

LevelB/ue



PRODUCT BRIEF / JUNE 2024

Fight Ransomware and Quickly Respond to Advanced Cyberattacks



LevelBlue Endpoint Security with SentinelOne uses machine learning and artificial intelligence (AI) to fend off increasingly sophisticated cyberthreats. Autonomous protection works even when endpoints are offline.

The speed, scale, and sophistication of modern cyberattacks are challenging businesses of all sizes. Signature-based antivirus—that is, antivirus software that can only detect known and documented threats—is no longer sufficient to defend against malware, ransomware, and fileless attacks.

LevelBlue Endpoint Security with SentinelOne rises to this challenge. It uses AI and machine learning to help ensure your endpoints are continuously protected, regardless of whether cyberthreats are well-documented or newly emerging.

LevelBlue Endpoint Security with SentinelOne comes in two options: Complete or Control. The Complete option includes Deep Visibility Active EDR™ with Storyline™, which contextualizes threat data automatically and helps security analysts find where attacks originated and gain context to better respond to threats. The single agent can be deployed on laptops, desktops, virtual desktop infrastructure (VDI), servers (on premises or cloud, physical or virtual), and cloud containers. You'll have consistent protection across Windows, MacOS, and Linux.

Features

- Global Software-as-a-Service (SaaS) implementation; highly scalable; choice of locality (U.S., European Union, and Asia-Pacific)
- Ability to roll back to the last clean state in the event of a ransomware attack
- Flexible administrative authentication and authorization: Signal sign on (SSO), multi-factor authentication (MFA), role-based access control (RBAC)
- Administration customizable to match your organizational structure
- Integrated SentinelOne Threat Intelligence and MITRE ATT&CK Threat Indicators
- LevelBlue Labs delivers continuous threat intelligence to help keep your defenses up to date

Benefits

- Consolidates endpoint protection, and endpoint detection and response (EDR) into one agent
- Customizable console with time-saving workflows
- Ransomware solved through superior behavioral artificial intelligence (AI)
- Autonomous protective responses trigger instantly
- Storyline™ with ActiveEDR® contextualizes threat data for incident responders and threat hunters, saving time and reducing fatigue
- Affordable EDR data retention of 365 days+ for full historical analysis

LevelBlue Endpoint Security with SentinelOne also provides autonomous protection. Even when users are working offline and endpoints are not connected to the cloud, the agent can continue to search for malicious files or malware and take action automatically.

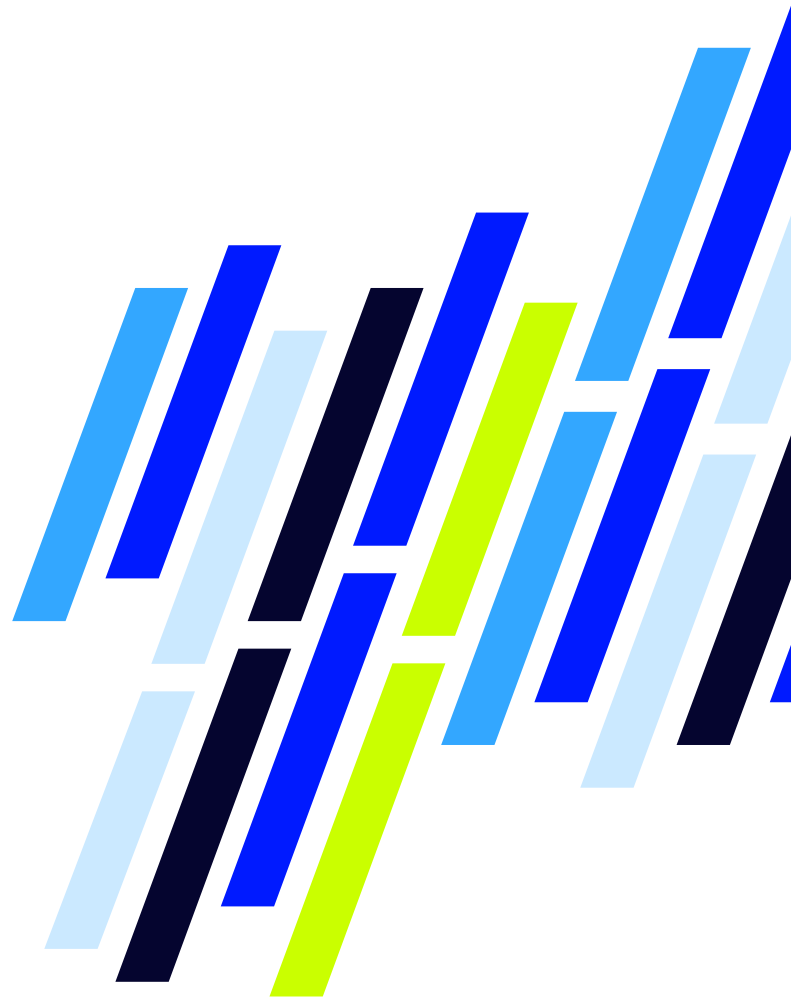
Ransomware attacks are growing in size and sophistication. In the event of a ransomware attack, LevelBlue Endpoint Security with SentinelOne can take your Windows systems back to a previously clean state.

Maximize your Cyber Defense with Guided Onboarding:

Leverage LevelBlue's white-glove guided onboarding service to fortify your organization against the most advanced endpoint threats. Our add-on service not only simplifies platform and security policy configuration but also guides you through seamless agent deployment and enables your team to manage and monitor across all endpoints. With a dedicated LevelBlue security engineer by your side, you'll receive a recommended agent deployment plan, learn deployment best practices, and ensure your agents are optimally functioning post-deployment. Through expert guidance, LevelBlue positions your team to excel in cybersecurity defense.

LevelBlue Endpoint Security with SentinelOne is designed so you can monitor, investigate, and manage security incidents yourself. LevelBlue provides technical support weekdays during business hours. Training is also included. To determine which solution is right for your business, please see comparisons in the table on the next page.

If you would like a managed solution that includes white-glove onboarding, 24/7 endpoint security monitoring and management, and training, we'll be happy to talk to you about LevelBlue Managed Endpoint Security with SentinelOne. Learn more at LevelBlue.com



	COMPLETE	CONTROL
Security Operations Endpoint Detection and Response (EDR) Features	•	
Deep Visibility ActiveEDR® with Storyline™ Context	•	
MITRE Engenuity ATT&CK® Integration	•	
Storyline Active Response (STAR™) Custom Detection Rules	•	
File Integrity Monitoring	•	
14-day EDR Hunting Data Retention	•	
Secure Remote Shell	•	•
IT OPS / Security Hygiene Features	•	•
OS Firewall Control with Location Awareness (Win, Mac, Linux)	•	•
USB device control (Win, Mac)	•	•
Bluetooth® / Bluetooth Low Energy® Control (Win, Mac)	•	•
App Vulnerability (Win, Mac)	•	•
Rogue Device Discovery	•	•
Base Endpoint Protection Features	•	•
Autonomous Sentinel Agent Storyline™ Engine	•	•
Static AI and SentinelOne Cloud Intelligence file-based attack prevention	•	•
Behavioral AI Fileless Attack Detection	•	•
Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)	•	•
Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)	•	•
Autonomous Rollback Response / 1-Click, no scripting (Win)	•	•
Quarantine Device From Network	•	•
Incident Analysis (MITRE ATT&CK®, Timeline, Explorer, Team Annotations)	•	•
Agent Anti-tamper	•	•
App Inventory	•	•
Optional Add-ons		
Ranger IoT	•	•
Extended Data Retention	•	
Binary Vault	•	

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.

To learn more, please contact your LevelBlue representative or visit [LevelBlue.com](https://www.LevelBlue.com)