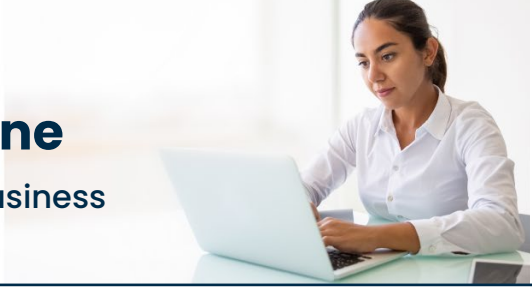
Castra's MXDR for SentinelOne

Enterprise-level Endpoint Security for Every Business



MXDR for SentinelOne includes:

Automated Incident Response **Custom Tuning from Castra SOC**

With MXDR for SentinelOne, organizations of any size can benefit from enterprise-quality security. This managed extended detection and response package combines SentinelOne with Castra's product expertise and highly effective operational talent.

We assign a dedicated primary security analyst to every new account. Your main point of contact will walk you through the process of implementing SentinelOne XDR designed to optimize detection and response capabilities. You'll receive a documented incident report plan that details every step Castra analysts take in response to suspicious activities and cyberattack attempts.

Round-the-Clock Security Comes Standard

This package puts Castra's 24x7 security operations center at your disposal. Guarantee peace of mind for your users with premium alarm monitoring and advanced response automation. We proactively adjust our threat detection systems to meet your organization's real-world needs and orchestrate comprehensive responses when suspicious activity occurs – 24 hours a day, 365 days a year.

Our US-based security operations center equips highly experienced analysts with some of the industry's most sophisticated technologies, including SentinelOne Singularity XDR. This gives our team deep visibility into emerging threats, allows us to explore the context of those threats, and mitigate attack risks before they cause severe damage.

Our analysts provide unmatched product expertise to customers, working continuously to reduce false positives and accelerate security event investigations. The faster analysts can conduct incident response investigations, the better your organization's security posture becomes.

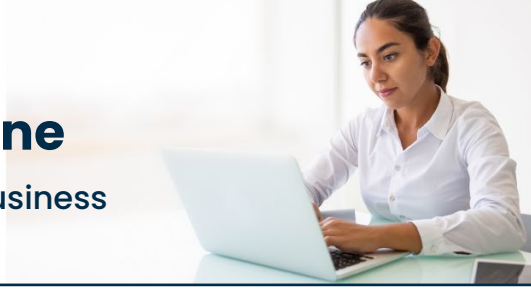
Automate Incident Response with SentinelOne Singularity XDR

A typical attack scenario might involve malware traveling through the network, landing in an email inbox, and then attacking a vulnerable endpoint. Organizations can't achieve

CASTRA
e: info@castra.io | p: 919.595.8560 (EST) | p: 408.476.8488 (PST)
a: PO Box 3222, Chapel Hill, North Carolina 27515

Castra's MXDR for SentinelOne

Enterprise-level Endpoint Security for Every Business



MXDR for SentinelOne includes:

Automated Incident Response **Custom Tuning from Castra SOC**

operational security while looking at those events independently of one another.

SentinelOne's XDR technology integrates multiple security controls into a single interface. Analysts conducting incident response can program the system to automatically isolate compromised endpoints, terminate unauthorized processes, and block additional executions. These pre-established rules can run the moment a user triggers them or operate as orchestrated one-click actions.

This comprehensive approach reduces the amount of time it takes to detect, investigate, and respond to security threats. Having Castra's expert team continuously fine-tune those rules enables small organizations to scale security performance for long-term growth.

Ensure Compliance with Custom Reports and Dashboards

Castra provides all MXDR subscribers with customized notifications and reporting services. Have alarm output notifications sent to the people who need to know about them in real-time. Show compliance-based dashboards and customized reports to company leaders and stakeholders. We also provide cloud-based monitoring solutions for event flow rates, system capacity, and performance.

Rely on your primary security analyst to help you deploy best-in-class security technologies with scalable expertise from our SOC. With Castra, the world's most advanced tools and techniques are no longer limited to large enterprises and public institutions – your organization can deploy them today.

CASTRA

e: info@castra.io | p: 919.595.8560 (EST) | p: 408.476.8488 (PST)
a: PO Box 3222, Chapel Hill, North Carolina 27515