SentinelOne

The Gold Standard of Enterprise Defense: Inside Yahoo's Hybrid Security Transformation with SentinelOne

yahoo!

CUSTOMER
Yahoo

INDUSTRY
Technology / Media

COUNTRY
USA

Yahoo operates one of the world's largest digital ecosystems, supporting hundreds of millions of users worldwide. Yahoo's elite security team, known as The Paranoids, deployed SentinelOne across a global hybrid environment in four months, establishing unified visibility and strengthening the team's ability to detect, investigate, and respond to threats at enterprise scale.

Defending Trust at Internet Scale

Every day, The Paranoids face the immense responsibility of securing the systems and data behind a platform used by hundreds of millions of people.

"We're paranoid for our employees, customers, and partners, so they don't have to be," said Sean Zadig, CISO and Chief Paranoid at Yahoo. "If Yahoo is the trusted guide to the digital wilderness, the foundation of that is trust."

Few companies have shaped the internet longer than Yahoo. Today, the technology pioneer has evolved into one of the globe's biggest digital ecosystems, spanning mail, media, advertising, and identity services.

Defending this footprint means protecting hundreds of millions of active mailboxes. The Paranoids must guard every corner of this environment against persistent, highly sophisticated threat actors without introducing operational drag that slows down business innovation.

Overcoming Legacy Performance Constraints

The Paranoids manage a predominantly Mac endpoint fleet, Linux-heavy production systems, and a global mix of cloud and on-premises infrastructure. This distributed architecture must comply with rigid international regulatory frameworks while maintaining maximum uptime.

As Yahoo's environment continued to evolve, The Paranoids sought a platform that could maintain comprehensive protection and visibility without introducing performance tradeoffs. SentinelOne delivered real-time, behavioral threat protection while supporting the performance and stability required across Yahoo's hybrid infrastructure.

"We needed one security partner that could support our entire environment," Zadig said. "SentinelOne gives us broad coverage across all of it, and when we tested it with simulated attacks, it outperformed the other options."

For 30 years and counting, Yahoo has served as a trusted guide for hundreds of millions of people globally, helping them achieve their goals big and small online through our portfolio of iconic products. For advertisers, Yahoo offers omnichannel solutions and powerful data to engage with our brands and deliver results.

400,000
Endpoint deployment in 4 months

Zero
Coverage gaps during deployment

Days → Minutes
Forensic investigation and data collection

PRODUCTS &SERVICES

Singularity
- Endpoint
- Cloud

Purple AI
Flex
Technical Account Manager

Learn More →

Securing 400,000 Endpoints in 4 Months

Yahoo migrated to SentinelOne by treating the security deployment exactly like a core engineering update, leaving zero room for coverage blind spots or deployment downtime. They integrated the Singularity agent directly into their centralized CI/CD pipelines, managing the rollout as production code.

“Deploying Singularity Endpoint was like changing the engine on the plane mid-flight,” recalled Chris Keast, Vice President of Cyber Defense, Yahoo. “It went smoother than expected and we transitioned roughly 400,000 endpoints in four months.”

SentinelOne Flex provided a unified agreement that gave the team immediate access to the full Singularity Platform without the friction of separate procurement cycles. Rather than buying individual point products, Yahoo consolidated their cyber defense strategy under a single commercial commitment, gaining the agility to seamlessly activate key platform capabilities like Hyperautomation and Data Pipelines, while concurrently evaluating cutting-edge innovations like Purple AI.

Forensic Investigation in Minutes, Not Days

With Singularity Endpoint and Singularity Cloud fully operational, The Paranoids possess a unified telemetry pipeline that grants total visibility across both employee hardware and cloud workloads. This centralized architecture allows Yahoo to neutralize automated, machine-speed attacks before lateral movement can occur.

Nation-state campaigns, large-scale credential abuse, and advanced attacks targeting Yahoo’s global ecosystem are part of the team’s daily reality. SentinelOne works continuously in the background, containing threats at machine speed so the team can remain focused on higher-priority, strategic threats.

“SentinelOne alerting and telemetry have become a central part of how our FIRE team (forensics and incident response) operates every day,” Keast said. “It’s been leaps and bounds better than where we were before.”

When a potential threat is flagged, analysts no longer face the exhausting barrier of manually connecting to individual machines scattered across the globe. In minutes, they now execute forensic data collection that previously took days of cross-department coordination, allowing the team to reclaim what Zadig calls “valuable brain space.”

Leveling the Playing Field with Purple AI

Proactive threat hunting is a core focus for Yahoo’s Forensics and Incident Response (FIRE) team. In an environment targeted by sophisticated adversaries, analysts regularly launch investigations based on emerging threats, new vulnerability disclosures, and intelligence from the security community.

At Yahoo’s scale, reviewing raw data lake telemetry historically required massive time and advanced query syntax expertise. Purple AI has fundamentally democratized these investigations. Analysts can now type an interrogation in plain English, describing the exact malicious indicators they want to find. Purple AI instantly handles the mechanical heavy lifting, translating the request into clean query logic and searching in real time.

“Purple AI increases the pace of our threat hunting, helping us uncover more adversary activity,” Keast said. “It also levels the playing field for our analysts and improves the quality of life for the people investigating and remediating threats.”

> “
>
> We needed one security partner that could support our entire environment. SentinelOne gives us broad coverage across all of it, and when we tested it with simulated attacks, it outperformed the other options.
>
> **Sean Zadig**
> CISO and Chief Paranoid

> “
>
> Deploying Singularity Endpoint was like changing the engine on the plane mid-flight. It went smoother than expected and we transitioned roughly 400,000 endpoints in about four months.
>
> **Chris Keast**
> Vice President of Cyber Defense

> “
>
> SentinelOne alerting and telemetry have become a central part of how our FIRE team (forensics and incident response) operates every day. It’s been leaps and bounds better than where we were before.
>
> **Chris Keast**
> Vice President of Cyber Defense

> “
>
> Purple AI helps us increase the pace of our threat hunting, and that helps us find more adversary activity. It helps level the playing field for our analysts and improves quality of life for our folks who are looking for and remediating threats.
>
> **Chris Keast**
> Vice President of Cyber Defense

Continuous Evolution Through Shared Innovation

Yahoo's SentinelOne Technical Account Manager brings unmatched responsiveness and technical alignment. Their TAM provides rapid troubleshooting for daily operational challenges while actively participating in long-term strategic planning, allowing Yahoo's real-world enterprise insights to directly shape SentinelOne's core product engineering.

"We've made suggestions that appear on SentinelOne roadmaps," Zadig said. "We can actually influence the direction that the company takes. There's true back and forth."

The Gold Standard for Global Security

While The Paranoids diligently work behind the scenes, their robust infrastructure also serves to assure customers, regulators, partners, and insurers worldwide of their rigorous controls. During risk evaluations, insurance underwriters have explicitly categorized Yahoo's framework as "the gold standard for how they evaluate other companies," according to Zadig.

For the team, that external recognition reinforces what they witness operationally every day: a modern, autonomous foundation capable of defending a massive digital ecosystem at internet scale.

"Protecting our users and their data is core to Yahoo's mission," Keast concluded. "SentinelOne takes that as seriously as we do and has demonstrated that through their responsiveness and commitment."

"We're able to tell a very comprehensive story that gives our stakeholders trust and confidence, and SentinelOne is a huge part of that," Zadig added.

> "We've been told by our insurance underwriters that we're basically the gold standard for how they evaluate other companies.
>
> **Sean Zadig**
> CISO and Chief Paranoid

> "Protecting our users and their data is core to Yahoo's mission. SentinelOne takes that as seriously as we do and has demonstrated that through their responsiveness and commitment.
>
> **Chris Keast**
> Vice President of Cyber Defense

> "We're able to tell a very comprehensive story that gives our stakeholders trust and confidence, and SentinelOne is a huge part of that.
>
> **Sean Zadig**
> CISO and Chief Paranoid

sentinelone.com

sales@sentinelone.com
+1 855 868 3733