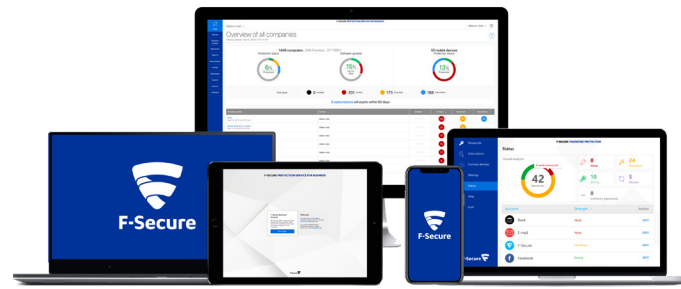Battlecard

F-SECURE VS SENTINELONE

F-SECURE STRENGTHS

Best protection: F-Secure has won the AV-TEST Best Protection award 7 times, and excelled in MITRE ATT&CK evaluations with 88% average visibility. SentinelOne has not won any AV-TEST awards, and in MITRE evaluation they delivered visibility of 88% across all rounds.

Platform support: SentinelOne also supports Mac and broad range of Linux distributions, but AV-TEST indicated performance degration on Mac. Also some Mac features appear to be missing, like remote response and response automation.

Complete portfolio: F-Secure has a complete portfolio including built-in patch management and extensive vulnerability scanning and management. SentinelOne is missing some vital security features, such as integrated patch management, application control and VPN support for the mobile devices.

Cyber security consulting services: F-Secure has own malware labs and offers a wide range of cyber security consulting services, including red teaming, incident response, cyber incident and resilience services that allow customers to respond to security breaches efficiently and effectively.

INDUSTRY CAUTIONS ABOUT SENTINELONE

"SentinelOne does not offer application whitelisting, nor does it offer sandboxing for suspicious file analysis (local, network or cloud). Workflow capabilities for large teams are limited. The EDR tool provides few guides or global contextual info. Watchlist alerts are limited to minimum three hours between runs, and thus, are not real time."

Gartner EPP MQ 2019

"New SentinelOne customers migrating from other enterprise solutions will miss add-ons like fully featured DLP and other extras that are not offered."

Gartner EPP MQ 2021

F-SECURE

Elements Endpoint Protection,
Endpoint Detection and Response

SENTINELONE

Singularity Complete

F-SECURE		SENTINELONE
✓	**PROTECTION LEVEL**	✗
F-Secure is the only vendor to have won the AV-Test's prestigious 'Best Protection' award in seven years since its inception. F-Secure also received the latest 'Top Product' for Windows, and 'Approved' for macOS.		SentinelOne has not won any endpoint protection tests and all their public tests are old. In recent SE Labs' Breach Response Test they "won" as the only vendor participating the test.
✓	**PC/MAC/LINUX**	⊖
F-Secure provides extensive endpoint security for Windows, macOS and Linux, with strong macOS capabilities, and optional cloud-native Microsoft 365 protection and vulnerability management capabilities.		SentinelOne supports wide range of operating systems, including Windows, Mac and Linux. However, their Linux features are limited compared to Windows and macOS.
✓	**MOBILE DEVICES**	✗
F-Secure provides fully integrated mobile protection for Android and iOS, including: browsing protection, mobile VPN for priv acy protection, malware protection (Android) and support for many 3rd party MDM systems.		SentinelOne does not offer mobile protection even though back in 2018 Lookout announced partnership with SentinelOne to offer a way to secure mobile endpoints.
✓	**PATCH MANAGEMENT**	⊖
F-Secure provides fully integrated patch management to identify and prioritize software vulnerabilities. It can be set to deploy missing security patches automatically as soon as they are available.		SentinelOne's patch management is called Risk & Vulnerability Management even though it is limited to only application inventory and listing vulnerable applications.
✓	**CENTRAL MANAGEMENT**	⊖
F-Secure provides streamlined multi-company management with cloud-native, integrated and single agent security management across EPP, EDR, Microsoft 365 and vulnerability management.		SentinelOne has both cloud and on-premise management console options, and an S1 Mobile Admin app. Cloud console lacks true cloud native multi-company management.
✓	**DETECTION AND RESPONSE**	⊖
F-Secure provides automatic threat identification and response across multiple hosts, also with macOS and Linux. Detections are stored for 1 year. Great average visibility of 88% across MITRE ATT&CK all three rounds demonstrates consistency.		SentinelOne has limited telemetry coverage which reduces possibilities to detect advanced and targeted attacks. High average visibility of 90% across all three MITRE ATT&CK rounds, but only 74% visibility in the first round.
✓	**EXPERT SERVICES**	⊖
World-class cyber security consulting and experts are available as a service through built-in 'Elevate to F-Secure' product feature under 2-hour target SLA 24/7/365. Advanced managed threat hunting and response service is also available.		SentinelOne doesn't offer similar elevate option, Vigilance managed detection and response (MDR) service requires continuous subscription. SentinelOne doesn't offer other cyber security consulting services.

F-Secure

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure

F-Secure®