SOLUTION BRIEF

Combine XDR with Advanced Security Analytics for a Modern Approach to Securing Your Enterprise

Fidelis Cybersecurity and Devo Joint Solution

The Defenders Challenge

Cyber attackers appear to have the advantage since they only need to succeed one time in order to steal data or disrupt your business. At the same time, new cloud environments are dynamic and ephemeral, which makes securing enterprises and their data more complicated. While digital transformation does indeed enable a more efficient, robust, and cost-effective work environment, it also opens new attack vectors that criminals and foreign states are happy to exploit.

In contrast, the defender needs to protect each of those new and varied attack vectors and environments – cloud, multi-cloud and private. Across all of them, the defender must quickly detect, correlate and respond to numerous threats every day. At the same time, the security market is comprised of disparate products that address single concerns, across endpoints, web traffic, email, IT, OT, and more. As a result, enterprises often deploy more than seventy cybersecurity-related tools on their networks. The widespread use of too many tools makes it harder to not only to effectively detect, but also to defend from active attacks. Organizations lack the personnel to fully comprehend and adequately use the security solutions in place.

Increase Security Efficiency with Integrated Platforms

The first step to improving security efficiency is to adequately place detection technology within the environment. Second, evaluate the security solutions in place and reduce the overlap. Third, combine all detections into a singular interface to allow for efficient operations to detect true incidents and threats. This improves efficiency because you're combining detections to enable a single point of analysis rather than requiring human intervention to connect the dots.

By relying on a smaller number of vendors, users can better understand the technology in place and the team can become experts across the board.

Joint Solution

The Fidelis Elevate® platform from Fidelis Cybersecurity provides full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response. It provides the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. It does this by bringing together deception with detection and response across endpoints, email, network, and cloud. In doing so, users can dynamically modify the threat landscape and use metadata to quickly detect an attack in flight. Used alone, Fidelis Elevate provides a dream environment for threat detection and threat hunting.

The cloud-native Devo Platform is a highly scalable logging and security analytics platform that enables organizations to detect, investigate, and hunt for threats across the entire attack landscape. Devo makes it seamless to collect data from all sources, provides the speed to detect cyberthreats in real time, and enables analysts to ask any question of their data, without limits. With 400 days of always hot data available by default, constructing a threat story that spans months is easier than ever. The Devo Platform can combine Fidelis Elevate detections with other devices in your environment to expand the threat hunt and correlation over the entire enterprise, including data from firewalls, secure web gateways, secure mail gateways, and more.

Solution Use Cases

Enterprise Risk Analysis

Identify all assets, managed or unmanaged, and access paths that an attacker may exploit. Use this combined with risk assessment to determine security gaps and rectify them before an active exploit begins.

Attack Data Correlation

Correlate detections from different security products. Fidelis data ingested to Devo provides an excellent source of correlation because every Fidelis detection is tagged with the appropriate MITRE ATT&CK tactic and technique as well as hundreds of additional fields about your network, endpoint, and decoy analyses. Devo combines this wealth of information with other security products to correlate and highlight detected threats in real time.

Deception

Only an active external exploit or malicious insider will attempt to access a decoy. Fast determination is required to thwart the attack quickly and effectively. The correlation of data from Fidelis and other solutions within Devo provides the necessary answers to take decisive action.

Threat Hunting

Fidelis data and correlation with Devo provides quick answers to common security team questions, including:

- Who else received this phishing email?
- Which devices communicated with a certain website?
- What is the reason for detected anomalies?
- Have the IOC's reported today been in my environment before?

Faster answers to these common questions can lead to faster response and remediation. Devo is a leader in enabling security teams to rapidly hunt for threats across 400 days of always-hot data.

Integration Benefits

- Holistic visibility over network, email, endpoints, and decoys, across data center, cloud, and hybrid environments
- Quickly identify incidents through data correlation rather than bombarding your security team with isolated detections from disparate and uncorrelated security products
- Increase the proficiency of your security team by relying on fewer, but correlated security solutions
- Ingest, correlate and analyze hundreds of terabytes of data per day

Conclusion

Fidelis Elevate analyzes all data on networks, endpoint, and decoys, over cloud, data center, and hybrid environments. By integrating Fidelis Cybersecurity data and detections with Devo cloud-native logging and security analytics, your security team is more efficient and speeds their reaction time to any threat – whether internal or external – including the advanced attack campaigns.

For additional information, visit our website:

Fidelis Cybersecurity
www.fidelissecurity.com

Devo
www.devo.com

About Devo

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.

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**