[redacted]

[redacted] Data Categories [redacted]

[redacted] SentinelOne protects McDonald'scorporate offices and restaurant devices and endpoints at sca[redacted] [redacted]t offers protection by monitoring all locations globally and then sending the relevant information [redacted] Global Endpoint Security team can visualize, detect, and respond directly to security events.

Metadat[redacted] falls broadly into the following categories:

Endpoint Data • Machine detai[redacted] • Operating System • Workgroup/Domain • Installed applications
Network Data • Connection interface details • Network traffic details • Networked device details
[redacted]**Agent Data** • Agent version • Agent health status Console check-in timestamp
End User Data • Logged-in user/username • McD email address • Network usage details
Threat Detection Data • Associated process details • Associated file details • Associated endpoint status details

[redacted] helps identify not just malicious activity but also associated events in order to provid[redacted] with the complete Storyline picture of a suspected or actual compromise. [redacted] monitor vast amounts of machine metadata to help ensure malicious activity is not only caught but is also contextualized and traceable; this metadata is also used i[redacted] [redacted] machine learning engines to detect and protect endpoints autonomously from malicious activity. This metadata is sent to the cloud where it is processed and parsed to separate benign metadata from data relevant to securing th[redacted] enterprise. Benign metadata not associated with an event is discarded, helping ensure we see only security relevant data needed to take action when necessary.

[redacted] data retention schedule is as follows:

Event/Record Type	Retention Period
Device Threats (i.e. blocked device events)	1 year
Notifications from Agents	3 months
Device connection and firewall events	1 month
Private files in Binary Vault	1 month
Threat file fetch	1 month
Activity passphrases, users, and applications	7 days
All other file fetches	3 days

Only authorized users have access to view and download file content,

The vast majority of metadata is machine-generated and contains non-attributable datapoints such as process ID, operating system version, information about applications, and command-line arguments. In limited situations however, the metadata may contain personal data, such as that associated with usernames, file names and generalized location inferred from public IP addresses of the endpoint where the metadata is collected