Fight ransomware and quickly respond to advanced cyberattacks

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

- AT&T AlienLabs 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

AT&T 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.

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

AT&T 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 premise or cloud, physical or virtual), and cloud containers. You'll have consistent protection across Windows, MacOS, and Linux.
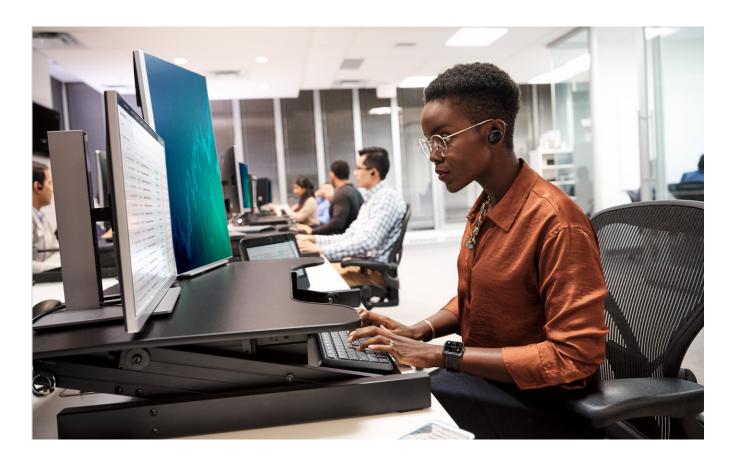
AT&T Endpoint Security with SentinelOne also provides autonomous protection. Even when users are working offline and endpoints are not connected to the cloud, the agent can continue to search for malicious files or malware and take action automatically.

Ransomware attacks are growing in size and sophistication. In the event of a ransomware attack,

AT&T Endpoint Security with SentinelOne can take your Windows systems back to a previously clean state.

AT&T Endpoint Security with SentinelOne is designed so you can monitor, investigate, and manage security incidents yourself. AT&T Business provides technical support weekdays during business hours. Training is also included. However, 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 AT&T Managed Endpoint Security with SentinelOne.

To determine which solution is right for your business, please see comparisons in the following table.

	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	✓	

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 AT&T Managed Endpoint Security with SentinelOne. Learn more at https://cybersecurity.att.com/products/sentinel-one.

Hello, I'm Wendy Oswald
with ZTrust Advisors
Please call me at +1-561-866-4538
or email me at wendy@ztrustadvisors.com

PRODUCT BRIEF