SentinelOne

WatchTower™

Threat Hunting & Compromise Assessment Services Made for Every Enterprise

WatchTower tracks today's most prolific threat campaigns & crimeware and their impact on your environment, empowering you to adapt and respond as they arise. Dive even deeper with WatchTower Pro to uncover and remediate hidden threats and environmental security risks that could compromise your unique organization.

Every day, the global threat landscape grows more treacherous and complex. Malicious threat actors evolve their motivations and techniques, and organizations' attack surfaces become increasingly dynamic and dispersed. To stay protected and adaptive, today's cybersecurity teams need an intelligence-informed solution for understanding how emerging and established threats are impacting their environments, and how to effectively mitigate those risks for the long run.

SentinelOne's WatchTower services offer peace of mind through a breadth-and-depth approach to threat hunting, providing you with agility for when new threats arise, as well as the confidence that comes with a clean house:

POWERED BY

Singularity SIGNAL

As SentinelOne researchers track emerging threat actors in the wild, WatchTower distills and prioritizes their intelligence from proprietary, commercial, open, and dark web sources to hunt purposefully within your environment.

01

WATCHTOWER

Active Campaign Threat Hunting & Intelligence Reporting

02

WATCHTOWER PRO

Customized Threat Hunting & Compromise Assessment, Plus Access to the Signal Hunting Library and All the Benefits of WatchTower

---

100%

Of Gartner Peer Insights Reviewers Recommend SentinelOne Threat Services

Gartner peerinsights™

WatchTower

WatchTower is SentinelOne's active campaign threat hunting service targeting global APT campaigns, novel attacker techniques, and emerging trends in cyber crime. By pairing data-driven intelligence insights with our experts' human-based knowledge, WatchTower identifies, prioritizes, and hunts for the most pressing threats and criminal activity experienced by organizations around the world at that moment in time.
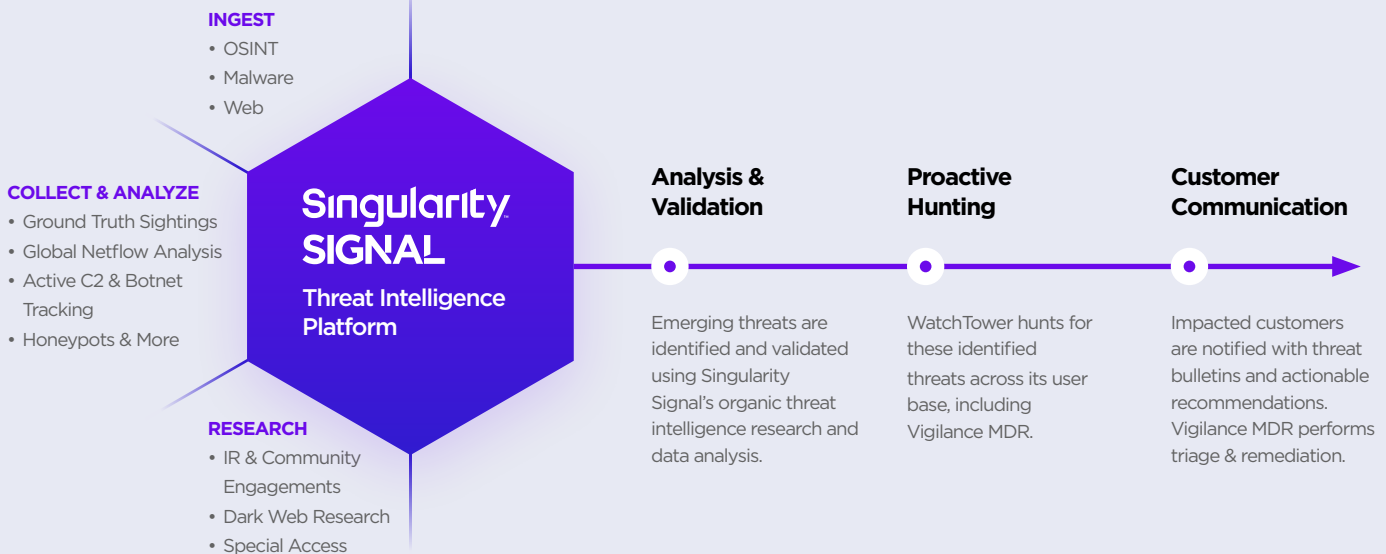
If and when those threats are detected in your environment, WatchTower notifies you immediately with relevant, remediation-oriented guidance; this enables you or our Vigilance MDR analysts to respond without adding noise to your inbox.

Every month, WatchTower also publishes a **Hunting Digest** with key findings and trends observed by our team across the global threat landscape from the previous month's hunting activity. These reports contain SentinelOne-exclusive intelligence and recommendations based on industry, sector, region, and more.

KEY BENEFITS

+ Cross-Geo, Cross-Industry Analysis

+ Human Lens to Machine-Powered Hunting

+ Pre-Validated, Reviewed Threats

+ Faster Response & Preparedness

+ Monthly Hunting & Intelligence Reporting

+ Practical Applications, Tangible Results

The WatchTower Approach

INGEST
• OSINT
• Malware
• Web

COLLECT & ANALYZE
• Ground Truth Sightings
• Global Netflow Analysis
• Active C2 & Botnet Tracking
• Honeypots & More

RESEARCH
• IR & Community Engagements
• Dark Web Research
• Special Access

Singularity SIGNAL
Threat Intelligence Platform

Analysis & Validation

Emerging threats are identified and validated using Singularity Signal's organic threat intelligence research and data analysis.

Proactive Hunting

WatchTower hunts for these identified threats across its user base, including Vigilance MDR.

Customer Communication

Impacted customers are notified with threat bulletins and actionable recommendations. Vigilance MDR performs triage & remediation.

Targeted

Hunts emerging, insidious threats found in the wild within your environment.

Tangible

Intelligence is distilled down to the most relevant, addressable details.

Actionable

Insights are designed for actual threat reduction - not just awareness.

2

WatchTower Pro

WatchTower Pro is SentinelOne's customized threat hunting and compromise assessment service tailored to your unique environment. WatchTower Pro empowers risk-conscious organizations with a detailed assessment of their attack surface, overall risk posture, and internal security practices—all delivered through a designated threat hunter and a supporting team of experts.

Common Cases for Engaging WatchTower Pro

✓ **Post-Breach (Internal or Within Your Industry)**

✓ **Post-Merger & Acquisition**

✓ **New or Changing Personnel**

✓ **Organizational Health Checks**

Your dedicated hunter will provide you with a custom report of their findings following their twice-yearly deep-dive hunts, and will also perform a verification hunt the following quarter to confirm that previously-detected issues were appropriately remediated and resolved by your team. Their bespoke recommendations are designed to close gaps in a timely manner, and build organizational resilience. Vigilance Respond and Vigilance Respond Pro customers can also lean on their MDR analysts to perform remediation and recovery on their behalf.

While WatchTower Pro leaves you in the careful hands of our experienced team, you can hunt on your own terms any time with unlimited access to queries in the Signal Hunting Library. The library is tagged and organized by threat actor, campaign, malware family, and MITRE tactic to make hunting simple and accessible without the need for a full-time intelligence team.

KEY BENEFITS

+ Deep-Dive Hunts That Scour Every Corner of Your Environment for Latent Security Risks

+ Appraisal of External and Internal Threats, Even Those Previously Unknown

+ Dedicated Threat Hunter and Expert Knowledge Base

+ Unrestricted Access to Signal Hunting Library

+ Customized Reporting With Tailored Recommendations for Remediation and Program Improvement

+ Emerging Threat Coverage With Active Campaign Tracking and Intelligence Reporting From WatchTower

WATCHTOWER PRO Hunting Targets

- Hidden APT
- Covert Cyber Crime
- Policy Misuse
- Insider Threats
- Poor Security Practices
- Environmental Vulnerabilities

Dive Deep With WatchTower Pro

WatchTower Pro thoroughly and precisely captures your security posture — including external and internal risk factors. Your designated hunter will search for the presence of not just outside threats, but also internal practices and misuse that leave you exposed.

The WatchTower Pro Process

ONGOING
Understand How You're Uniquely Impacted
Gain insight into how you're affected by emerging threats in your industry, sector, geographic region, and more

2X PER YEAR
Dive Deeper Into Your Security Posture
Collaborate with your designated team of hunters to search for covert threats, indicators of compromise, and risky practices

2X PER YEAR
Build Confidence in Your Defenses
Confirm if previously-identified issues still exist or have been successfully resolved with verification hunts

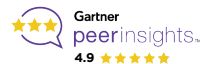|	WATCHTOWER	WATCHTOWER PRO Includes WatchTower
SCOPE	**Targeted** Quickly detect & diagnose your exposure to current APT and crimeware	**Comprehensive** Know how you've been impacted by all current & historical, external & internal threats
RECOVERY	**Emergency Response** Remediate quickly through Vigilance MDR or provided instructions when threats are detected, with Vigilance DFIR escalations as needed	**Recovery for the Long Run** Take immediate steps to clean up threats or an attack with remediation instructions, then apply our experts' tailored recommendations for improving overall risk posture
REPORTING	**Monthly Digest** Receive a global-scale, intelligence-based analysis of our hunters' findings across all WatchTower customers	**Custom Reporting** Dive deeper into your designated hunter's findings in the context of your own environment, plus verification of remediated issues
ACCESS	**Expert-Curated** Rely on the WatchTower team to identify, prioritize, and hunt today's most aggressive, pressing threats	**Controlled & Customized** Trust our hunters to identify relevant threats to your business, with added flexibility to hunt yourself using the Signal Hunting Library
	Included with Vigilance MDR, Available Standalone	**Available Standalone or as an Add-On Service**

Innovative. Trusted. Recognized.

Gartner®

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

• No missed detections. 100% visibility
• Most Analytic Detections 2 years running
• Zero Delays. Zero Config Changes

Gartner peerinsights™
4.9 ★★★★★

100% of Gartner Peer Insights™

Reviewers recommend SentinelOne Threat Services

FR FedRAMP

AAA

ISO 27001 CERTIFIED by schellman

vb 100 VIRUS virusbtn.com

AAA

TEVORA
PCI DSS Attestation
HIPAA Attestation