SOLUTION BRIEF

Symantec Endpoint Protection + Secure Web Gateway

Network Security + Endpoint Security = Better Together.

For too long, information security has been a piecemeal battle. Security leaders have been forced to stitch together an array of point products that weren't designed to work together. Those days are about to end.

Symantec's acquisition of Blue Coat combines two established security pioneers with deep roots across several technology categories. The unified portfolio creates new opportunities that analysts have said will "change the way organizations buy security"[1] with an integrated approach "to attack some of the more fundamental transformations that are reshaping IT security."[2] That potential is quickly coming to fruition with new versions of Symantec's flagship products for the enterprise – Symantec™ Endpoint Protection™ and Secure Web Gateway.

Working together, Symantec Endpoint Protection and Secure Web Gateway allow companies for the first time to fully leverage and orchestrate security management across networks and endpoints. Endpoint security now learns from network security, and vice versa. Threats can be identified and blocked at either control point. Customers no longer need to build their own integrations and correlations. Network and security leaders can focus on fighting the bad guys rather than fighting their technology.

It's such an obvious solution – and it's now available from the leading global provider of network, endpoint and cloud security. It's just one step in Symantec's vision of an integrated cybersecurity platform that listens, learns and adapts across the enterprise. It's also an important sign of maturity in the security technology market – and comes at the right time for network and security leaders who face more threats on more fronts at a faster pace than ever before.

How Does Integrated Endpoint + Network Security Work?

Let's start with some background on the core products involved:

Symantec Endpoint Protection addresses malware and other threats with a layered approach to endpoint security – including new innovations for advanced machine learning and memory exploit mitigation, along

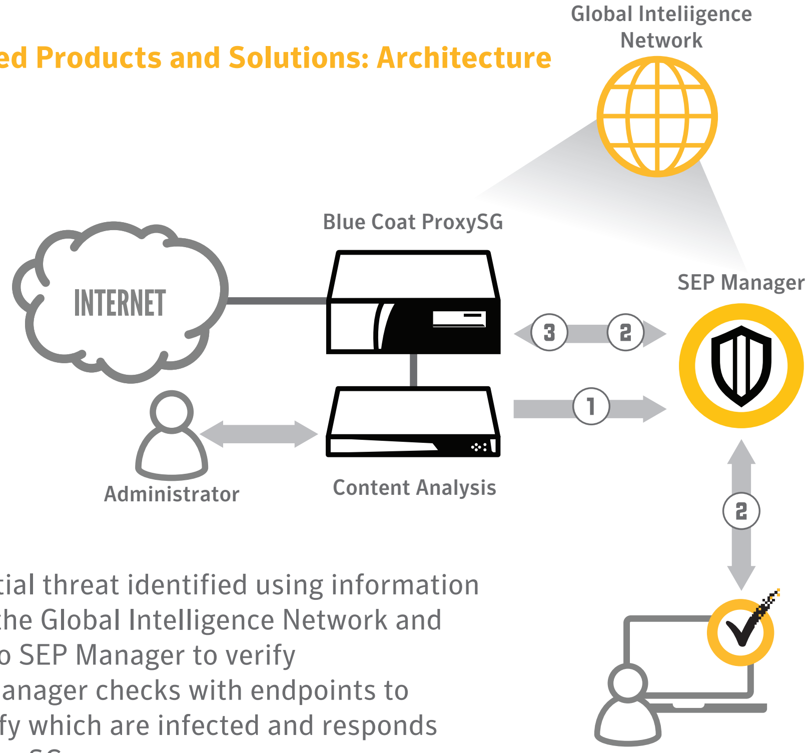
> "The fragmentation that exists amongst threat intelligence solutions continues to have a negative impact on organizations across all industries," said Jon Oltsik, Senior Principal Analyst at the Enterprise Strategy Group. "In today's threat landscape, an integrated solution that combines security intelligence and detection engines, helps organizations stay ahead of advanced threats."
>
> *– Jon Oltsik,*
> *Senior Principal Analyst,*
> *Enterprise Strategy Group*

[1] http://www.bankinfosecurity.asia/symantecblue-coat-deal-game-changer-a-9205

[2] http://www.infosecurity-magazine.com/news/blue-coat-acquired-by-symantec-for/

with established technologies for file reputation and behavior analysis, firewall and intrusion prevention – all powered by the world's largest civilian threat intelligence network. This network consists of telemetry data coming from 175 million endpoints and 57 million attack sensors in 157 countries, providing unique visibility into the latest security threats. Based on this intelligence, advanced machine learning analyzes key file attributes, behaviors and relationships via the cloud and endpoints – blocking threats before they execute while defending against rapidly mutating malware. Memory exploit mitigation stops zero-day threats that exploit vulnerabilities in popular software by monitoring process memory and preventing such attacks. The software works efficiently without compromising performance, while granular policy controls provide easy management across physical and virtual platforms.

Combined Products and Solutions: Architecture



1. Potential threat identified using information from the Global Intelligence Network and sent to SEP Manager to verify
2. SEP Manager checks with endpoints to identify which are infected and responds to ProxySG
3. Remediation: blacklist communicated to:
   - ProxySG / Content Analysis
   - SEP Manager

Meanwhile, on the network itself, the ***Secure Web Gateway*** authenticates, decrypts and inspects Internet content for compliance and advanced threat protection. The gateway's full proxy architecture allows it to effectively monitor, control and secure traffic to ensure a safe Internet experience. Security leaders can enforce policies, detect threats and block advanced attacks from entering their network. Traffic is terminated at the proxy and all downloaded and uploaded objects are processed through multiple layers of security in a single efficient pass.

How do they work together? Symantec's latest version of Symantec Endpoint Protection (v14.0) uses new APIs to collaborate with Secure Web Gateway. This allows the two products to communicate with each other and share blacklists, whitelists, security logs, etc. Data and insights are exposed through the Content Analysis System software (v2.1) built into Blue Coat's Secure Web Gateway products (including Advanced Secure Gateway and Blue Coat ProxySG), which then communicate with the Symantec Endpoint Protection Manager to improve security across the network.

Security managers simply log in to the Content Analysis System console, and everything is available. They can then look at logs across their security infrastructure, define correlation parameters and set remediation roles all from the same console – without needing to switch back and forth. Beyond making it easier to use, the combined system allows leaders to benefit from the most powerful threat data set that you can possibly combine – leveraging insight from thousands of customers, millions of networks and billions of endpoints captured via Symantec's and Blue Coat's combined Global Intelligence Network.

SOLUTION BRIEF

What Are the Use Cases for Endpoint + Network Security?

Here are some common use cases that are easily addressed by the integration between Symantec Endpoint Protection and Secure Web Gateway:

Network to Endpoint Incident Verification: When security managers receive an alert from Blue Coat's sandboxing system, they want to know which endpoints across their network have seen these same indicators of compromise. This will shorten incident response time by eliminating hours or days of unnecessary work to confirm if the malicious sample infected an endpoint. The workflow is simple: the Blue Coat sandbox discovers malicious content, then Blue Coat's Content Analysis System queries Symantec endpoints to verify indicators (file hash, registry changes, URLs, process name, registry changes, etc.). The list of infected endpoints (along with a URL to the Symantec Endpoint Protection Manager) are then added to the sandbox report showing the administrator not only what happened in the sandbox but which endpoints are infected.

Endpoint Blacklisting: Security managers want attacks that are discovered via the network to be isolated without spreading to other endpoints. Again, the workflow is simple: Blue Coat's sandbox discovers malicious content with high certainty. Blue Coat's Content Analysis System queries Symantec Endpoint Protection – and adds a file to the blacklist for all endpoints via the Symantec Endpoint Protection Manager. This prevents the spread of this file to other endpoint devices.

Information regarding threats are also sent to the Global Intelligence Network to share with the Secure Web Gateway and Symantec Endpoint Protection community worldwide.

Beyond these use cases, Symantec will continue extending integration between endpoint and network security to address other customer needs. We also anticipate our customers will identify new use cases as they explore the possibilities.

Bottom Line: Better Protection from Endpoint to Cloud

Security leaders can now leverage and optimize protection across networks and endpoints, providing a full spectrum of threat protection with fewer integration headaches. Shared intelligence results in early and effective threat detection, fueled by a massive global intelligence network. Granular controls allow you to take proactive action to blacklist attacks and apply security policies that prevent the spread of attacks. And automated remediation allows you to remediate issues with one click via integrated management consoles.

Find out more about Symantec Endpoint Protection at http://go.symantec.com/SEP

Find out more about Secure Web Gateway at http://go.symantec.com/ProxySG