SOLUTION BRIEF

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

## 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?

# Threat-Aware Data Protection

## Keep Your Data Safe from Malicious and Dirty Apps

### Overview

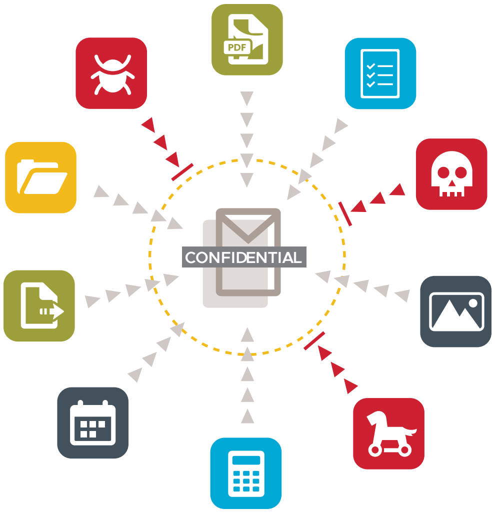
You can't trust your users' apps any more than you can trust cyber criminals. Data is always at risk, whether it's being endangered by unsuspecting employees or targeted by malicious actors.

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.



## 3 WAYS DLP CAN RESPOND TO DATA EXFILTRATION

- Block a data exfiltration attempt by a malicious app
- Encrypt a file accessed by an unknown app
- Notify the user, who can decide to allow or deny access by a suspicious app

## Keep Data Safe from Malicious and Dirty Apps

The Symantec threat-aware data protection solution combines unmatched data loss prevention with endpoint protection, defending against stealth data theft by malicious and dirty (suspicious or unknown) apps.

Powered by the Symantec Global Intelligence Network (GIN)—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 (DLP) does just that, identifying, locating, and monitoring sensitive data (such as intellectual property and regulated data) on endpoints. DLP 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:

1. **Detect and check:** DLP 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:** DLP 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 accesses sensitive data, DLP notifies the user via a pop-up message, which may include a justification for a policy violation, and automatically applies the appropriate policy response.

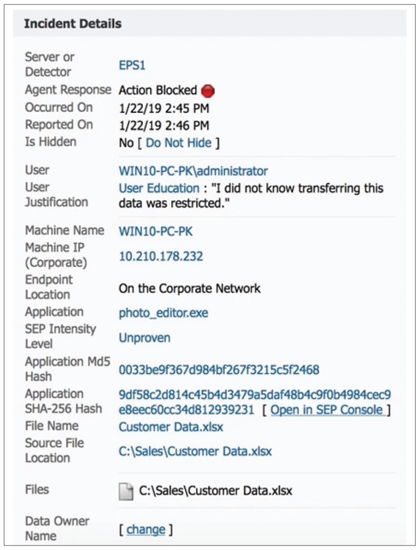
When DLP detects a malicious, suspicious, or unknown app trying to exfiltrate data, the DLP Enforce console generates an incident snapshot with full contextual information, including the application name, intensity level, sensitive data that was targeted, its location, and more, so you can quickly analyze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

## THE TOOLKIT

Your Zero Trust data security toolkit should include the following:

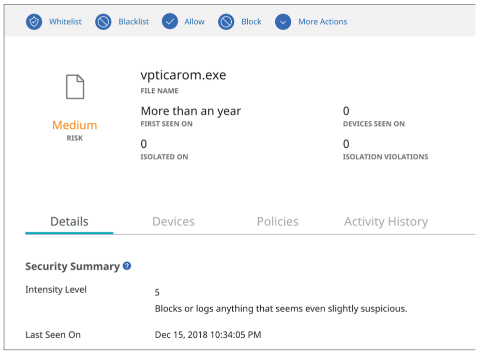
- Data Loss Prevention
- Cloud Access Security Broker
- Digital rights management
- Data classification
- User and entity behavior analytics
- Identity and access management
- Web gateways

Additionally, DLP 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.



**Incident Details**

| | |
|---|---|
| Server or Detector | EPS1 |
| Agent Response | Action Blocked ● |
| Occurred On | 1/22/19 2:45 PM |
| Reported On | 1/22/19 2:46 PM |
| Is Hidden | No [ Do Not Hide ] |
| User | WIN10-PC-PK\administrator |
| User Justification | User Education : "I did not know transferring this data was restricted." |
| Machine Name | WIN10-PC-PK |
| Machine IP (Corporate) | 10.210.178.232 |
| Endpoint Location | On the Corporate Network |
| Application | photo_editor.exe |
| SEP Intensity Level | Unproven |
| Application Md5 Hash | 0033be9f367d984bf267f3215c5f2468 |
| Application SHA-256 Hash | 9df58c2d814c45b4d3479a5daf48b4c9f0b4984cec9e8eec60cc34d812939231 [ Open in SEP Console ] |
| File Name | Customer Data.xlsx |
| Source File Location | C:\Sales\Customer Data.xlsx |
| Files | C:\Sales\Customer Data.xlsx |
| Data Owner Name | [ change ] |



vpticarom.exe
FILE NAME

Medium
RISK

More than an year
FIRST SEEN ON

0
DEVICES SEEN ON

0
ISOLATED ON

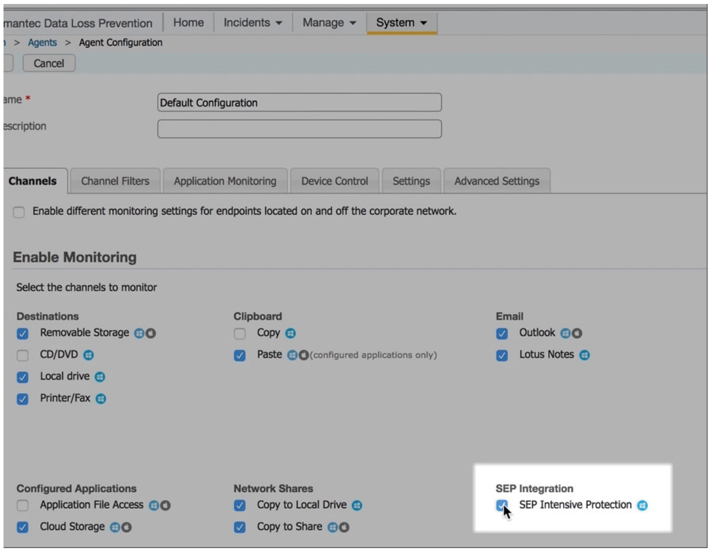
0
ISOLATION VIOLATIONS

**Security Summary**

| | |
|---|---|
| Intensity Level | 5<br>Blocks or logs anything that seems even slightly suspicious. |
| Last Seen On | Dec 15, 2018 10:34:05 PM |

## Getting Started

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



ame * Default Configuration
escription

□ Enable different monitoring settings for endpoints located on and off the corporate network.

**Enable Monitoring**

Select the channels to monitor

**Destinations**
☑ Removable Storage
□ CD/DVD
☑ Local drive
☑ Printer/Fax

**Clipboard**
□ Copy
☑ Paste (configured applications only)

**Email**
☑ Outlook
☑ Lotus Notes

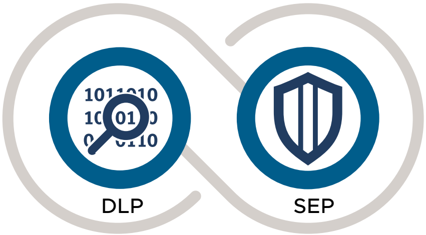
**Configured Applications**
□ Application File Access
☑ Cloud Storage

**Network Shares**
☑ Copy to Local Drive
☑ Copy to Share

**SEP Integration**
☑ SEP Intensive Protection

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.

## THREAT-AWARE DATA PROTECTION



## 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 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.

To learn more about Symantec threat-aware data protection, visit broadcom.com/dlp.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-TADP-Apps-SB100 March 18, 2025