AT&T

Next-generation endpoint security with world class managed services

AT&T Managed Endpoint Security with SentinelOne

Current State of Endpoint Security

Prime Targets
70% of breaches originate on the endpoint*

Sophisticated Attacks
and insufficient protection against them

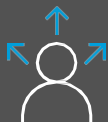**Multiple Agents**
for each endpoint security function

Overwhelmed Staff
who are unable to act quickly and confidently

AT&T Security Operations Center (SOC) 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(s) in-house.

Experience

Visibility

Comprehensive Endpoint Security

AT&T Cybersecurity

- The largest MSSP in the world[1]
- 25+ years of experience in delivering managed security services
- Dedicated team of security analysts
- Certifications including GSE, CISSP, CEH, CompTIA Security+, and more

AT&T Alien Labs Threat Intelligence

- USM sensor network – 20 million threat observations per day
- AT&T Alien Labs Open Threat Exchange (OTX)- 145,000 security professionals submitting 20 million threat indicators per day
- Collaboration with AT&T CSO– 446 PB of traffic from 200 countries and territories

SentinelOne® Autonomous Protection

- MITRE ATT&CK test - APT 29: #1 Most Total Detections2; correlated alerts with comprehensive storyline
- 1 agent: next-gen Antivirus, EPP, and EDR Physical and virtual workstations, servers, and cloud containers
- 3 OS types: protection for Windows, macOS, and Linux endpoints
- Protection even while endpoint is offline

AT&T Security Operations Center (SOC) 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(s) in-house

A high-touch service delivery model

- Platform onboarding
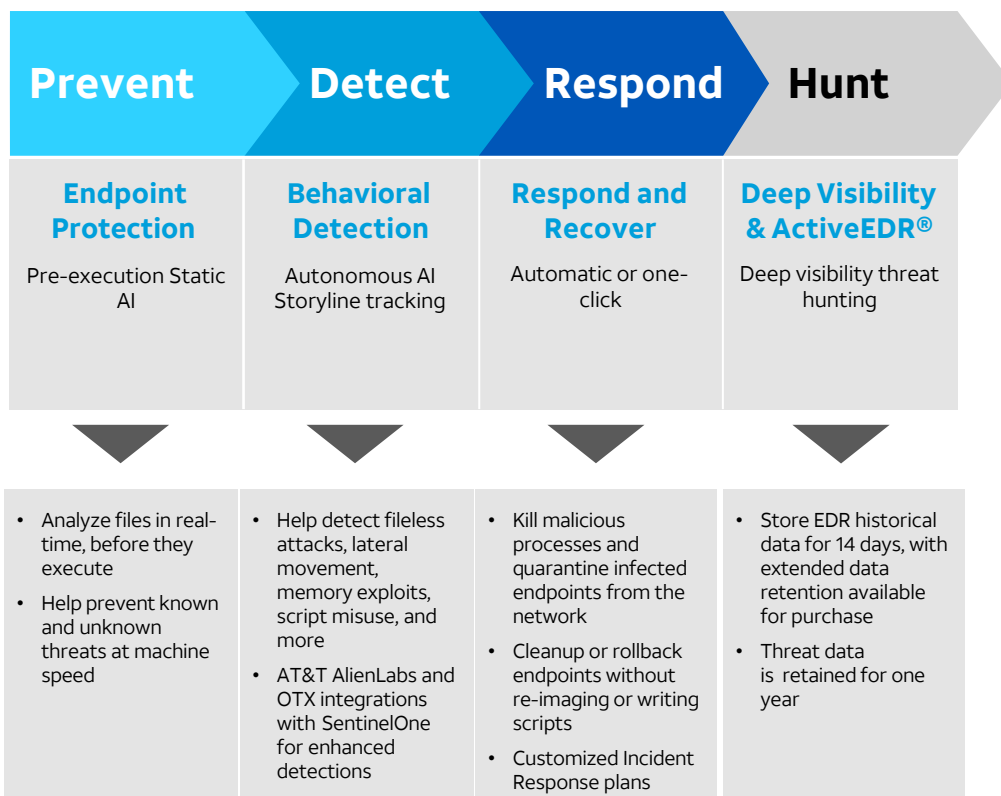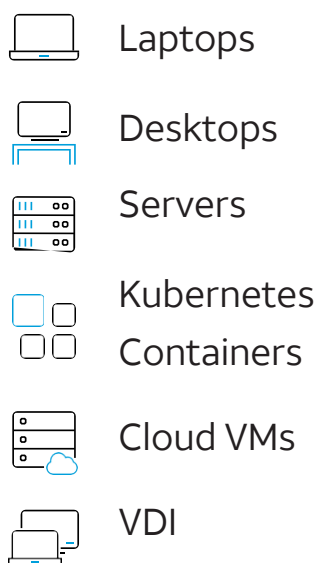- Guidance on agent deployment
- Initial policy tuning
- Customer training
- Custom incident response plan
- Incident response retainer available

Continuous monitoring, management, support

- 24x7x365 eyes on glass
- Review and triage alarms
- Investigate and respond to threats
- Provide ongoing system fine-tuning
- Regular reviews with Tier 2 Analyst
- Ticket resolution and support

AT&T Cybersecurity

How it works

AT&T

Endpoint protection, detection, response, and control for advanced forensic mapping and automated response.

SentinelOne® Endpoint Security for the Entire Attack Chain

- Laptops
- Desktops
- Servers
- Kubernetes Containers
- Cloud VMs
- VDI

Prevent	Detect	Respond	Hunt
Endpoint Protection	**Behavioral Detection**	**Respond and Recover**	**Deep Visibility & ActiveEDR®**
Pre-execution Static AI	Autonomous AI Storyline tracking	Automatic or one-click	Deep visibility threat hunting
• Analyze files in real-time, before they execute • Help prevent known and unknown threats at machine speed	• Help detect fileless attacks, lateral movement, memory exploits, script misuse, and more • AT&T AlienLabs and OTX integrations with SentinelOne for enhanced detections	• Kill malicious processes and quarantine infected endpoints from the network • Cleanup or rollback endpoints without re-imaging or writing scripts • Customized Incident Response plans	• Store EDR historical data for 14 days, with extended data retention available for purchase • Threat data is retained for one year

Why AT&T Managed Endpoint Security with SentinelOne

Through **deep technical integration**, the AT&T AlienApp and AT&T Alien Labs Open Threat Exchange provides richer insights and easier detection of evasive threats to help enable the AT&T SOC management team to detect more threats and act faster

The AT&T SOC management team can provide a **simplified experience** by managing multiple AT&T offers while providing better protection through correlated alerts

AT&T Cybersecurity offers **end-to-end solutions**, from the endpoint to the network to the cloud.

AT&T Cybersecurity