SentinelOne

Securing MacOS

Autonomous Endpoint Protection That Saves You Time

Sentinelone - Autonomous Endpoint Protection That Saves You Time

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

The Need to Secure Apple's MacOS

Enterprise Security is only as strong as its weakest link, and macOS endpoints are not as secure as popularly believed. Malware authors know how to circumvent Apple's built-in protections, and as the use of Macs in the Enterprise has risen, so has the number of threats.

The Solution - Sentinelone

The SentinelOne agent offers you a single window to peer inside all your endpoints, whether they are running macOS, Linux or Windows.

Multiple Engines

We use static AI to stop threats pre-execution and behavioral AI to identify threats on-execution. Automated EDR ensures that your Mac fleet is protected against all attack vectors.

Control What Devices Your Users Can Plug into Your Macs

SentinelOne's Device and Firewall Controls are integrated into the same management console. It's designed for extreme ease-of-use and does not require a huge SOC team to manage.

Minimal Impact on Performance

SentinelOne Agent's core components are sandboxed and tamper-proof for enforced security. In-process anti-exploitation, ROP, and stack pivot detection enable exploits to be reported and stopped even if they are unknown. Our macOS offering is autonomous and protects your endpoints even when offline.

Replacing Legacy AV Solutions

Legacy solutions cannot protect your network from adversaries using encrypted traffic, and they cannot protect your endpoints from novel threats. SentinelOne offers a single agent architecture, available seamlessly in cloud-delivered or on-premises deployment models. We provide unparalleled endpoint detection and response (EDR) capabilities integrated with MITRE ATT&CK framework to provide both context and relevance with full context monitoring and control of every aspect of the endpoint device.

Sentinelone's MacOS Benefits

- Pre, on, and post-execution protection and maximum endpoint visibility aperture
- Decreases the attack surface without performance impact; Core components are separated and sandboxed to enforce security
- In-process anti-exploitation for MacOS (ROP & stack pivot detection)
- ROP and stack pivot detection enables stopping and reporting exploits as they occur on the running system, even if the exploit itself isn't known
- Tamper-resistant
- Autonomous, protects in offline mode

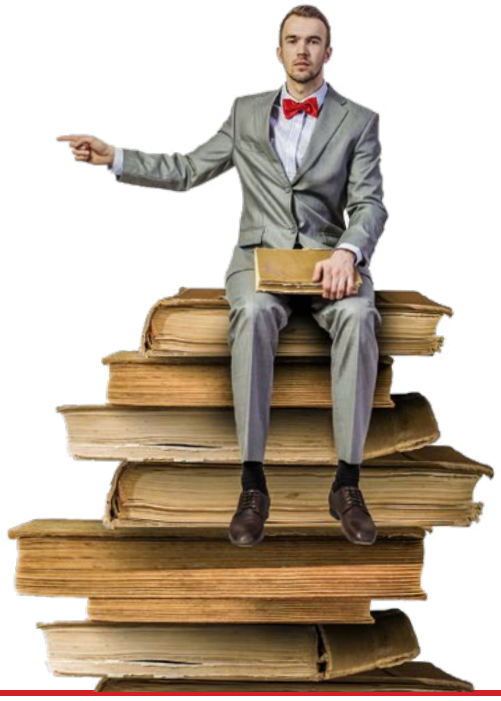
Our Mission

Our mission is to enable enterprises to most effectively and efficiently manage risk. We implicitly acknowledge that security teams have to do more with fewer people while constantly stay ahead of the evolving threat landscape. These realities define our design principles; we're just getting started transforming endpoint security and beyond!

READY FOR A DEMO?

SentinelOne™

Bedankt voor uw interesse in SentinelOne!



Hopelijk heeft dit document u de benodigde informatie en inzicht gegeven waar u op zoek naar was.

Wilt u meer informatie over SentinelOne? Hier hebben we nog meer voor u:

» **SentinelOne whitepapers en e-books**
» **SentinelOne videos**

Andere tools die uw organisatie weerbaarder maken

ProteQtor IT Security is niet alleen reseller partner van SentinelOne, maar biedt nog meer cybersecurity tools aan om uw organisatie zo weerbaar mogelijk te maken.

Hieronder tools die wellicht interessant zijn ter bescherming van uw organisatie:
» Bescherm smartphones en tablets met **Lookout mobile security**
» Beveilig uw e-mail met **Proofpoint email security**
» Train uw medewerkers met laagdrempelige **Wizer security awareness trainingen**
» Bescherm het inloggen met **Watchguard Authpoint multi-factor authenticatie**
» Voorkom bezoeken aan ongewenste websites met **NSOC360 Safeweb webfiltering**
» Krijg inzicht in de veiligheid van uw netwerk met **Guardian360 scans**
» Herstel verloren data met **NSOC360 Safedata online backup**

ProteQtor
Next-Gen IT Security

Laat hackers uw bedrijfscontinuïteit niet in gevaar brengen!

Cyberaanvallen bedreigen privacy, bedrijfskritische data, de reputatie en andere 'kroonjuwelen' die cruciaal zijn voor de continuïteit van uw organisatie. De vraag is allang niet meer 'of' uw organisatie aangevallen wordt, maar 'wanneer' uw organisatie (weer) aangevallen wordt. Het is essentieel om cyberaanvallen te voorkomen en de gevolgen van cyberaanvallen tot een minimum te beperken. Het feit dat u deze pdf leest, toont dat u dat belang inziet.

Vanwege de grootte, de complexiteit en de diversiteit van moderne cyberaanvallen is een multidisciplinaire aanpak nodig. We helpen u graag met praktische adviezen en effectieve oplossingen om deze aanpak te realiseren.

Met de juiste trainingen, tools en support helpen wij u hackers het hoofd te bieden en er voor te zorgen dat alles wat voor uw organisatie van waarde is, beschermd blijft.

Hulp nodig? Bel 088-0660770 of plan een afspraak in

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl