

# SentinelOne

Cyber Security wordt een steeds belangrijker onderdeel van de IT omgeving. Om de risico's hierop zoveel mogelijk te beperken, kunnen simpele en uitgebreide maatregelen genomen worden. Op het gebied van Endpoint Security gebruiken we bij e-Quest SentinelOne.

## EDR: Endpoint Detectie en Respons

SentinelOne is een geavanceerde endpoint-beveiligingsoplossing die gericht is op het beschermen van endpoints, zoals laptops, desktops en servers. De software beschermt primair tegen cyberdreigingen waaronder malware en ransomware aanvallen. Het staat bekend om zijn geavanceerde AI-gestuurde detectie- en preventiemogelijkheden met functies zoals gedragsanalyse, machine learning, sandboxing, en endpoint-detectie en -respons (EDR). Deze benoemde EDR geeft de mogelijkheid voor het geautomatiseerd ingrijpen bij detectie van verdachte en kwaadaardige malware. Hiermee wordt de endpoint op dat moment volledig ontsloten van het netwerk waarmee het gevaar beperkt blijft tot het betreffende endpoint. SentinelOne geeft de beheerders van e-Quest inzicht in én controle over de beveiligingsstatus van de apparaten binnen uw bedrijf.

## Verkleinen van risico's

Met deze oplossing staat er een stabiele basis en wordt het risico verkleind dat het bij optreden van verdachte en kwaadaardige malware mogelijk impact heeft op de gehele omgeving. In tegenstelling tot traditionele anti-virussoftware, die slechts malware detecteren en in quarantaine zetten, zal SentinelOne ook alle onderliggende processen stoppen en opruimen.

