Reach + SentinelOne

SOLUTION BRIEF

# See Every Change to Your SentinelOne Defenses

Know what security controls changed, who changed them, when, and the security risks introduced.

THE CHALLENGE

### Shared Ownership. Unseen Changes. Weakened Defenses.

Security technologies like SentinelOne are often managed by multiple teams, including security, IT, and endpoint operations. Administrators across these teams can modify security policies and controls, often without the security team knowing when changes are made.

A change that broadens an exclusion, disables a response rule, or adds a privileged administrator can unintentionally weaken protection and create openings for attackers. Without visibility into these changes, security teams may only discover the problem after an incident, leaving them to piece together what changed, who made the change, and how their defenses were weakened.

THE SOLUTION

### Track Every Change and Understand Its Security Impact

Reach continuously monitors SentinelOne configurations, identifies risky changes, and provides a clear history of what changed, when, who made the change, and its security implications.

Security teams can:

- see how configurations have evolved
- identify changes that weaken protection
- prioritize what needs attention
- automatically remediate and realign controls
- continuously validate that defenses stay aligned with security policy

### SentinelOne Configuration Drift History

ILLUSTRATIVE EXAMPLE · SIMULATED DATA

**WHAT CHANGED** — Before-and-after settings

**WHEN** — Change timestamps

**WHO** — Administrator responsible

**SECURITY IMPACT** — Risk and current state

**Mar 18, 2025 · 11:18 AM** — Added — IT Analyst, Desktop Support

```
null
+ C:\Program Files\BuildTools\
```

**Oct 7, 2025 · 3:44 PM** — Modified — IT Analyst, Desktop Support

```
- C:\Program Files\BuildTools\
+ C:\ProgramData\BuildCache\
```

**May 21, 2026 · 6:21 PM** — Modified — IT Analyst, Desktop Support

```
- C:\ProgramData\BuildCache\
+ C:\ProgramData\
```

**Sep 13, 2026 · 2:14 AM** — Modified — IT Analyst, Desktop Support

```
- C:\ProgramData\
+ C:\
```

Current value `C:\` **CRITICAL** — Exclusion broadened to entire system drive; endpoint activity may go unmonitored.

EXAMPLES

## SentinelOne Configuration Changes That Can Introduce Risk

### Endpoint protection exclusion broadened

A Windows path exclusion is expanded to the entire `C:\` drive, effectively disabling in-process monitoring across the system drive and allowing malware to run unseen.

### Lateral movement prevention disabled

A SentinelOne STAR rule changes from BLOCK to DETECT, disabling Active Response and network quarantine. Lateral movement is no longer contained automatically.

### Unapproved administrator added

A new SentinelOne administrator is granted account-wide access without a matching ServiceNow change ticket, allowing them to modify or remove security policies, exclusions, and response rules across every site.

## Get started with Reach + SentinelOne. Connect your deployment and uncover risky configuration changes.

CONTACT THE REACH TEAM AT
www.reach.security/connect

**01 An API key to start**
Read-only SentinelOne API key

**02 Setup in 3 minutes**
Create your account and set up the integration

**03 Results in < 5 days**
See configuration changes, security risks, and drift history, without modifying your deployment