WHITE PAPER:
SYMANTEC™ ADVANCED THREAT PROTECTION

Symantec Advanced Threat Protection

Accelerating Incident Response with Symantec Synapse™

Who should read this paper

Read to discover how Symantec Synapse brings enhanced incident response and workflow, to reduce false positives and prioritize security events by integrating and correlating across endpoint, network, and email.

Symantec

Content

Overview

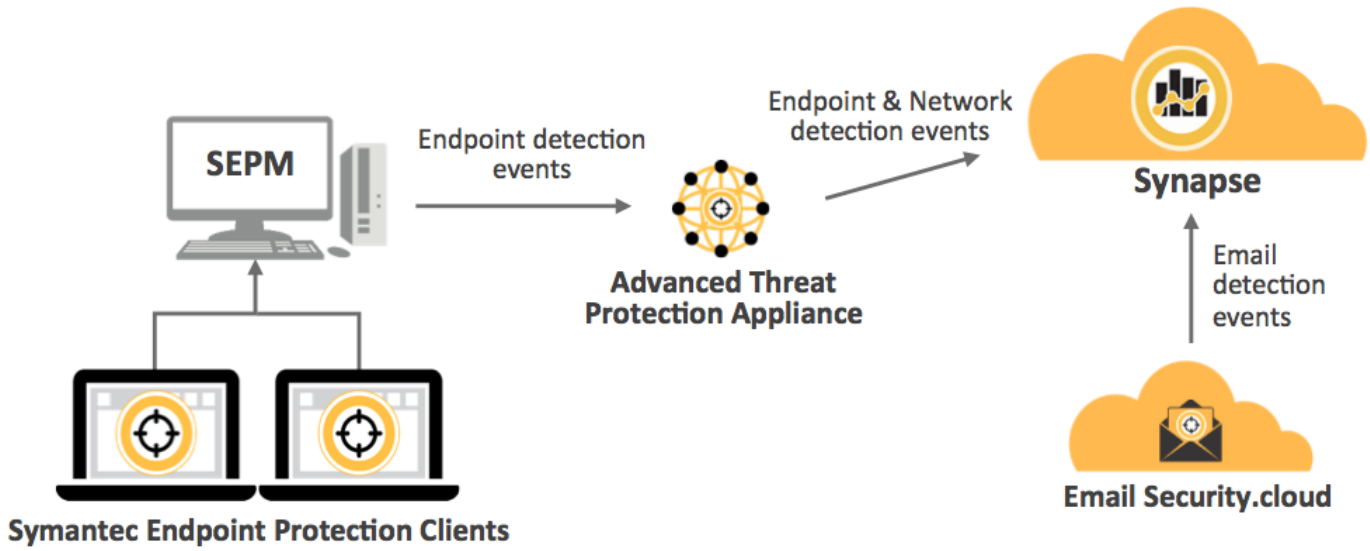
Symantec Synapse is a new technology included with Symantec Advanced Threat Protection that brings together and correlates security event data across Symantec™ Endpoint Protection, Symantec™ Email Security.cloud, and the Symantec Advanced Threat Protection: Network appliance to help organizations identify which incidents they should respond to first and which incidents have been blocked by existing security controls. This significantly reduces the number of incidents that security analysts need to investigate and allows analysts to "zero in" on just those events of greatest importance. With Symantec Synapse, Symantec Advanced Threat Protection can be installed, configured and start to ingest, search for, and correlate data across all control points in under an hour.

Security events generated by threat protection and threat detection applications have a number of attributes which are examined by Synapse for potential correlations. These events are correlated when either a given network or email event is closed out with an endpoint block of the payload and/or where other events are shown that have one or more of the same below attributes:

- **URL/EXTERNAL IP ADDRESS** - lists incidents where the same external URL was involved in the event.
- **INTERNAL IP ADDRESS** - displays the incidents that were detected on the same internal machine.
- **FILE HASH (SHA256)** - displays incidents where the same file was downloaded.
- **VANTAGE SIGNATURE** - lists the incidents that were convicted by Symantec Vantage intrusion prevention technology because the same behavioral characteristics were detected.
- **AV SIGNATURE** – lists the incidents that were convicted by the same Symantec Antivirus signature(s).

The continual process of checking for related attributes and correlating events can be resource-intensive, so we rely on the power of our Synapse cloud platform to perform a significant portion of the computational effort to maintain relationships between all of the security events for each organization. This helps reduces the on-premises hardware requirements and ensures that Symantec Advanced Threat Protection quickly uncovers attacks that would otherwise evade detection.

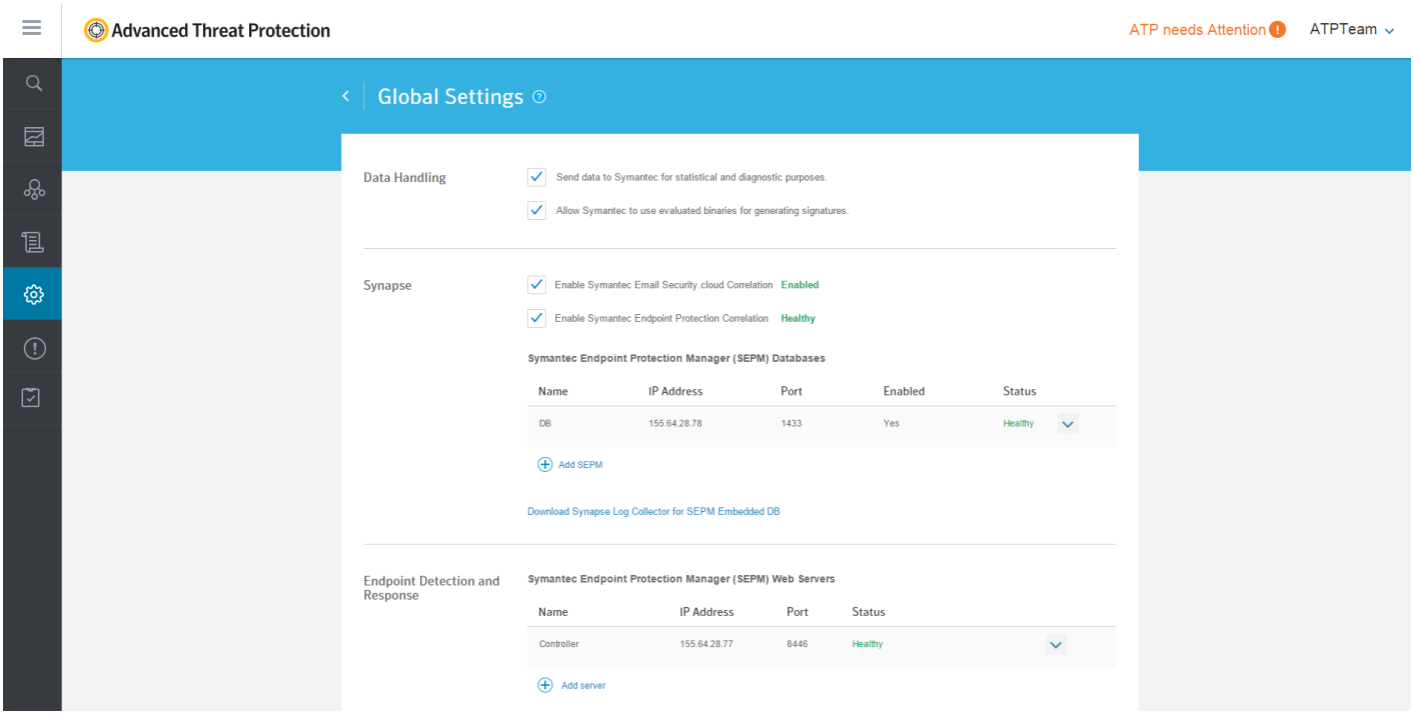
Using Symantec Synapse, the Symantec Advanced Threat Protection console provides all the data that a customer needs to know about attacks in one place, without requiring any manual searching.



Configuring Symantec Synapse

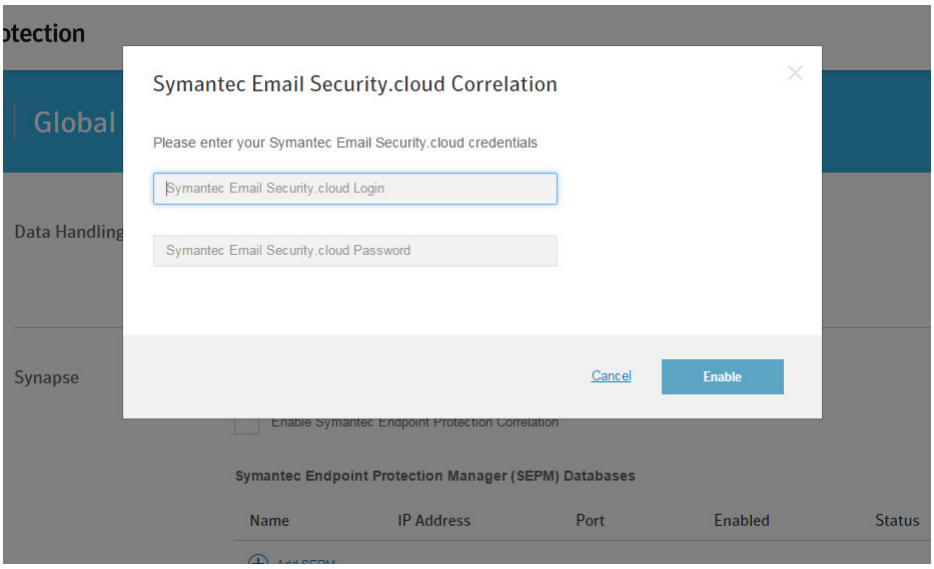
Synapse setup has been designed to be a simple process. To enable endpoint event correlation with network and email detections, you will need to provide three pieces of information:

- Account credentials that allow access to the Symantec Endpoint Protection Manager (SEPM) server.
- Specify which database type the SEPM uses - either an embedded DB or Microsoft SQL Server.
- The IP address assigned to the SEPM server.



After completing the setup process, Synapse will begin pulling in endpoint convictions at the heartbeat set within SEPM. These endpoint events are pulled in, along with all other Advanced Threat Protection: Network events, to the Synapse cloud platform. Event data is stored and maintained by the Synapse cloud platform for 90 days. Symantec Endpoint Protection events will start to appear in the Advanced Threat Protection console based on the Symantec Endpoint Protection client heartbeat set by the SEPM admin. This is the frequency at which the Symantec Endpoint Protection client checks in with the SEPM server. The default heartbeat is five minutes, but this can be customized – check with your Symantec Endpoint Protection administrator to determine the rate of updates from clients to SEPM. This near real-time ingest and correlation of events helps drive a fast and powerful search across your enterprise environment.

Setup of email correlation is even simpler, as users just need to provide their organization's Symantec Email Security.cloud administrative credentials to start the event synchronization process. This initial process can take up to 24 hours; however, once setup completes, Synapse will check for changes every five minutes.



Use Case 1: Synapse Provides Visibility with Simple but Powerful Search

With Synapse technology in Symantec Advanced Threat Protection, customers are able to create a broad and deep security view of all network, endpoint, and email conviction events that have occurred in their environment. In addition, Synapse makes searching within all these security events simple and easy, and provides fast answers to powerful questions.

Example

A user at Company A is online at a location protected by Symantec Advanced Threat Protection: Network. Company A also subscribes to Symantec Email Security.cloud and has Symantec Endpoint Protection on some, but not all, of its endpoints.

Three user accounts are sent an email with a malicious URL. The email is convicted and blocked by Email Security.cloud and is not delivered to the end users. Later that same day, a user receives an email with same malicious URL to their personal mailbox at work. The email is not blocked, and the user visits the URL. Once at the site, the user receives a payload from the compromised server. Symantec Advanced Threat Protection: Network detects the payload as suspicious and sends it off to Symantec Cynic™ for analysis.

In the meantime, the file has already been passed to the endpoint. The endpoint is not managed by Symantec Endpoint Protection, so no automatic conviction or blocking occurs. Cynic returns a malicious conviction on this payload and a detection event is created in Advanced Threat Protection as a network event. A security analyst at Company A reviews the detection event that afternoon, five hours after the chain of activity initially began. Seeing the Cynic conviction, she is able to quickly initiate a Synapse search across the entire environment with one click to determine which endpoints have this payload, searching by hash and file name.

The search returns three email convictions with the URL that the file was downloaded from and one network event containing the IP address of the unmanaged endpoint that has the file. Armed with this intelligence, the security analyst is able to quickly begin remediation on the specific device that downloaded the malicious payload and is confident that no other instances of this attack have been detected.

By bringing together all these security events into a single solution, Synapse greatly simplifies search and helps responders quickly ascertain the scope of endpoints impacted by a detection event. In addition, Synapse also supports a full environment search based on any of the following basic Indicators of Compromise (IOCs): file name, file hash, URL (full or partial), and registry key.

Use Case 2: Synapse Powers Hunting in Your Environment

Synapse powers endpoint interrogation for IOCs, even on files that Symantec did not previously convict or know as malicious.

Example:

You are alerted by a federal agency that another company in your industry has been successfully attacked with a specific payload. One of the IOCs of the attack is a file hash; you want to know if that hash is in your environment. To do this, the analyst enters the file hash into the search field with the “query endpoints” slider set to green.

Synapse queries the endpoints and finds that of the 10,000 endpoints in your environment, the hash is found on three endpoints. Additionally, only one of the three endpoints has a correlating block event. At this point, no further action needs to occur on that one endpoint where the event was blocked. The other two endpoints, however, do not have a block event, so the analyst decides to immediately isolate those endpoints to contain them from the rest of the environment.

In order to follow up and close out this query, the analyst then blacklists that file hash so that subsequent detections at all local endpoints are blocked. Lastly, he deletes the file on the two isolated endpoints to clean the system before allowing them to rejoin the environment.

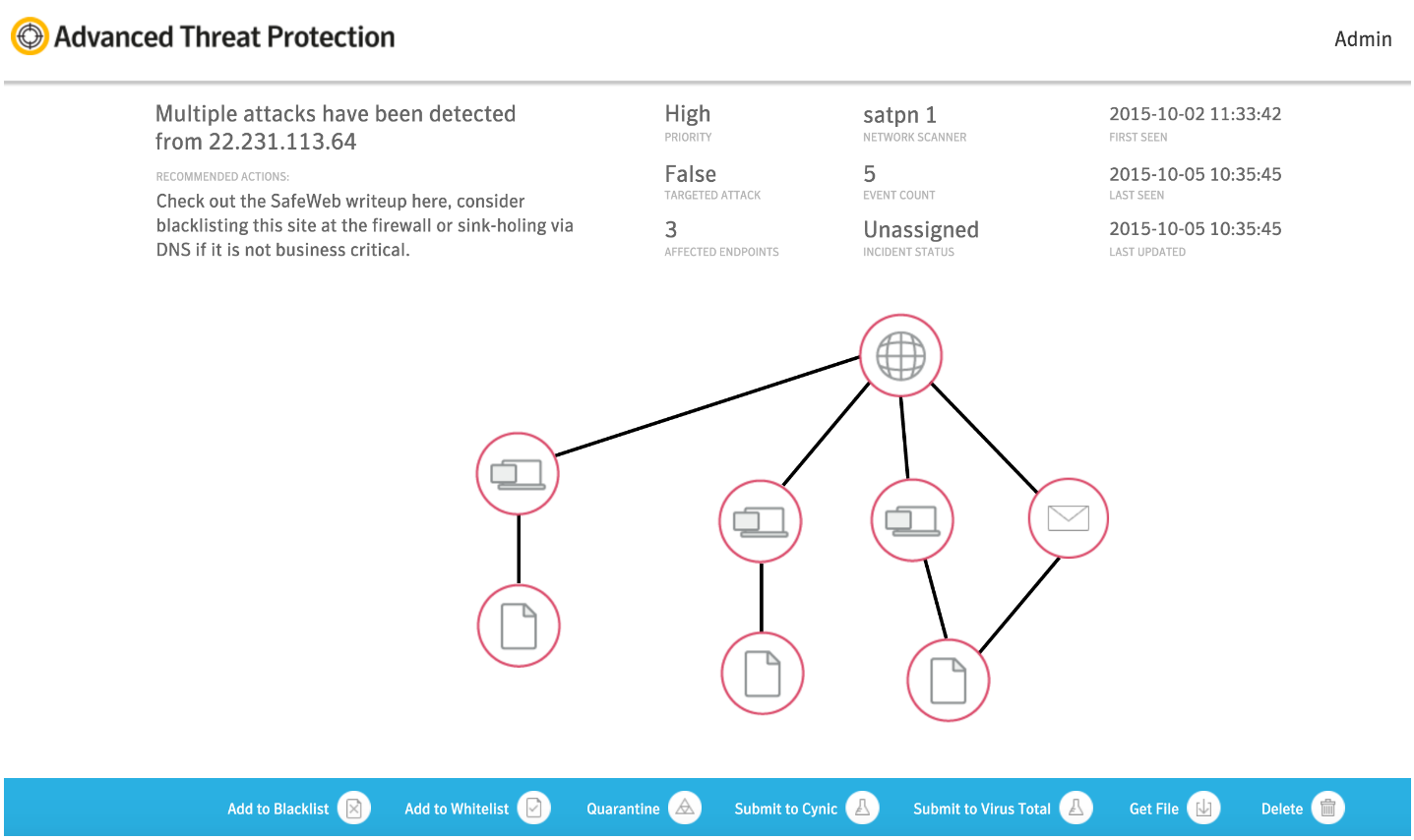
Use Case 3: Synapse Helps Security Analysts Investigate and Remediate Efficiently

Synapse correlates related events from all three Advanced Threat Protection sensors (endpoint, network, and email) into a security incident that requires further security analyst attention and investigation. All incidents that are created in the system are the result of the streaming rules engine, a collection of logical statements that helps Advanced Threat Protection understand if there is enough activity to trigger the creation of an incident.

Example

An incident can be created when we have proof of an infected endpoint. The proof required can be either a detection of infected network traffic out to a Command-and-Control server or a payload we know to be malicious from which the endpoint cannot completely clean up all artifacts. These are known infections, and they create incidents that the security analyst will have to address.

Additional incident creation happens when we have confirmed event activity leading to a domain, IP, or URL that was originally neutral, around a specific, relatively short time frame. This could involve the same or multiple network locations, or multiple file downloads to one or more endpoints, or one or more endpoints all being targeted by a given domain/IP/URL/external machine. The intelligence in deciding which events are related is driven by Synapse, which sees the relationships between seemingly disparate events and brings them together visually into an "organism" for easy and simple exploration, investigation, and pivoting through the data.



From one place, the organism view, an analyst can immediately understand the scope of an attack and have access to a number of actions.

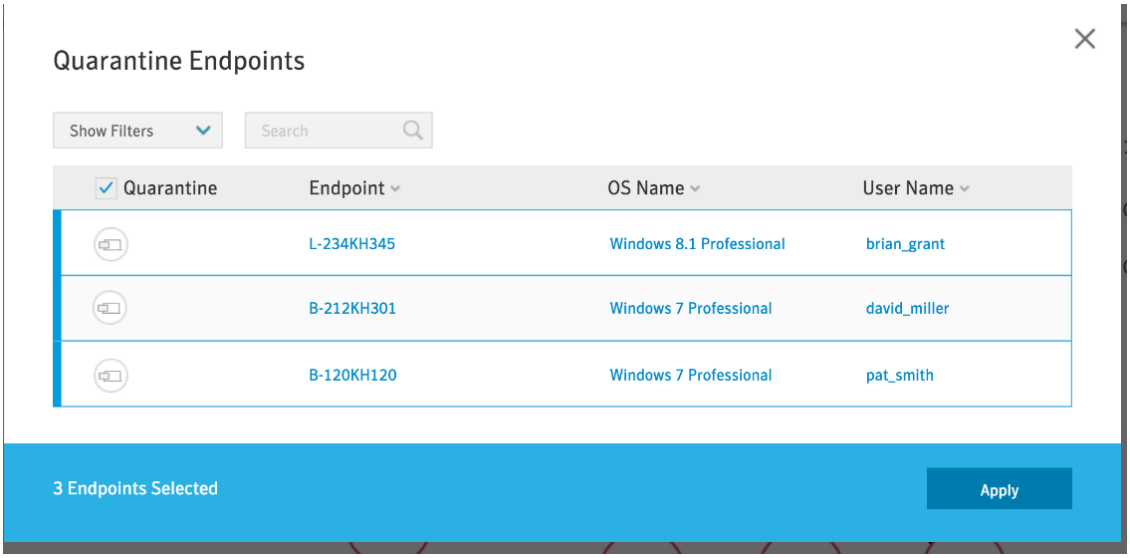
Blacklisting and Whitelisting

From the organism view, the security administrator can quickly and easily blacklist specific file or network traffic attributes across the entire environment immediately. Symantec Advanced Threat Protection can blacklist access to files or locations based on SHA256 and MD5 file hash, URL or domain, and IP addresses or IP subnets. Attempts to access blacklisted files or locations will be denied and will always generate a detection event in the Advanced Threat Protection console

Similarly, security administrators can whitelist access to files or network locations, forcing Advanced Threat Protection to bypass the detection engines and allow unfettered access.

Quarantining Endpoint Devices

Clicking on the quarantine button in the organism view will quickly isolate the devices that are within the scope of this incident.

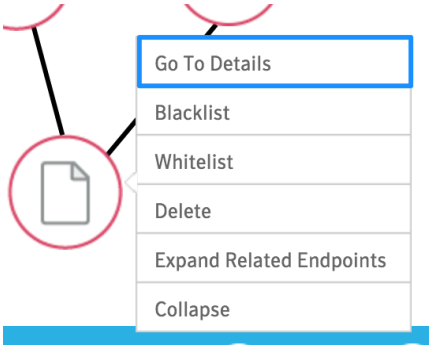


Quarantining devices uses the network control components of the Symantec Endpoint Protection client to block all network access attempts. The only location a quarantined device will be able to communicate with is the SEPM server with which it is associated. This prevents the spread of infection and blocks unauthorized attempts to network services and data, but the security administrator remains able to investigate and remediate the device. Once the investigation is complete, the same interface can be used to remove the quarantine and restore full network access to the device.

Further Investigation

The suspicious or convicted file can be sent to the Symantec Cynic sandbox for further inspection, which will provide the exact behavior of the payload. Additionally, it's easy to see what Virus Total and other security vendors know about this file with a single click.

The context menu for a suspicious or convicted file allows the administrator to view all of the intelligence that Symantec Advanced Threat Protection knows about it.



Local context is provided in the form of the number of times this file has been seen in the environment, when it was first seen, where it has been detected, and where it originated from.

The output of the Symantec Cynic sandbox analysis details the behavior and actions that the file takes when it is active on a device, along with any locations and destinations with which the file processes attempt to communicate. These Indicators of Compromise can be used to search for evidence of other infections in the environment that may be part of a wider targeted attack campaign.

Cynic Observed File, Registry, System Changes

Severity	Type	Description	PID
1	Process Started	C:\Windows\SysWOW64\cscript.exe	2940
1	Process created by	C	2940
1	Opened a registry key	HKEY_CURRENT_USERS\Software\Microsoft\Windows Script Host\Settings	2940
1	Created window	0	2940
1	Opened a registry key	HKEY_CLASSES_ROOT\.js	2940

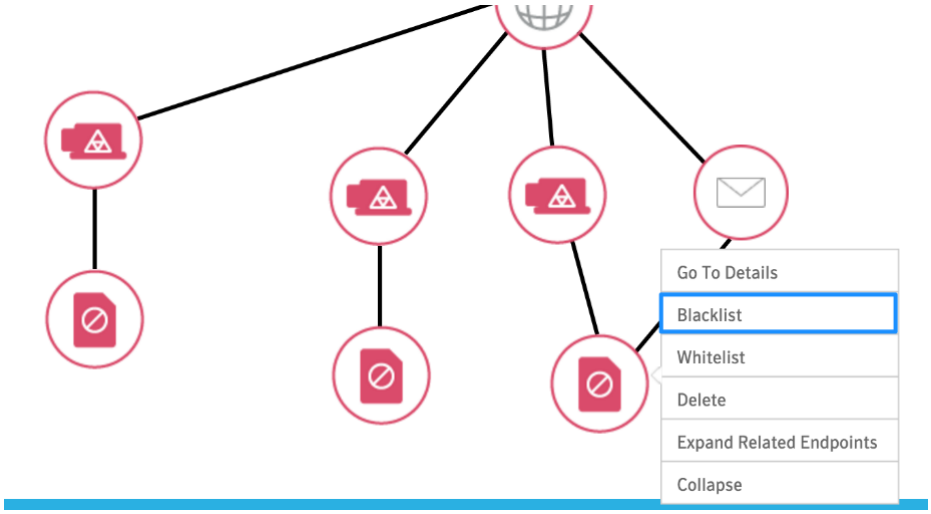
15 Total

Cynic Observed Network Analysis

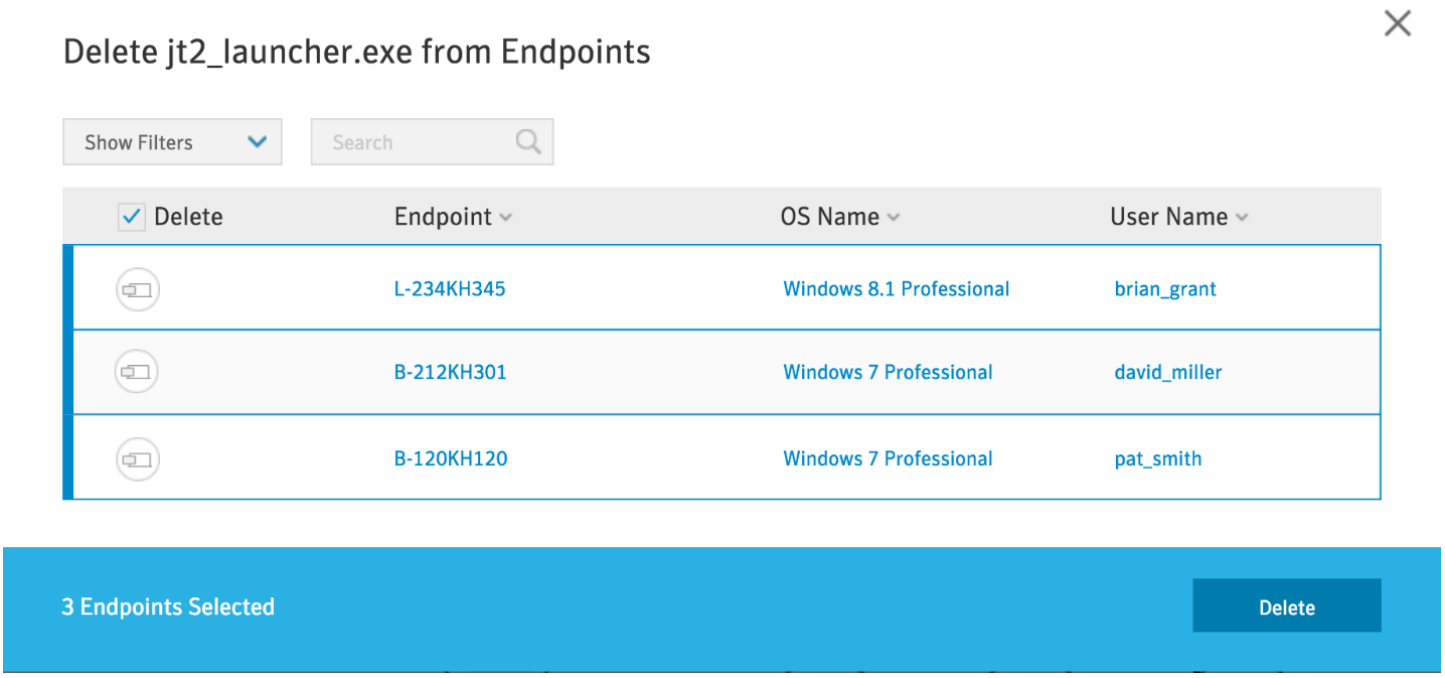
Domain/IP	Protocol	Port	URL
router.bittorrent.com	DNS	--	--

Single Click Remediation

Once the investigation has been completed, Symantec Synapse makes it extremely simple to remediate. It already knows exactly which machines contain the file and can take advantage of the Symantec Endpoint Protection client to remove the file and prevent further infection. Using the context menu again, the security analyst is able to automatically add the file information to the blacklist.



Once the file has been blacklisted, choosing “Delete” will remove the file and any associated artifacts from all endpoints in the incident’s scope.



Summary

It is possible for organizations to build their own platform for data sharing and intelligence correlation, using a Security Information and Event Management (SIEM) platform and writing log parsers and collectors to pull data into a single place, and for some security organizations this can be a sensible approach. However, the work required to write and tune policies to accurately detect the difference between an attack and a false positive, along with the operational requirements to manage, maintain, and update such an environment puts this out of the question for the vast majority – especially when factoring in the cost and time to remediate when an attack is discovered.

With Symantec Advanced Threat Protection, Synapse aggregates intelligence across all control points, significantly reducing the number of incidents that security analysts need to investigate, and automatically prioritizes those systems that remain compromised and require immediate remediation. It provides all the data that a customer needs to know about an attack in one place without requiring any manual searching, and it fuses global telemetry from one of the world's largest cyber intelligence networks with local customer context across endpoints, networks, and email to uncover attacks that would otherwise evade detection.

By leveraging existing installations of Symantec Endpoint Protection and Symantec Email Security.cloud, Symantec Advanced Threat Protection brings security analysts the visibility they need to work fast and make informed decisions, including one-click remediation and the ability to hunt for Indicators of Compromise across all your endpoints from a single console, all without having to install any new endpoint agents.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com