Solution Brief

Symantec Technology Integration Partner: ziften

Business Challenge

As enterprise network administrators deal with BYOD, shadow IT and the Internet of Things, the need for endpoint detection and response is crucial. Symantec's product portfolio integrates with EDR technologies allowing security professionals to see what is happening at the endpoint and on the network in real time or through historical analytics repositories. This "anywhere, anytime" visibility is vital to identifying critical attack indicators and performing impact analysis as attackers move within an organizations' network.

Solution: Symantec Security Portfolio and Ziften's Adaptive EDR Capabilities

The combination of Symantec's Security Portfolio with Ziften's adaptive EDR capabilities provides comprehensive prevention, detection, and response across the network and all endpoints. The Ziften solution empowers security teams of all sizes to do more with less by providing real-time visibility into all endpoint activities as well as fingertip access to what has occurred in the past. Ziften's advanced detection capabilities are combined with swift mitigation to allow security teams to quickly address threats as they enter their environments. Symantec's Security Portfolio protects the enterprise network, and when combined with Ziften's endpoint protection capabilities security teams can be sure that they have complete coverage across their entire environment.

ziften

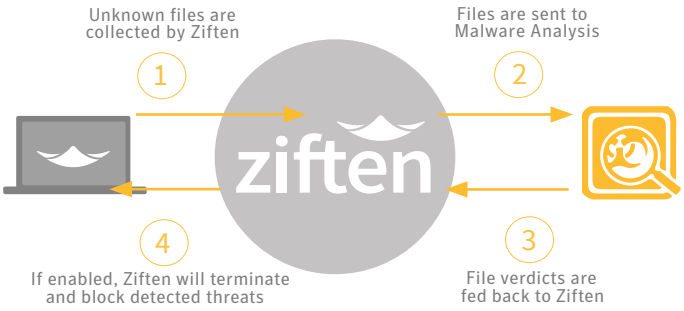
Partner: Ziften

Partner Product: ZDR Technology

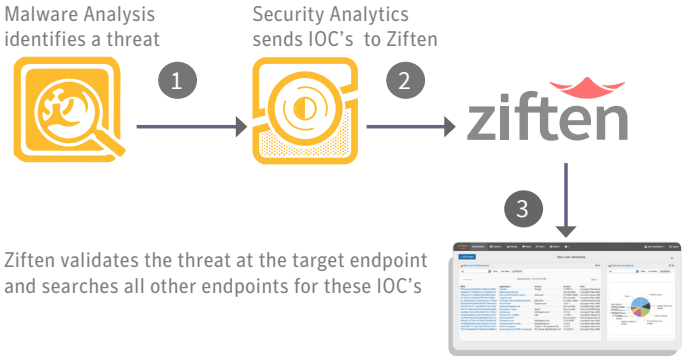
Symantec Product: Malware Analysis and Security Analytics

How it Works

Extend malware analysis to the endpoint: Ziften complements and extends the value of Symantec Malware Analysis by automating the detonation of any file from any endpoint. Ziften sees all files on the endpoint, including those which are downloaded while the device was off-network or files downloaded from removable media (a USB drive, for instance). The file verdicts from Malware Analysis are automatically fed back into Ziften, and all detected threats can be remediated and blocked from executing again.



Symantec



Trace suspect activity from the network to the endpoint: Symantec Security Analytics solution provides rich context behind all network activity. Ziften's integration with Security Analytics offers quick pivot capabilities to understand the context of what had occurred on an endpoint: the last-mile network visibility. By combining the power of the Symantec and Ziften solutions security teams can rest assured that they have complete protection across their entire network and endpoint environments.

The Symantec products gain additional visibility and functionality through the Ziften end point integration. Symantec provides zero-day threat visibility which was once only done through network traffic but now at the end point using the integration. This closes loop holes in file inspection and adds additional threat information to attack vectors that are not even seen on the network. In addition, the visibility and threat information discovered by Symantec products can now be traced from the network down to the end point providing full context across the enterprise. Finally, to prevent this malware from entering the network again, Symantec automatically updates its Global Intelligence Network, and if the file hash is ever seen again, Blue Coat ProxySG with Content Analysis will simply block it at the network.

Benefits

The combined Symantec Security Analytics, Malware Analysis and Ziften solution:

Detect threats on your network and across endpoints by combining the malware analysis capabilities of Symantec Malware Analysis and the Ziften solution, including while the endpoint is off-network

Investigate the scope of a breach by quickly correlating network and endpoint activity, regardless of whether the threat is a recent infection or if it occurred in the past

Terminate and block threats once Ziften or Symantec Malware Analysis determine that a file is malicious, preventing it from executing again in the future

Prioritize network alerts by using Ziften's rich endpoint context that helps illuminate which alerts are the greatest danger to an organization

About Ziften

Global enterprises of all sizes rely on Ziften to enhance their existing security posture, and amplify their limited resources. The Ziften solutions take the complexity, time, and cost out of threat detection with a solution that deploys and can be utilized in minutes, not days. Ziften's continuous monitoring solution helps organizations quickly detect and stop threats, monitor for vulnerabilities and exposures, and identify abnormalities utilizing context-rich historical data. Ziften's ZDR technology extends network telemetry down to the endpoint, providing critical "last mile" network visibility with rich endpoint context. By pairing end-to-end visibility with actionable intelligence, Ziften customers secure their environment and protect their reputation.

To learn more, please visit: http://www.ziften.com

For More Information

Learn more about Symantec Technology Integration Partners on our website.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com