SOLUTION BRIEF

HAUMOUN IT PIONEERS

Threat-Aware Data Protection Keeps Your Data Safe from Malicious and Dirty Apps

Stop malware and user-installed apps from exfiltrating sensitive data with unparalleled threat awareness and data loss prevention

Symantec

At a glance

- **Untrusted apps:** When users bypass IT to install unauthorized apps, they could open the door to cyber criminals out to collect your data. Are you protected against data theft by fake and malicious apps?
- **Targeted attacks:** Bad actors use malware to infiltrate corporate networks and steal information from targeted endpoints without being detected. Are you protected against stealth data exfiltration?

You can't trust your users' apps any more than you can trust cyber criminals

Data is always at risk whether it's being endangered by unsuspecting employees or targeted by malicious actors.

A dizzying array of fake apps masquerading as legitimate apps are trying to sneak into your corporate network to exfiltrate sensitive data. Unfortunately, users unwittingly usher in these threats when they install unauthorized apps. (Your users want greater efficiency, so hackers focus on creating productivity tools—such as PDF splitters and mergers, calculators, video capture and editing tools—as a prime vehicle for their fake apps.)

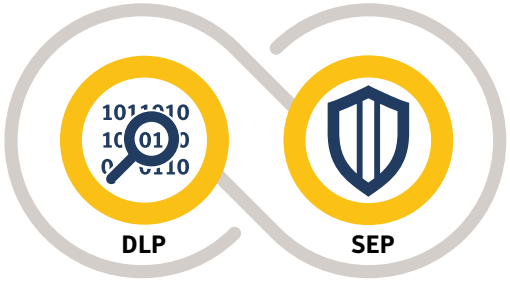
Similarly, cyber criminals rely on sophisticated malware to exploit security gaps more efficiently.

You have two main weapons in your defense arsenal.

Good endpoint security detects and blocks suspicious and malicious apps. But endpoint security alone is not enough to combat surreptitious data theft. For example, malware, such as an infostealer trojan, lies dormant on an endpoint until an attacker uses a command-and-control connection to exfiltrate data.

Good data loss prevention tools stop unauthorized data exfiltration by insiders. But they lack visibility into external threats. By harnessing the power of Symantec reputation security and threat intelligence, our data loss prevention tools become threat-aware to safeguard data from both insider and outsider threats.

Threat Aware Data Protection



Keep your data safe from malicious and dirty apps

Symantec threat-aware data protection combines our unmatched data loss prevention with our endpoint protection, defending against stealth data theft by malicious and dirty (suspicious or unknown) apps. Powered by the Symantec Global Intelligence Network—the world's largest civilian threat database—our endpoint security stops apps from seizing control of devices and stealing sensitive information, without interrupting your business.

Symantec Data Loss Prevention

Detecting illegitimate data exfiltration first requires understanding where your sensitive data is stored, how it is being used, and who is accessing it.

Symantec Data Loss Prevention does just that, identifying, locating, and monitoring sensitive data (such as intellectual property and regulated data) on endpoints. Data Loss Prevention uses machine learning, fingerprinting, and other advanced detection capabilities to classify data with the greatest accuracy.

Symantec Endpoint Protection

Marrying data visibility with a broad and deep understanding of evolving threats lets you unmask hidden threats.

That's where Symantec Endpoint Protection (SEP) comes in. SEP detects malicious and untrusted apps without compromising user productivity. SEP goes beyond signature blocking to fuse signatureless technologies (such as advanced machine learning and behavior analysis) with time-tested ones including file reputation analysis.

How Threat-Aware Data Protection works

Symantec threat-aware data protection detects and checks user-installed apps, surveils app behavior, and prevents apps from exfiltrating sensitive data.

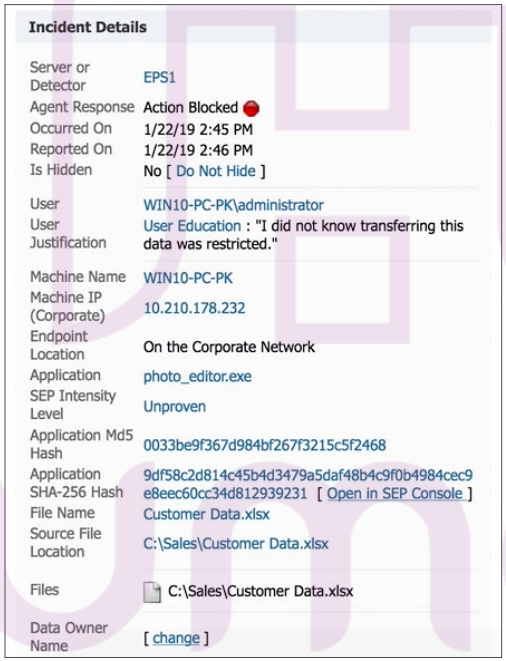
Here's how it works:

1. **Detect and check—**Data Loss Prevention detects when a user launches a new application and immediately queries SEP for the app's risk level. (Windows apps on the Microsoft Store and system processes are prefiltered and treated as trusted.) SEP returns a numeric score based on attributes derived from reputation and advanced machine learning.
2. **Monitor—**Data Loss Prevention maps the SEP score to specific intensity levels. It then monitors apps rated malicious, suspicious, or unknown for attempts to access sensitive data.
3. **Prevent—**When one of these applications (or processes) access sensitive data, Data Loss Prevention notifies the user via a pop-up message—which may include a justification for a policy violation—and automatically applies the appropriate policy response.

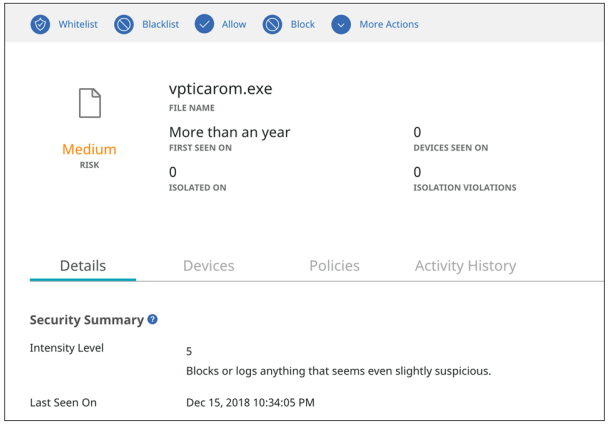
3 Ways DLP Can Respond to Data Exfiltration

- **Blocking** a data exfiltration attempt by a malicious app
- **Encrypting** a file accessed by an unknown app
- **Notifying** the user—who can decide to allow or deny access by a suspicious app

When Data Loss Prevention detects a malicious, suspicious, or unknown app trying to exfiltrate data, the Data Loss Prevention Enforce console generates an incident snapshot with full contextual information—including the application name, intensity level, sensitive data that was targeted, its location, and more—so you can quickly analyze policy violations and threats.

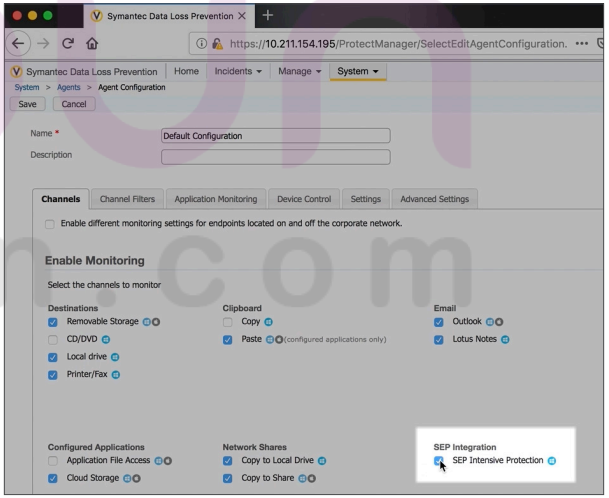


Additionally, Data Loss Prevention gives you access to the SEP cloud console where you get full details about the suspicious app such as its reputation, prevalence, digital signature, and more.



Getting started

Current SEP and Data Loss Prevention customers easily turn on Symantec threat-aware data protection just by checking the SEP Intensive Protection control in the Data Loss Prevention Enforce console. This connects your Data Loss Prevention and SEP agents.



Your Zero Trust data security toolkit should include:


Data Loss Prevention


Cloud Access Security Broker


Digital Rights Management


Data Classification


User and Entity Behavior Analytics


Identity and Access Management


Web Gateways

From there, configure your data loss prevention policies to take advantage of Intensive Protection response rules based on the app's risk intensity level (as determined by SEP).

Protect your data with Zero Trust

Symantec threat-aware data protection is a foundational building block in a Zero Trust architecture.

The Zero Trust model, coined by Forrester Research, considers that threats are everywhere—both outside and inside your organization. Data should be brought 'into the clear' only after you have evaluated all user and device risk factors.

Zero Trust relies on gaining visibility into who is accessing your data, both on premises and in the cloud. No wonder companies wishing to reliably prevent data exfiltration, and better defend against modern cyber threats, embrace Zero Trust.

Next steps

To learn more about Symantec threat-aware data protection, visit the Symantec Data Loss Prevention microsite.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, 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 and LifeLock product suites to protect their digital lives at home and across 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, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

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

19D214527_SB_THREAT_AWARE_DLP_SEP_EN