



SOLUTION BRIEF / MAY 2024

LEVELBLUE + SENTINELONE: BETTER TOGETHER

Get Exponential Protection Across Your Business and Strengthen Cyber Resilience

LevelBlue and SentinelOne are collaborating to extend detection and response across your environment—from the endpoint to the hybrid network—and every connection in between.

As one of the world's leading security service providers,¹ LevelBlue has been trusted with providing cybersecurity consulting and managed security services to multinational enterprises, regional businesses, and government entities for more than three decades.²

Our alliance with SentinelOne extends our managed detection and response (MDR) service and boosts the efficacy of your security operations by bringing together two world-class technology platforms and the expertise of seasoned cybersecurity professionals in one premium managed service.

“LevelBlue is among the innovation leaders in the Americas, thanks to a broad portfolio that includes cutting-edge managed security solutions and varied consulting services.”*

Frost Radar™: Americas Managed and Professional Security Services, 2023

*(LevelBlue, formerly AT&T Cybersecurity)

¹ Top 250 MSSPs List: Managed Security Services Provider Company Research 2022 - Page 25 of 25 - MSSP Alert

² Gartner Emerging Tech: Security — Leverage Emerging MDR Trends to Grow Your Security Service Revenue. June 23, 2023

All the support you need in one place



One smooth, simplified customer experience

One team keeps watch across your attack surface. LevelBlue analysts monitor and manage your hybrid network and endpoints (e.g., laptops, servers, Kubernetes containers) with the LevelBlue USM Anywhere and SentinelOne Singularity platforms in one view, giving you a single point of contact across the two technology stacks. Get 24/7 eyes on glass as our analysts investigate—and help you respond to—threats across your diverse and distributed attack surface.

Our threat hunters proactively search for threats across your environment, leveraging intelligence from LevelBlue Labs, the LevelBlue Labs Open Threat Exchange (OTX), SentinelOne Deep Visibility, and other sources.

This high-touch service includes platform onboarding, guidance on agent deployment, continuous policy tuning, hands-on training, and ongoing technical support.


World-class technology that supports our service delivery

The entire service is built on the USM Anywhere™ open XDR platform, proprietary technology that allows LevelBlue to deliver holistic threat detection, incident response, and compliance management. We also offer incident readiness and response through LevelBlue Consulting.


USM Anywhere continuously monitors for threats, collecting data that is enriched by threat intelligence from LevelBlue Labs and OTX. The platform's integration ecosystem extends its security capabilities to more than 600 third-party security and productivity tools.

The deep integration between the two platforms means greater visibility for faster, more efficient detection and response. LevelBlue analysts respond to all alarms directly from USM Anywhere. All information is propagated to the SentinelOne platform—if an alarm is closed in USM Anywhere, it is also closed in SentinelOne—and we can query the SentinelOne platform from USM Anywhere.

Better together



LevelBlue/Labs



More data, better visibility

- USM Anywhere collects and correlates data from across on-premises and multi-cloud environments
- SentinelOne endpoint data is ingested directly into USM Anywhere
- One centralized view of assets and threats

Improved analytics

- Threat intelligence from LevelBlue Labs and OTX is fed into both platforms to enhance detections
- Both platforms align to the MITRE ATT&CK® framework
- LevelBlue SOC proactively hunts for threats

Improved response actions

- USM Anywhere Advanced BlueApp integrations enable response actions from an ecosystem of security and IT tools
- Orchestrated responses to SentinelOne detections directly from USM Anywhere

Visibility, analytics, and AI-driven detection and response across your network and on the endpoint

SentinelOne agents installed on all your endpoints combine powerful endpoint protection with real-time detection and response, leveraging static and behavioral artificial intelligence (AI) models to protect against the most advanced malware and ransomware threats.

SentinelOne Storyline™ technology provides actionable context, allowing analysts to quickly connect the dots by automatically linking all related events and activities into one view. Each agent starts protecting as soon as it is deployed (even when offline), and all alerts are ingested directly into the USM Anywhere platform. USM Anywhere uses AI to enhance detections, so threats across your network can be detected and identified faster and more accurately.

The robust SentinelOne Advanced BlueApp integration into the USM Anywhere platform provides a range of orchestrated response actions that your team or our analysts can take to respond to threats in real time. SentinelOne’s automated and one-click rollback capability automatically restores files to a previously known-good state, simplifying ransomware response and slashing mean time to respond (MTTR).

Continuous tactical threat intelligence

LevelBlue Labs has visibility into multiple sources of threat data, including the award-winning³ OTX, which hosts a community of more than 235,000 security professionals submitting over 20 million threat indicators a day.

Because this service is built on the USM Anywhere platform, SentinelOne alerts are enriched by the same threat intelligence from LevelBlue Labs and OTX that is fed into USM Anywhere. This includes information about device identity, geolocation, associations with known threat actor infrastructure and malware families, and other intelligence. Additionally, both platforms map to the MITRE ATT&CK framework.

"

Cyber attackers are using sophisticated AI-driven techniques to unleash devastating attacks. SentinelOne has recognized the need to complement human skills with greater automation and more intelligence-based pre processing in order to assist security teams with their often onerous workloads."

Sarah Pavlak, Industry Principal, Frost & Sullivan

Frost & Sullivan Leadership Award

³ <https://www.scmagazine.com/news/sc-award-winners-2023-att-cybersecurity-best-threat-intelligence-technology>

“LevelBlue should appear on shortlists for enterprises that seek global scale in managed network security, network transformation, and deep threat intelligence capability.”*⁴

[Omdia Universe: Selecting a Global IT Security Services Provider, 2021](#)

*(LevelBlue, formerly AT&T Cybersecurity)

LevelBlue

Managed security services leader

LevelBlue helps make complexity easy to understand and navigate. Our managed security services, threat awareness, and ground-breaking research are dedicated to help keep you protected today and prepared for tomorrow.

- Named MSS and MDR leader by Gartner⁵, IDC⁶, and Forrester⁷



Endpoint expertise and innovation

- A leader in the 2023 Gartner Magic Quadrant for Endpoint Protection Platforms⁸
- SentinelOne leads in the 2023 MITRE ATT&CK Evaluation with 100% prevention⁹
- Ranked highest across all customer use cases in Gartner 2022 Critical Capabilities for Endpoint Protection Platforms report¹⁰

4 Omdia Universe: Selecting a Global IT Security Services Provider, 2021

5 Listed as a provider in the 2023 Gartner Emerging Tech report on managed detection and response

6 IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment

7 <https://cybersecurity.att.com/resource-center/analyst-reports/frost-radar-americas-managed-professional-security-services-2023>

8 <https://www.sentinelone.com/blog/sentinelone-a-gartner-magic-quadrant-leader-for-three-consecutive-years/#>:

9 <https://www.sentinelone.com/blog/sentinelone-achieves-100-protection-and-detection-in-the-2023-mitre-engenuity-attck-evaluations-enterprise/>

10 <https://www.sentinelone.com/press/sentinelone-ranks-highest-across-all-customer-use-cases-in-the-gartner-2022-critical-capabilities-for-endpoint-protection-platforms/>

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.