PROTECT PILLAR — ENDPOINT SECURITY

SentinelOne Singularity

SentinelOne

Modern cyber threats don't announce themselves. They move fast, hide in plain sight, and bypass traditional antivirus tools before your team even knows an attack is underway. SentinelOne changes that — using artificial intelligence to detect, stop, and recover from threats automatically, on every device, everywhere.

- Gartner Magic Quadrant Leader 2025
- MITRE ATT&CK — 100% Detection
- AV-TEST Certified
- EPP + EDR + XDR in One Agent

OAS · Protect. Detect. Recover.

Prepared 11 September 2026

SOLUTION OVERVIEW

The Three Pillar Solution

OAS's Three Pillar Solution is a **methodology** — a complete approach to defending against malware and ransomware attacks on all devices across your organisation. The solution is implemented using **N-able SentinelOne EDR** and is designed to give your business continuous, autonomous protection — stopping threats before they cause damage, detecting what gets through, and recovering rapidly when needed.

- **Protect** — stopping threats before they cause damage
- **Detect** — identifying what gets through
- **Recover** — restoring operations rapidly when needed

PLATFORM OVERVIEW

What SentinelOne Is — and What It Isn't

SentinelOne Singularity is not simply a better antivirus. It is a complete endpoint protection platform — a single, lightweight agent installed on each device that handles prevention, detection, response, and recovery, all without needing a human to approve every action.

THE CORE ENGINE

Behavioural AI — Not Signatures

Traditional antivirus matches files against a list of known threats. SentinelOne watches how software *behaves* — catching attacks that have never been seen before, because suspicious behaviour is suspicious behaviour, regardless of the file's name or origin.

AUTONOMOUS RESPONSE

Stop Threats Without Waiting for a Human

When a threat is confirmed, SentinelOne acts immediately — terminating the offending process, isolating the device from the network if needed, and in ransomware cases, rolling back encrypted files to their clean state. All in seconds, not hours.

ONE AGENT, FULL PICTURE

Every Event, Connected and Visible

Every click, file write, network connection, and process on a protected device is recorded and linked into a complete attack story — giving your OAS team full forensic visibility from the moment a threat enters to the moment it is contained.

KEY CAPABILITIES

What It Does For Your Business

Six capabilities that make SentinelOne the protection standard for organisations that cannot afford downtime, data loss, or the slow response of legacy tools.

Stops Threats Before They Execute

Before any file or script is allowed to run, SentinelOne's AI analyses its structure and intent. Known and unknown malware — including brand-new variants — are blocked before they can cause any damage, with no signature database required.

PRE-EXECUTION AI

Catches What Others Miss

Many modern attacks never write a file to disk — they run entirely in memory using legitimate Windows tools. SentinelOne watches the behaviour of running processes in real time, catching these "invisible" attacks that traditional antivirus cannot see.

RUNTIME BEHAVIOURAL DETECTION

Ransomware Rollback in One Click

If ransomware does attempt to encrypt your files, SentinelOne detects the encryption behaviour, halts the process, and restores affected files to their pre-attack state — automatically, from the management console. Recovery in minutes, not days.

1-CLICK ROLLBACK

Full Attack Story, Not Just Alerts

Rather than generating a flood of disconnected alerts, SentinelOne's Storyline technology presents each incident as a complete, visual chain of events — from the first entry point through every action taken — so your OAS team understands exactly what happened.

STORYLINE VISUALISATION

Instant Device Isolation

If a device is compromised, your OAS team can cut it off from the entire network in seconds from the management console — stopping lateral movement and preventing the attack from spreading to other machines — while keeping the management connection open.

REMOTE NETWORK ISOLATION

Agent That Protects Itself

Sophisticated attackers try to disable your security tools before deploying their payload. SentinelOne's anti-tamper protection means the agent cannot be stopped, uninstalled, or bypassed by any unauthorised process or user — even with administrator rights.

ANTI-TAMPER PROTECTION

WHY IT MATTERS

SentinelOne vs Traditional Antivirus

Legacy antivirus was built for a different era. Modern attacks — particularly ransomware, fileless malware, and AI-generated threats — were designed specifically to bypass signature-based tools. Here is how the two approaches compare on what matters most.

Traditional Antivirus

- **How threats are detected** — Matches files against a database of known threats. New and modified threats go undetected until the database is updated.
- **Protection when offline** — Depends on regular definition updates via internet. A device that hasn't updated recently has gaps in protection.
- **Fileless attacks** — Cannot detect attacks that run in memory without writing a file to disk. A large and growing category of threats go undetected.
- **Ransomware response** — May detect known ransomware. No recovery capability — remediation means manual rebuild or restoring from backup.
- **Incident visibility** — Single-event alerts with no context. No way to see how an attack entered, what it touched, or how far it spread.
- **Resource impact** — Scheduled full-disk scans cause significant slowdown. Heavy I/O load particularly affects older machines and servers.

SentinelOne Singularity

- **How threats are detected** — AI analyses behaviour before and during execution. Detects zero-day attacks and novel variants without any database.
- **Protection when offline** — Fully self-contained AI on the device. No internet connection needed — protection is identical in the office, at home, or overseas.
- **Fileless attacks** — Monitors the behaviour of running processes directly. No file on disk needed — suspicious behaviour is caught regardless.
- **Ransomware response** — Detects encryption behaviour, halts the process, and restores files to their pre-attack state. Recovery in minutes.
- **Incident visibility** — Complete visual attack chain from first entry to containment — every process, file, and connection mapped automatically.
- **Resource impact** — Lightweight agent with no scheduled scans. Minimal CPU and memory footprint in normal operation.

PROTECTION EVERYWHERE

Your Team Is Protected Wherever They Work

One of the most important differences between SentinelOne and legacy tools is that protection does not depend on your corporate network. The AI runs entirely on the device — so your people are just as safe working from home or travelling abroad as they are at the office.

In the Office — Full Operation, Real-Time Visibility

- All AI protection active with live cloud telemetry

- Your OAS team has real-time device visibility and alerts
- Remote isolation, rollback, and shell access available
- Policy changes push to devices within minutes

Working From Home — Full Protection, No VPN Required

- AI prevention and detection run entirely on-device
- No corporate network or VPN needed for protection to work
- Threats blocked and remediated automatically
- Events sync to the cloud when the device reconnects

Travelling or Overseas — Full Protection, Any Network, Any Country

- Protection identical on hotel Wi-Fi, airport, or cellular
- AI models cannot be bypassed by blocking cloud endpoints
- Anti-tamper prevents removal even on untrusted networks
- All events timestamped and synced on reconnection

Why this matters for South African businesses: with remote and hybrid work now standard, your endpoints are frequently outside the corporate perimeter. Tools that rely on your network for protection leave roaming employees exposed. SentinelOne's on-device AI means every laptop is fully protected regardless of where it connects — a critical consideration for organisations with field teams, executives who travel, or staff working across multiple sites.

SCOPE OF PROTECTION

What SentinelOne Replaces — and What It Doesn't

Understanding scope helps you plan your overall security architecture. SentinelOne is an endpoint platform — exceptionally comprehensive at the device layer, and designed to work alongside complementary tools for email, network, and backup.

What SentinelOne Replaces

- Traditional and modern antivirus suites — Sophos, ESET, Trend Micro, Symantec, McAfee
- Standalone EDR tools — detection, investigation, and response are built in to a single agent
- Host-based intrusion detection and prevention (HIDS/HIPS)
- Host firewall management — included in the Control tier
- USB and removable device control tools
- Manual rollback processes for ransomware recovery

What It Works Alongside

- Email gateway and mail filtering — SentinelOne protects the endpoint, not the mail flow
- Network firewall and perimeter security — SentinelOne is endpoint-centric, not

network-perimeter

- Backup and disaster recovery — rollback complements but does not replace full DR
- DNS filtering and web proxy — these address different threat surfaces
- SIEM platforms for non-endpoint log aggregation

HOW IT'S DELIVERED

Delivered as a Managed Service by OAS

SentinelOne is powerful — but its value is maximised when monitored and managed by experienced hands. OAS handles the full lifecycle on your behalf.

24/7 Monitoring & Alert Response

OAS monitors your SentinelOne console continuously. Threats are reviewed, triaged, and acted on — you are notified of what matters, not overwhelmed with noise.

ALWAYS ON

Deployment & Policy Management

We handle agent rollout, policy configuration, and ongoing tuning across your entire fleet — ensuring protection is correctly calibrated for your environment from day one.

FULLY MANAGED

Reporting & Compliance Evidence

Regular reports covering threat activity, device coverage, and policy compliance — giving you the documentation you need for POPIA accountability and audit requirements.

POPIA READY

Incident Response Support

When an incident occurs, OAS is your first call. We investigate, contain, and remediate — using SentinelOne's tools to resolve threats quickly and keep your business running.

EXPERT SUPPORT

Ready to Replace Your Antivirus?

Speak to an OAS consultant about deploying SentinelOne Singularity as part of your Three Pillar protection strategy.

TELEPHONE

+27 11 485 3454

EMAIL

info@oas.co.za

WEB

https://www.oas.co.za

OFFICE

25 Durham Street, Raedene Estate, Johannesburg

Request a demo: https://www.oas.co.za/contact/demo

Open Architecture Systems — Protect. Detect. Recover. Citrix Platinum Partner since 1987.