SentinelOne

Building Security That Endures

Sundt Construction Cuts Investigation Time by 75% and Gains 24×7 Coverage with SentinelOne

SUNDT

CUSTOMER
Sundt Construction

INDUSTRY
Construction

EMPLOYEES
4,500

COUNTRY
USA

Endless Alerts & Manual Threat-Hunting

When Dan Howard joined Sundt Construction as VP of Information Technology, he inherited a high-performing but lean security team and a fragmented legacy security stack that buried them in noise and left true threats dangerously obscured.

As he assessed the global construction leader's cybersecurity infrastructure, he uncovered a brittle threat-detection foundation:

- Tens of thousands of alerts per day with no automated triage or prioritization
- No unified correlation layer to validate attacks or map activity across systems
- A small team operating without 24×7 SOC coverage
- No measurable MTTD or SLA-driven detection benchmarks
- Slow, manual incident recovery workflows
- Threat hunting limited to manual log-chasing across disparate tools

With Microsoft security tools, Sundt lacked the automation, depth, and operational scale required to protect a rapidly expanding enterprise. Risk grew exponentially every evening when the team logged off. "The one thing that kept me up most nights was the fact that we just didn't have visibility into our operations after hours," Howard explained.

Unified Protection Across Endpoint, Identity, and Cloud

From the historic headquarters of the Manhattan Project to the Moscow American Embassy, from the London Bridge relocation to major U.S. infrastructure projects, Sundt Construction has delivered some of the world's most iconic builds. As the company scaled, Howard sought cybersecurity defenses as resilient and future-proof as the structures his company creates.

After evaluating multiple solutions, Sundt selected SentinelOne's Singularity Platform to unify endpoint security, identity protection, and cloud workload coverage under a single, autonomous solution.

"SentinelOne was the clear winner across all our requirements," Howard said. "It's part of an overall strategy to help us mature our security practice."

A major differentiator: managed detection and response. With Wayfinder MDR, Sundt gained a fully staffed, 24×7 SOC, delivering continuous monitoring, threat validation, and rapid response without the financial burden of building equivalent in-house capacity.

In just one week, the Wayfinder pilot delivered clear value. SentinelOne identified and remediated more suspicious issues than previous tools, enabling the Sundt team to begin each morning with sharper focus.

Sundt Construction, Inc. is one of the country's largest and most respected general contractors. The 135-year-old firm specializes in transportation, water and wastewater, advanced facilities, heavy industrial and mining, building, concrete and renewable power work, and is owned entirely by its 4,500 employees. Sundt is distinguished by its diverse capabilities and experience, unique employee-ownership culture, and depth of self-perform expertise in multiple trades. Sundt has 13 offices throughout California, Arizona, North Carolina, Texas, Washington, Utah and Florida and is currently ranked the country's 46th largest construction company by ENR, the industry's principal trade magazine. Learn more at Sundt.com.

90%

SLA attainment after no previous measurability

72 Hours

Faster ransomware recovery time, powered by rollbacks

PRODUCTS &SERVICES

Singularity
- Platform
- Endpoint
- Identity
- Cloud

Purple AI

AI SIEM

Wayfinder MDR

Learn More →

Centralized Security Oversight and 24×7 SOC Coverage

Today, Sundt operates with a real-time view of their entire environment, spanning anomalies, suspicious behavior, endpoint compromises, and malware or ransomware indicators, and enabling rapid triage and precise investigation. They maintain continuous endpoint visibility and can instantly roll back ransomware or malicious modifications to a known-good state, eliminating downtime and removing the need for time-consuming manual recovery.

The shift has been transformative, from "alert hell" to actionable alert indicators.

"With Sentinel One, alerts are triaged and we only see the ones that are meaningful to our organization," said Scott Shedd, Director of Cybersecurity.

Purple AI expedites investigations by consolidating telemetry and enabling analysts to query the environment via natural language, collapsing hours of manual correlation into minutes.

Previously, threat hunting required pivoting between tools, stitching events together, and manually validating what mattered. Now, Wayfinder MDR proactively searches for latent threats, including stealthy behaviors or weak signals that haven't yet triggered alerts, dramatically reducing Sundt's exposure window.

"The average dwell time for a threat actor is 276 days," Shedd explained. "That's why Wayfinder MDR has been so significant for us. It identifies potentially undetected threats in our network."

With Wayfinder MDR serving as their 24×7 SOC, SentinelOne escalates only priority issues and collaborates with Sundt during daily standups, functioning as a true extension of the internal team.

A Night and Day Security Shift

With SentinelOne, Sundt quickly gained measurable speed, resilience, and operational confidence:

- 90% SLA attainment across detection and response
- 72-hour acceleration in ransomware recovery, powered by rollback
- ~75% reduction in investigation and analysis time using Purple AI
- $1.6M saved by not building an in-house SOC
- Hours or days faster threat detection
- Zero alert overload

"Compared to our previous provider, SentinelOne is night and day," Howard said. "We're able to easily and quickly identify risky concerns and remediate. I sleep much better at night knowing Sentinel One's managed detection and response team has eyes on my operations 24×7."

As Sundt doubled in size the past few years, SentinelOne scaled seamlessly with them, providing security readiness, compliance confidence for upcoming government projects, and a blueprint for continued maturity.

"SentineOne has been a partner and almost a division of our cybersecurity team," Howard added. "The future is bright and we're excited to see how SentinelOne's technology can help us continue to mature our practices here at Sundt Construction."

> "
>
> Compared to our previous provider, SentinelOne is night and day. We're able to easily and quickly identify risky concerns and remediate. I sleep much better at night knowing SentinelOne's managed detection and response team has eyes on my operations 24×7.
>
> **Dan Howard**
> VP of IT

> "
>
> SentinelOne was the clear winner when compared against all our requirements. It's part of an overall strategy to help us mature our security practice.
>
> **Dan Howard**
> VP of IT

> "
>
> With SentinelOne, alerts are triaged and we only see the ones that are meaningful to our organization.
>
> **Scott Shedd**
> Director of Cybersecurity

sentinelone.com

sales@sentinelone.com
+1 855 868 3733