SentinelOne

SentinelOne GDPR White Paper

How SentinelOne Helps Achieve GDPR Compliance

Executive Summary

Starting on May 25, 2018, GDPR sets strict new requirements for protection of personal data for EU residents, requiring all organizations that control and process PII to implement best in class technical measures to secure and prevent data breaches. In this document, learn:

- What is GDPR?
- What is its impact on your network?
- How SentinelOne helps achieve GDPR compliance?

GDPR's Impact On Organizations

Data Breach Prevention

GDPR (Articles 25 and 32) requires the implementation of effective endpoint protection solutions throughout organizations that can block, detect, and remediate the effects of malware infiltration through an organization's endpoints.

Data Privacy

GDPR (Article 25 & 33) requires companies who collect and process PII from EU citizens to implement comprehensive security measures to ensure adequate protection of PII, including the implementation of advanced technical security measures in the course of handling PII.

Data Security

GDPR (Article 32) requires organizations to implement technical measures to maintain an appropriate level of security for processing of personal data, ensuring the ongoing confidentiality, integrity, availability, and resilience of such processing systems and services is maintained.

Data Breach Notification

GDPR (Articles 33 & 34) requires covered organizations to notify a supervisory authority of data breaches within 72 hours of becoming aware of such breaches, unless the breach is unlikely to result in a relevant risk to data subjects' PII.

Data Breach Assessment

GDPR (Article 33) requires controllers to conduct a data protection impact assessment for high-risk processing activities. These are processing activities that rely on new technologies and are "likely to result in a high risk for the rights and freedoms of individuals."

Data Breach Remediation:

GDPR (Article 33) requires capabilities to remediate and mitigate the effects of a data breach.

+1 855 868 3733
sales@sentinelone.com

How SentinelOne Helps Achieve GDPR Compliance

Protection

- Using Static and Behavioral AI, SentinelOne prevents malware attacks. Continuous monitoring of all activity on the endpoint helps organizations proactively prevent, identify, and contain threats. Beyond preventing breach attempts in real time, SentinelOne helps organizations identify and contain threats, detect and eliminate ongoing breaches, and remediate the harmful effects of existing threats. Another aspect of proactive prevention is the isolation of a suspected endpoint by disconnecting it from the network upon detection of a suspicious event.

Visibility

- SentinelOne's Deep Visibility and automated EDR capabilities help customers understand the scope, source, and automated actions taken to remediate a suspicious event. It allows system administrators to configure specific policies for files containing PII. If a malicious event cannot be prevented before execution, information about the affected files will be sent to the console, enabling administrators to be aware and to take additional action. Administrators may configure File Integrity Monitoring to get alerts for any changes made in specific files containing PII.
- Deep Visibility enables encrypted traffic inspection, and as such, proves to be extremely effective in understanding phishing attempts and interactions with external data.

Remediation

- SentinelOne leverages Static and Behavioral AI to prevent and detect threats before they occur. If a threat is active, SentinelOne allows customers to remediate and mitigate the effects. After stopping attacks, SentinelOne allows rollback of the device to its pre-infected state and auto-immunization of any other endpoints on the network from the threat.

Monitoring

- SentinelOne's Vigilance automated SOC services offer security experts who proactively search, investigate, and advise on threat activity in an organization's environment, assisting organizations in detecting data threats and providing first response assistance as well as guidance in the event of an attack. The service helps organizations continuously monitor their SentinelOne instance, receive alerts on suspicious events, and execute policy-driven actions at machine speed to minimize threats.

BEFORE	DURING	AFTER
Static AI	**Behavioral AI**	**Automated EDR**
Prevent attacks Pre-execution	Constantly monitor and map each running process for incongruous behaviors	Automate remediation and response...even rollback

+1 855 868 3733
sales@sentinelone.com