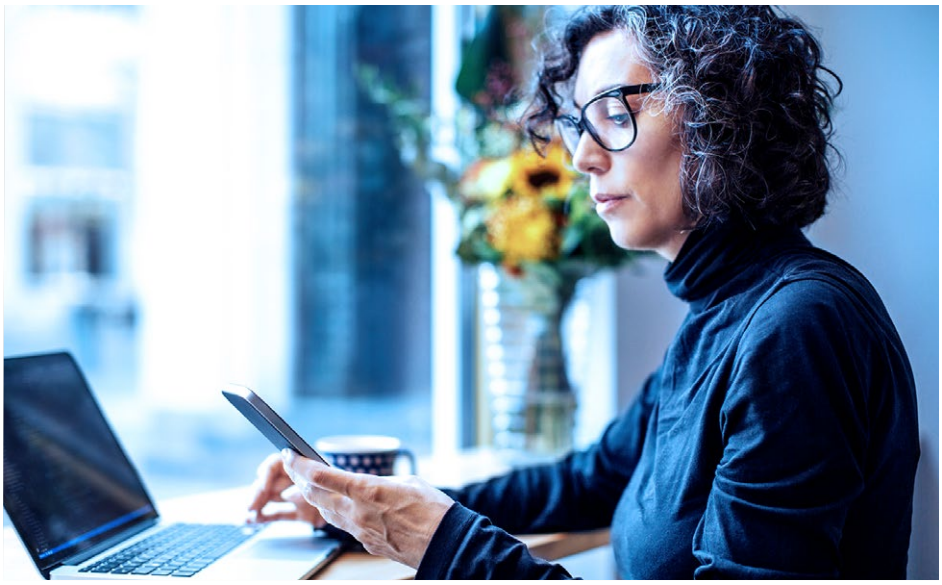
LevelBlue

PRODUCT BRIEF

# Protect Your Business with Leading Endpoint Security and World-Class Managed Services



## Boldly Embrace Digital Transformation

Success in today's digital age demands that organizations transform with confidence and speed. By adopting next-generation networking, mobility, and cloud services and connecting data edge-to-edge, organizations can open new markets, create stunning customer experiences, and drive cost and operational efficiencies.

Businesses are counting on security solutions that can keep pace with the rate of change. Endpoint security has never been more central to that effort.

## Endpoints Are the First and Last Line of Defense

With faster networks, compute power moving closer to the edge, and the need for access to corporate data centers and cloud data from anywhere, endpoints have become prime targets for attacks. And, with high velocity attacks, weaponized documents, and evasive malware, these highly sophisticated attacks can go undetected through traditional endpoint security measures. There has never been a more important time to supply your endpoints with strong protection. LevelBlue is prepared to help you take on this transformation with industry-leading managed security services and endpoint security solutions that can protect your endpoints at machine speed.

## Potential Benefits

- Act faster and more decisively with highly effective threat detection and incident response managed services
- Minimize dwell time with consistent threat prevention, detection, and response
- Provide fast, automated remediation to keep endpoints in a constant clean state
- Reduce complexity with consolidated security functions
- Protect the endpoint in real time, even when offline with persistent protection performed on the endpoint agent

## Product Features

- SentinelOne® comprehensive endpoint security
- 24/7 monitoring by a dedicated LevelBlue Security Operations Center (SOC) team
- LevelBlue Labs delivers continuous threat intelligence to help keep your defenses up to date
- Provides policy configuration, threat monitoring and response, and ongoing policy tuning
- Support for Windows™, macOS®, Linux®, and Kubernetes® and support a variety of form factors including physical, virtual, VDI, data centers, and cloud virtual machines
- Ability to rollback to the last clean state in the event of an attack

## Next-Generation Technology Is Taken to the Next Level with SentinelOne

Businesses need to protect against known and unknown threats well beyond what a traditional antivirus would provide. Through Artificial Intelligence (AI), machine learning, and an autonomous agent, LevelBlue Managed Endpoint Security with SentinelOne can help provide continuous protection, even when users are working offline. Gain thorough coverage over your endpoints with one consolidated solution for endpoint protection, endpoint detection, and endpoint response while helping to protect your business across the entire attack chain. By integrating LevelBlue Labs threat intelligence with SentinelOne, customers stay up to date on the latest threats so they can help to detect emerging threats sooner.

## Prevent

Dynamic whitelisting/blacklisting and static AI analysis helps protect endpoints:

- Analyze files in real time, before they execute
- Prevent known and unknown threats at machine speed

## Detect

Identify Advanced Persistent Threats (APTs) with behavioral AI and complete storyline tracking:

- Detect Fileless and PowerShell attacks, lateral movement, memory exploits, script misuse, and more
- LevelBlue Labs and LevelBlue OTX integrations with SentinelOne for enhanced detections

## Respond

Respond and recover with automatic or one-click actions:

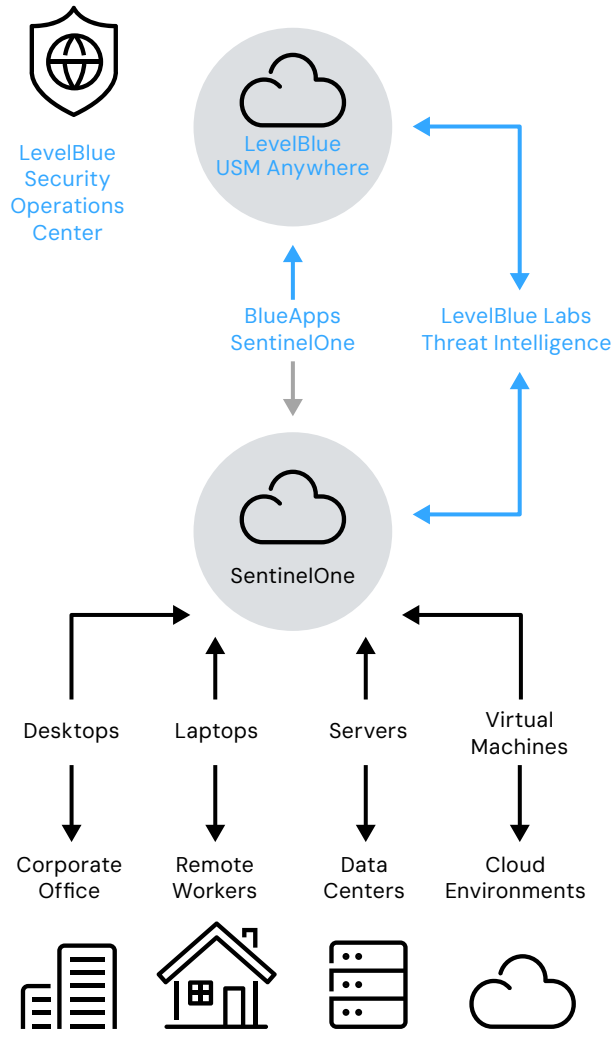
- Kill malicious processes and isolate infected endpoints from the network
- Clean up or rollback endpoints without re-imaging or writing scripts
- Customized Incident Response Plan

## Hunt

Deep Visibility and Active EDR provide the insights and tools to easily conduct threat hunting and investigations:

- Store historical EDR data for 14 days, with extended data retention available for purchase
- Threat data and alerts are retained for one year

## How It Works



## Managed Security Service Benefits

LevelBlue Managed Endpoint Security with SentinelOne includes high-touch onboarding support and system setup, and 24/7 threat monitoring and management by the LevelBlue SOC. This helps alleviate the cybersecurity skills shortage, as well as the burden of daily operations and troubleshooting, at a cost that is often lower than hiring a specialist in-house.

## Onboarding

- Set up environment including implement console, create users, complete platform integration, and configure policies
- Guidance and recommendations provided throughout agent deployment
- Policy tuning by creating exclusions, filtering or suppressing rules, creating orchestration rules, and changing policies
- Create an Incident Response Plan (IRP) and keep it updated to provide a common framework of procedures for investigating and responding to security incidents
- Training of the platform, including an overview of the agents, platforms, integration tools, and demo of the management consoles

## LevelBlue SOC Management

- Enhanced detections through the LevelBlue Open Threat Exchange (OTX) and LevelBlue Labs threat intelligence to improve detections on the agent and the platform
- Triage alarms to identify actionable security threats, update alarm status, or open investigations
- Investigate threats by gathering additional forensic information, update the severity, and determine remediation steps
- Respond to threats, per the IRP, and remediate threats by taking actions including to isolate, disconnect, or rollback an agent
- Ongoing policy tuning based on recurring false positive exclusions, block lists, or policies can be updated
- Schedule recurring analyst meetings to review recent investigations, outcomes, and any compliance or audit reporting need

## Why LevelBlue Managed Endpoint Security with SentinelOne

**Deep technical integration** enables the LevelBlue SOC management team to help detect more threats and act faster

- Orchestrated and automated incident response for your endpoints
- LevelBlue Labs Open Threat Exchange (OTX) IOCs correlated with SentinelOne agent detections delivers added context and threat detection
- LevelBlue Labs informs threat hunting on SentinelOne EDR data, yielding richer insights and easier detection of evasive threats

**Single LevelBlue SOC team** manages multiple LevelBlue offers for even greater protection

- Monitors and manages multiple distinct threat detection technology stacks
- Correlated alerts add context and better detections
- Single point of contact for simplified experience

LevelBlue

# 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.**

**Contact us to learn more, or speak with your LevelBlue sales representative.**