AT&T Business

Protect your business with leading endpoint security and world class managed services

Boldly embrace the 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. AT&T 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
- 24x7 monitoring by a dedicated AT&T Security Operations Center (SOC) team
- AT&T AlienLabs delivers continuous threat intelligence to help keep your defenses up to date
- Provides policy configuration, threat monitoring and response, and on-going 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, AT&T 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 AT&T Alien 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
- AT&T Alien Labs and OTX integrations with SentinelOne for enhanced detections

Respond

Respond and recover with automatic or one-click actions:

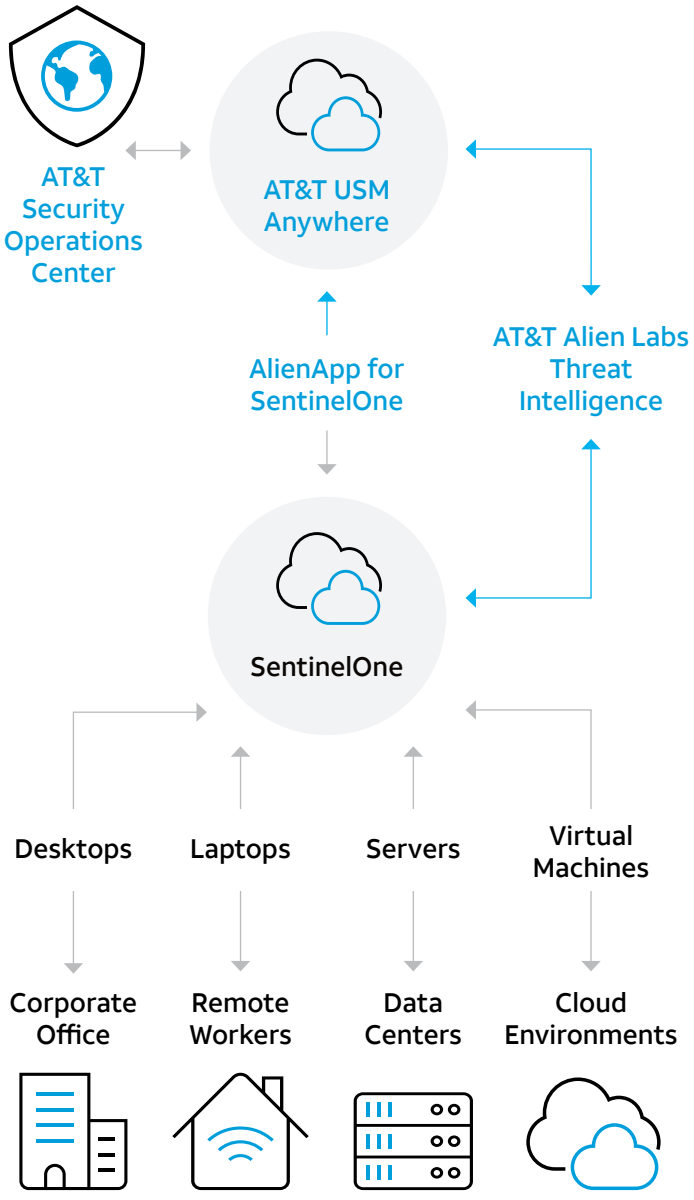
- Kill malicious processes and isolate infected endpoints from the network
- Clean up or rollback endpoints without re-imaging or writing scripts
- Customized Incident Response Plan

Hunt

Deep Visibility and ActiveEDR 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:



Secure Containerized Workloads in the Cloud

As businesses increasingly rely on cloud workloads, cloud security is more important than ever before. With new license types for Kubernetes containers or K8s, you can now protect a range of workloads in the cloud. Secure VMs and containers from a variety of sophisticated attacks, including zero-day attacks. Gain visibility through correlated event telemetry that is mapped to MITRE ATT&CK TTPs which includes K8s metadata. With Kubernetes licenses, AT&T Managed Endpoint security with SentinelOne can help protect all your endpoints including workstations, servers, virtual machines, and cloud workloads.

Enhance EDR Capabilities with Add-On Features

Take advantage of add-on features to increase visibility across all endpoints in your organization and improve threat hunting and automated response.

Ranger

Protect endpoints from compromised assets on your network, including those that don't support an S1 agent.

- 1-click network visibility and control over unknown and IoT network devices
- Machine learning device fingerprinting via active and passive scanning
- Highly configurable per subnet
- No added software, hardware, or network changes

Extended Data Retention

Extend EDR data retention in the SentinelOne cloud beyond 14 days to enhance threat hunting with historical EDR data.

- Choose between 30, 90, 180 and 365-day options

Binary Vault

Retain files for forensic analysis and integrate with other security tools.

- Files are stored in the SentinelOne cloud for up to 30 days for investigation
- Automatically upload executables to the SentinelOne cloud
- Integrate with tools such as a sandbox or SOAR application

Remote Ops (NEW)

Remotely investigate threats on multiple endpoints across your organization.

- Accelerate incident triage and response with a pre-built library of scripts
- Eliminate time consuming efforts to collect and consolidate forensics data
- Evaluate security defenses to identify potential compromises before an incident occurs

Cloud Funnel (NEW)

Data subscription enabling the storage of endpoint EDR data locally in your data lake.

- Correlates Deep Visibility EDR data with non-SentinelOne data sources.
- SIEM and SOAR Integration
- Expedite audit response
- Simplify data extraction with sample code from Kafka

STAR Pro (NEW)

Customize and automate detection rules that fit your environment. With STAR Pro, you can create up to 400 custom rules.

- Augment SIEM data with low volume, high-value telemetry
- Proactively monitor and respond by turning queries into automated hunting rules
- Simplify queries with easy to use, powerful Deep Visibility query language with regular expression support

Managed security service benefits

AT&T Managed Endpoint Security with SentinelOne includes high-touch onboarding support and system setup, and 24x7 threat monitoring and management by the AT&T Security Operations Center (SOC). This helps alleviate the cybersecurity skill 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 the management consoles

AT&T SOC Management

- Enhanced detections through the Open Threat Exchange (OTX) and AlienLabs 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 AT&T Managed Endpoint Security with SentinelOne

Deep technical integration enables the AT&T SOC management team to help detect more threats and act faster

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

Single AT&T SOC team manages multiple AT&T 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

About AT&T Cybersecurity

AT&T Cybersecurity's enterprise-grade technologies provide phenomenal threat intelligence, collaborative defense, security without seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning — helping to enable our customers around the globe to anticipate and act on threats to protect their business.