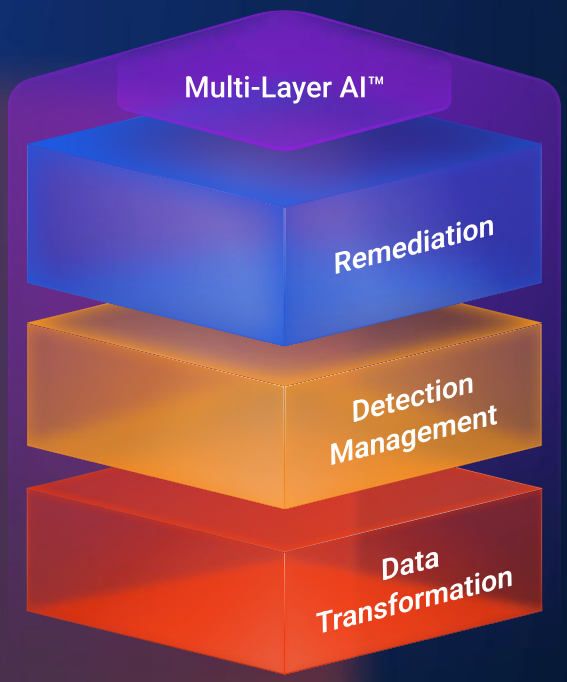
STELLAR CYBER®



Case Study

DEEPTREE
business serenity, delivered.

Deeptree Delivers Scalable, High-Confidence Managed Security Services

Enabling MSSP Growth Through Unified Visibility and Automated Triage

Deeptree is a managed detection and response (MDR) provider headquartered in Alaska with offices in Montana and Puerto Rico. The company delivers tailored cybersecurity services to clients in finance, healthcare, education, manufacturing, and other sectors across the United States. Facing increasingly complex attack surfaces—especially during the shift to remote work—Deeptree needed a way to efficiently scale security operations while maintaining white-glove service for organizations of all sizes.

To meet this need, Deeptree adopted an **open and unifying SecOps platform** to power its managed services, unify visibility across domains, and automate the triage and correlation of security events.

Before

Scattered Security Stack

Tools operated independently, making event correlation slow and manual.

Manual Correlation

Analysts manually stitched alerts together, slowing detection and response.

High Operational Cost

Disjointed tools increased cost and complexity

Inconsistent Service Delivery

SMB and enterprise customers lacked consistent protection.

Delayed Response

Incident context lagged due to siloed logs and fragmented workflows.

With Unified SecOps Platform

Unified Operational View

Security data from endpoints, network, cloud, identity, and logs appeared in one place, giving analysts full context.

Automatic Triage & Prioritization

Multi-Layer AI™ grouped related signals into high-confidence incidents for faster action.

Lower Overhead with Scale

Unified operations reduced tool sprawl and centralized workflows for broad service delivery.

Scalable Protection

Platform scaled seamlessly from small clients to large accounts without sacrificing quality.

Faster Response

Analysts saw curated incidents with full context, reducing investigation time.

Life Before a Unified SecOps Platform

Before centralizing around a unified SecOps platform, Deeptree's analysts had to manually correlate alerts coming from disparate tools—a process that slowed detection, increased operational overhead, and limited the ability to scale efficiently. Fragmented visibility made it harder to understand complex attack paths, especially across cloud, on-premise, and remote user environments.

Analysts spent excessive time gathering logs, weaving together scattered signals, and constructing context manually. This not only delayed response but also reduced productivity, making it costly to maintain high service levels across a diverse customer base.

Why Deeptree Modernized Its SOC

Deeptree needed a platform approach that would:

- **Integrate with existing security investments**
- **Unify telemetry across environments**
- **Automate triage and correlation**
- **Enable scalable managed services**
- **Provide consistent context across the attack lifecycle**

After evaluating major SOC solutions, Deeptree selected an **open and unifying SecOps platform** that consolidated multiple security techniques—such as user behavior analytics, network detection, endpoint signals, and log telemetry—into one contextualized view.

This approach reduced alert noise, surfaced actionable incidents quickly, and let analysts focus on high-value investigation and response instead of manual signal stitching.

Security Operations After Adoption

Once deployed, the unified platform became the central hub of Deeptree's MDR services. **Multi-Layer AI™ automatically triaged and grouped related activity into prioritized incidents**, enabling analysts to see the full attack picture rather than disjointed alerts.

Analysts worked from a unified incident queue that presented correlated data across endpoints, network traffic, cloud services, and identity behavior. This allowed faster identification of real threats and reduced false positives dramatically.

With noise reduced and context automated, Deeptree's team could respond faster, helping clients address threats before they escalated. The platform's scalable architecture supported a broad range of client environments without requiring proportional increases in staff.

Outcome

The transition to a unified SecOps foundation delivered measurable operational advantages for Deeptree:

- **Improved Analyst Productivity** — Analysts now focus on complex threats and strategic investigation rather than manual correlation.
- **Faster Detection and Response** — Prioritized incidents reduced both time to detect and time to remediate.
- **Consistent Service Across Clients** — The platform scales from small businesses to large enterprises without changing service quality.
- **Lower Operational Costs** — Consolidated tooling reduced overhead and simplified SOC workflows.
- **Greater Competitive Differentiation** — Tailored, enterprise-class services become viable even for smaller clients.

> **We wanted a security platform that helped us see more, know more, and act faster across diverse customer environments. Automating correlation and unifying visibility have been key to our success**
>
> – Peter House, President and CEO of Deeptree

By unifying data and automating routine triage with **Multi-Layer AI™**, Deeptree now delivers comprehensive managed security services with clarity, speed, and scalability—helping clients stay ahead of threats in an evolving risk landscape.

About Stellar Cyber

Stellar Cyber's open and unifying SecOps platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments.

With Stellar Cyber, organizations move from manual, alert-driven operations to a human-augmented autonomous SOC that identifies, validates, and responds to risk with speed and precision. Customers reduce false positives by more than 80%, improve analyst productivity, and lower operational costs—while retaining existing security investments and gaining measurable improvements in risk reduction and response consistency. The company is based in Silicon Valley.

stellarcyber.ai
sales@stellarcyber.ai

STELLAR CYBER®