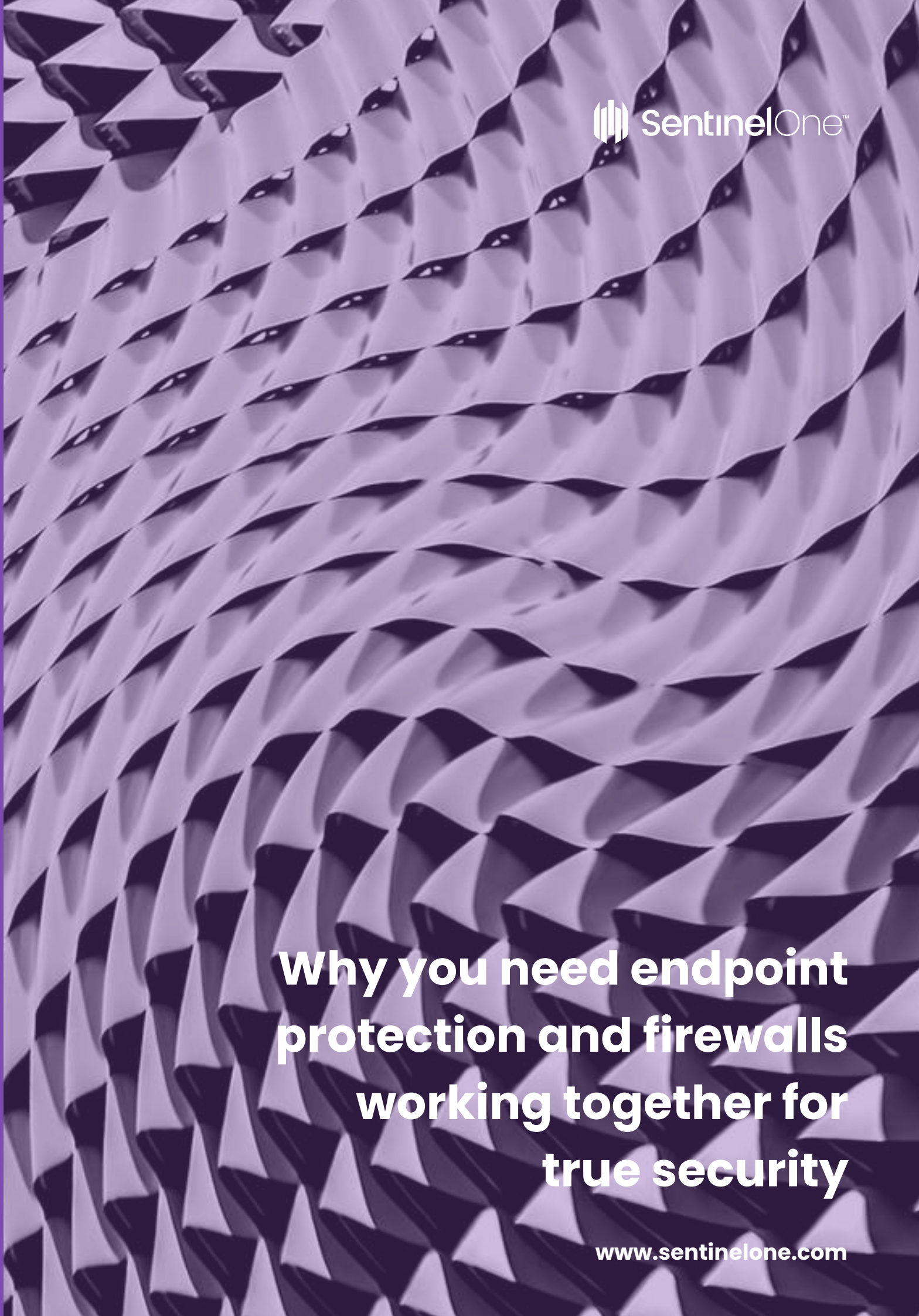

SentinelOne™
Why you need endpoint protection and firewalls working together for true security
www.sentinelone.com

SentinelOne™

The Advancing Cyber Threat

Why you need endpoint protection and firewalls working together for true security

The advancing cyber threat

Cyber security presents an increasingly difficult challenge for organisations today, with both the volume and sophistication of attacks continuing to increase. The accessibility of malware that even an unskilled cybercriminal can carry out a devastating campaign, while more skilled attackers can evade defences to steal or damage crucial files and systems.

Some of the biggest threats facing businesses today include:

Ransomware

Ransomware, specialised malware which spreads through a network to encrypt and exfiltrate essential files and systems, is one of the most difficult cyber challenges facing organisations. A single click on a malicious file or link can quickly shut down entire operations until the company can restore the files or takes a chance and pays the ransom demand. Even after paying ransom demands, many of today's cybercriminals do not return data or even unencrypt files. Incident response and investigation expenses, additional IT resources, operational downtime, reputation hits, and lost business all combine to make a ransomware infection an extremely costly incident. SentinelOne discovered that ransomware attacks are costing individual businesses an average of $833,716 per annum.

Advanced Persistent Threats (APTs)

With a combination of social engineering practices and previously unseen malware exploiting zero-day vulnerabilities, advanced threat actors can penetrate even the most secure defences. Once attackers are inside a network or system, the use of vectors such as fileless malware means that they can harvest data and prepare further attacks while remaining undetected for months at a time or even longer.

To protect against these increasingly sophisticated threats, organisations must take an interconnected, holistic approach to security. One of the most effective strategies is to combine technologies that can identify threats across the enterprise network and act to prevent them in concert before they can spread. Integrating a firewall solution with an next-gen protection platform, including integrated Endpoint Detection and Response (EDR) capabilities, allows the two solutions to work together and provide complete, integrated security.

The power of connecting with Fortinet

To help organisations establish a complete enterprise defensive network, SentinelOne has partnered and integrated with Fortinet. The relationship combines Fortinet's market leading next generation firewall technology with SentinelOne's powerful next-gen endpoint platform which combines prevention, detection, and response in a single autonomous agent.

In 2017, SentinelOne joined Fortinet's Fabric Ready-Program, a scheme designed to help connect its solutions with those of other vendors to combat the highest level of advanced threat. Now SentinelOne has taken the partnership to a new level with the SentinelOne-Fortinet Connector, making it incredibly easy to integrate the SentinelOne Endpoint Protection Platform with Fortinet's suite of solutions.

Powered by over 200 APIs, SentinelOne users can connect seamlessly with any of Fortinet's offerings, including email security solution FortiMail and identity and role-based access management tool FortiAuth. However, the most powerful synergy comes from its next generation firewall and sandbox capabilities;

FortiGate

FortiGate - an award-winning firewall that provides granular visibility across the entire digital perimeter, protecting enterprise networks from both known and unknown threats, zero-day exploits and advanced malware.

FortiSandBox

FortiSandbox – Central to Fortinet's Advanced Threat Protection (ATP) capabilities, FortiSandbox provides actionable threat intelligence in real time to identify and mitigate malware and other threats the moment an attack begins.

FortiGate

FortiGate

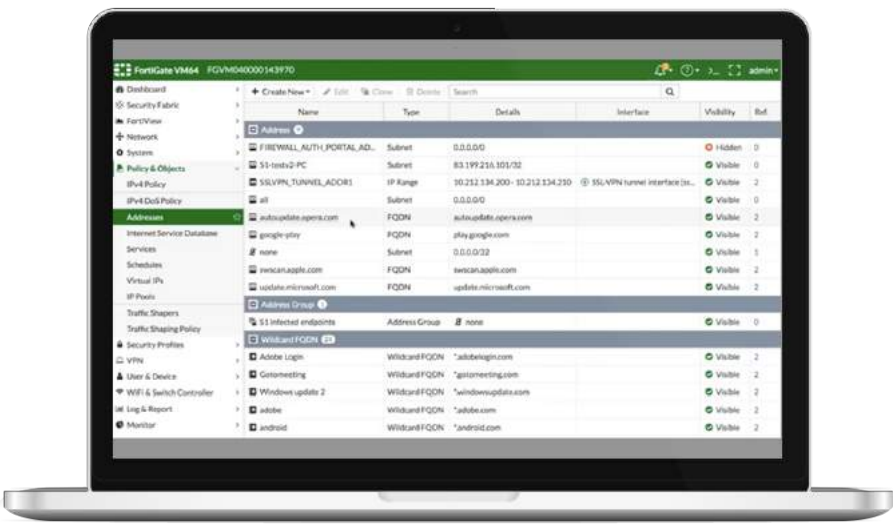
FortiGate is a Next Generation Firewall (NGFW) designed to protect the entire network, from the edge to the datacentre and from connected IoT devices to the cloud network. The award-winning solution's capabilities earned Fortinet a leading position in Gartner's 2017 Magic Quadrant for Enterprise Network Firewalls as well as the leading position in NSS Labs' 2018 NGFW Group Test.

Using purpose-built security processes and threat intelligence delivered from FortiGuard labs, FortiGate provides granular visibility of all network activity, including encrypted traffic, to identify both known threats and previously unknown zero-day exploits and advanced malware. FortiGate is also designed around ease of use, providing automated visibility into all applications, users and networks to create an accessible view of the entire digital attack surface.

Enhancing Threat Detection with SentinelOne

The SentinelOne Endpoint Protection Platform (EPP) integrates with FortiGate to share its real-time, perimeter-less threat data with the dynamic firewall policy. Working together, the two solutions can immediately detect and isolate a compromised endpoint device via both its IP and Mac addresses - inside and outside the confines of the enterprise network.

Once a compromised endpoint is detected by SentinelOne, FortiGate instantly adds it to the "infected" group, preventing the device from accessing the corporate network. A combination of automation and straightforward network controls means that handling an active threat becomes far easier and the risk of escalation is greatly diminished. The power of the firewall is extended by each of the SentinelOne endpoints, serving as sensors and communicating with the firewall. Once the threat is resolved and the endpoint is verified to be clean, the device is automatically removed



FortiSandBox

FortiSandbox

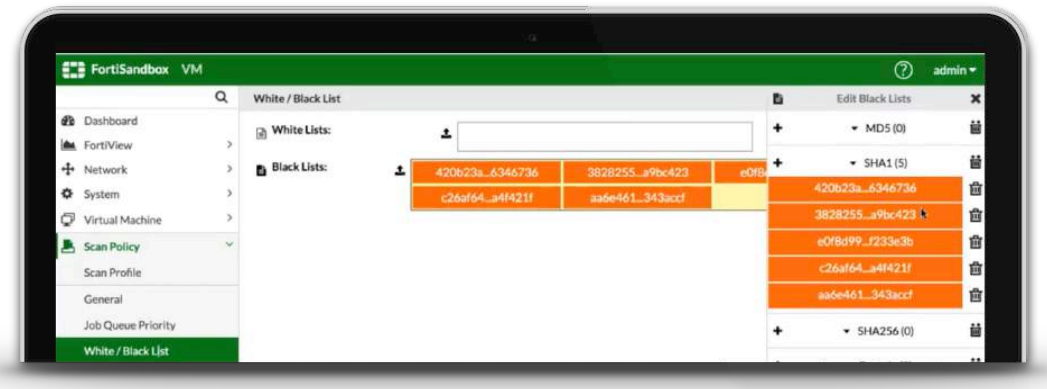
FortiSandbox is at the core of Fortinet's advanced threat protection capabilities. The solution combines advanced detection and automated mitigation to understand and block targeted attacks. The FortiSandbox minimises damage to the organisation by providing the security team with real attack artefacts and actionable insights in real time.

Sharing intelligence with SentinelOne

FortiSIEM

SentinelOne's Behavioural AI engine constantly monitors and maps each running process for incongruous behaviours locally at the endpoint to provide real-time, anadromous analysis. These two solutions complement one another, each providing their own dynamic analysis capabilities, creating synergy that leaves no gaps in the defences for advanced threats to slip through.

Any threat intelligence from the SentinelOne protected endpoint is shared with FortiSandbox in real time, enabling the solution to automatically update its blacklists. The entire network covered by FortiSandbox is therefore instantly protected against any malware so that even zero-day exploits are detected and stopped.



Syncing with FortiAuthenticator

FortiAuthentificator

The synchronisation with FortiGate and FortiSandbox is strengthened further by adding FortiAuthenticator's role-based access management to the network. By sharing its endpoint threat intelligence with FortiAuthenticator, SentinelOne enables the solution to instantly block a user ID when a machine is compromised or even in a suspicious stage and needing investigation. This prevents the attacker from using the hijacked devices and also stops them from using stolen credentials to log in elsewhere to continue the attack.

SentinelOne Connector - Empowering the Fortinet Security Fabric