Solution Brief

Symantec Technology Integration Partner: Carbon Black

Business Challenge

Endpoint Security technology has evolved over the last several years moving beyond simple AV protection, encompassing new technologies from application protection and privilege management, whitelisting, execution isolation and comprehensive visibility and controls. While the network, and in particular, the secure proxy, remain the main control point in effective data security, the intelligence and actionable data that can now be gathered from endpoint devices such as Windows PCs and Linux machines is extremely useful for both the security operations and incident response teams.

As enterprise network administrators deal with BYOD, shadow IT and the "Internet of Things," the need for endpoint detection and response are crucial. Symantec's portfolio of products integrate with Endpoint Detection and Response (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 your network.

Solution: Symantec and Carbon Black

As traditional signature-based defenses, such as antivirus and intrusion prevention systems, increasingly fail to stop advanced attacks, organizations must look to next-generation technologies to stay secure. By integrating Symantec's security portfolio with Carbon Black's leading endpoint detection and response solution, security organizations can now leverage their existing network investments to quickly detect, investigate, and prevent advanced threats, on-or-off network, leveraging the industry's only solution to provide real-time visibility and live response.

Partner: Carbon Black

Partner Product: Carbon Black

Symantec Product:
Security Analytics, Malware Analysis

How it Works

The integration of Symantec Security Analytics and Malware Analysis with Carbon Black provide a closed-loop integration between network threat analysis and endpoint threat detection and response. All network traffic and incoming files are captured by Security Analytics, and any unknown files are detonated and analyzed by Malware Analysis. File verdicts and alerts are immediately sent to Carbon Black. The Carbon Black server then correlates these alerts to identify which, if any, endpoints these files hit and if they are executed. Once identified, Carbon Black can then isolate a machine either automatically or on-demand, kill a process or block new infections. In addition to receiving alerts directly from Symantec, Carbon Black can also retrieve any file from any endpoint or server – automatically or on demand – and submit the file to Malware Analysis for sandboxing to analyze and assess its risk level.

Benefits

The combined solution of Symantec Security Analytics and Malware Analysis Appliance coupled with Carbon Black enables security and incident response teams to:

- **Analyze any file on any endpoint or server** with just a few clicks. Often security analysts need to determine the risk level of a particular file. Now they can use Carbon Black to retrieve the file from any endpoint or server and directly submit it to Symantec for analysis.
- **Prioritize** network alerts based on how many machines have been infected and if the malware has executed.
- **Investigate** the scope of threats using the recorded details all network and endpoint activity to trace the root cause and progression of the attack.
- **Remediate** breaches targeting endpoints or the network by knowing precisely which machines are impacted and need attention and automatically ban files from executing based on Symantec-detected malware.
- **Automatically block the execution of files** on endpoints or servers based on analysis results. Leveraging Carbon Black, analysts can automatically ensure that any file deemed malicious by Symantec can never execute again throughout the enterprise.

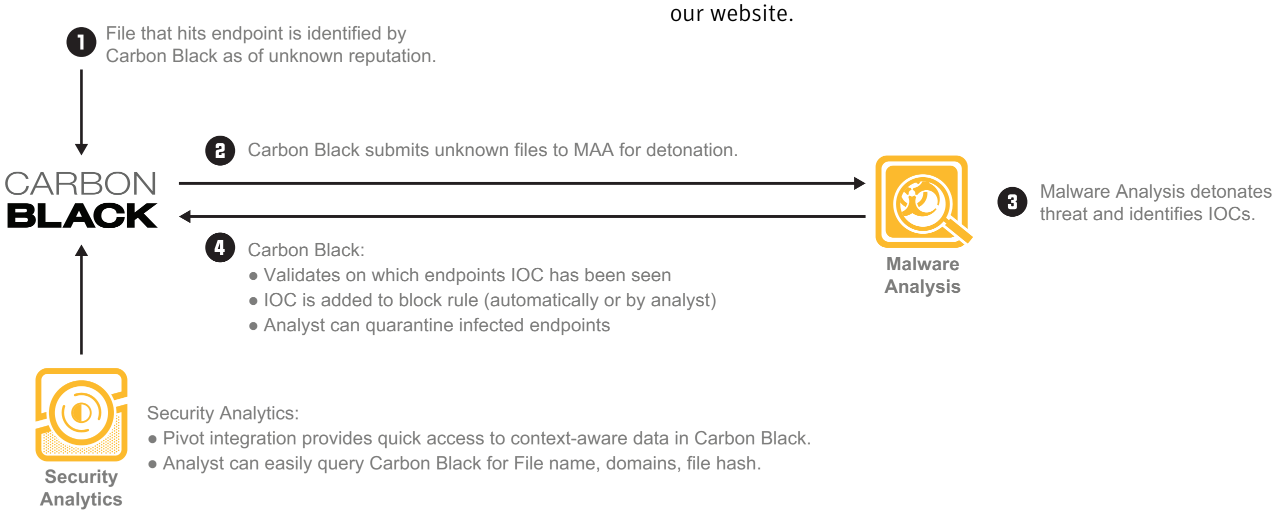
About Carbon Black

Carbon Black is the market leader in Next-Generation Endpoint Security. We have sold more licenses, have more experience, and more customers than any other NGES company because our solution is the most effective way to prevent, detect and respond to advanced threats that target users, servers, and fixed-function devices. That's why more than 60 MSSP and IR leaders, including Dell SecureWorks, EY, Optiv and Solutionary, have chosen our technology as a key component of their security offerings, and 25 of the Fortune 100 rely on us as a critical element of their advanced threat defense and compliance strategies.

To learn more, please visit: www.carbonblack.com

For More Information

Learn more about Symantec Technology Integration Partners on our website.



1 File that hits endpoint is identified by Carbon Black as of unknown reputation.

2 Carbon Black submits unknown files to MAA for detonation.

3 Malware Analysis detonates threat and identifies IOCs.

4 Carbon Black:
● Validates on which endpoints IOC has been seen
● IOC is added to block rule (automatically or by analyst)
● Analyst can quarantine infected endpoints

Security Analytics:
● Pivot integration provides quick access to context-aware data in Carbon Black.
● Analyst can easily query Carbon Black for File name, domains, file hash.

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

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.