SOLUTION BRIEF

Comprehesive Visibility Detection and Response with EDR & NDR

Fidelis Cybersecurity® & SentinelOne Joint Solution Brief

The SOC Visibility Challenge

With growing cloud adoption and the rise of remote work, modern IT environments are more complex and harder to secure than ever before. Security teams juggle multiple security solutions, making it challenging to get holistic visibility across the environment. A lack of integration among various best-in-class security products becomes a manual effort for security teams to correlate information for investigation and triage. Combining security data from multiple sources, like EDR and NDR, provides security teams a more complete picture of the enterprise attack surface, improving threat hunting and detection.

Joint Solution Highlights

- Discover, disrupt, respond, and prevent network and endpoint threats
- Improve visibility and detection across networks and endpoints
- Correlate and enrich NDR with EDR metadata

Joint Solution

Endpoint and network solutions are key components of the SOC visibility triad and provide the means to discover, disrupt, respond, and prevent network and endpoint threats. Fidelis Cybersecurity and SentinelOne have partnered to provide unified visibility and integrated investigation workflows for mutual customers.

The joint solution will find every network instance of threats and data leakage and automatically correlate detections with EDR data from SentinelOne. With Fidelis and the SentinelOne platform, instances of malware, or lateral movement, phishing, and other detected threats are immediately elevated in priority and rise to the top of the security team's focus. Furthermore, response to incidents can be automated to block or quarantine at the endpoint or immediately on the network. When Fidelis Cybersecurity is combined with the SentinelOne solution, the security analyst has total visibility into all activity to enable investigations, threat hunting, and retrospective analysis of newly discovered IOCs.

How it Works

- Fidelis Network® will analyze all network and email traffic, collect metadata, and produce threat detections including data leakage (DLP) events. Fidelis Network works at the session level, analyzing reassembled network sessions in addition to each packet, using our patented Fidelis Deep Session Inspection® technology.
- Metadata is produced for all network sessions, which includes netflow, protocol analysis, file decoding, and content analysis. Each detection includes all information of the violating network session, including metadata, recorded sessions, content of all data including file content, sandbox reports, MITRE ATT&CK identification, and one-click access to all files.
- Each threat detection will be correlated to SentinelOne EDR data to determine if the threat is actively engaged and not already blocked, to escalate high priority incidents.
- SentinelOne's endpoint metadata enriches Fidelis Cybersecurity NDR asset discovery, identification, and risk analysis providing an accurate depiction of the enterprise terrain.

Solution Use Cases

Network Detection and Response – Together, Fidelis Network and SentinelOne EDR enable a more comprehensive threat response. In addition, use Fidelis Network metadata to determine the scope and source of any attack on the enterprise to adequately determine the response.

Enterprise Risk Analysis – Fidelis Network builds a picture of the enterprise by identifying all assets by passive network data analysis. Information from EDR and vulnerability scanners build a more complete picture of the state of the environment. Fidelis Cyber Terrain Mapping describes the attack surface of the enterprise including communication paths, vulnerabilities, coverage based on assets where EDR is or is not installed, and exploit activity by threat detection at EDR and NDR.

Deception – Fidelis Deception® is an optional addition to Fidelis NDR. Fidelis Deception builds an automated decoy network based on Terrain or manual creation. Decoys are built to detect the presence of an attacker during the earliest stages of their activity. Breadcrumbs are distributed over endpoints and Active Directory to create lures for attackers and guide them to decoys in the environment. The combination of EDR, NDR, and Deception creates a holistic view of the environment and makes it easier to detect and study adversary tactics and techniques that are in play and stop them earlier in the attack lifecycle.

Conclusion

Fidelis Network Detection and Response platform and SentinelOne Singularity Platform provide a powerful solution to help customers quickly discover, disrupt, respond, and prevent network and endpoint threats.

Integration Benefits

Combine endpoint and network visibility for a complete view of threats

Coordinate response capabilities between network quarantine and endpoint response actions

Correlate network events with endpoint analysis to promote the priority of incidents

Ready for a demo?

Visit the Fidelis Cybersecurity or SentinelOne websites for more details.

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic visibility and asset discovery, multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit **www.fidelissecurity.com**

Fidelis Cybersecurity