Dom Moore
DLP / Classification

Scenario

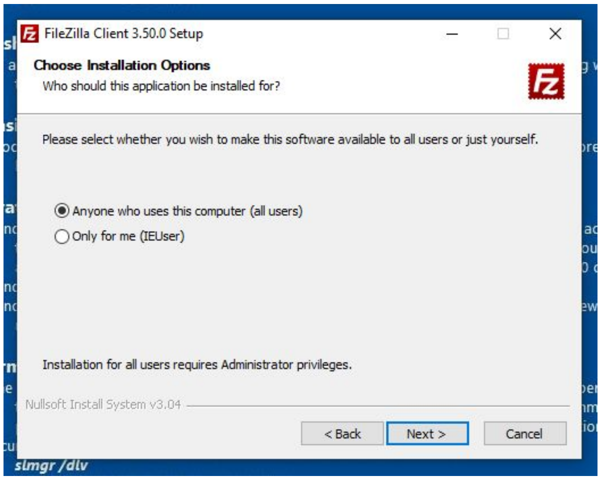
Today you are performing a security consultation for a familiar client, Globex Nuclear Corp. After evaluating a recent security audit performed by Globex's banking partner, it was determined that PCI-DSS compliance was not achieved by existing IT systems and policies. Due to your sales teams' regular handling of customer credit card information as part of the sales order creation process, you will need to classify data and implement a DLP solution to control the movement of data on sales team computers. The auditing team is requiring controls that restrict the transmission of both PCI and PII data. Furthermore, a clear data classification policy will need to be composed and reviewed by the executive team for immediate implementation.

Part 1: Staging

For this lab you'll need a trial license for Trend Micro's endpoint security agent software.

- Register for an account at Trend Micro Worry-Free Business Security Services 30-Day Trial.
- From the PC or VM you're installing agent to, access the portal and download the agent.

FileZilla Install



FileZilla Client 3.50.0 Setup

Choose Installation Options

Who should this application be installed for?

Please select whether you wish to make this software available to all users or just yourself.

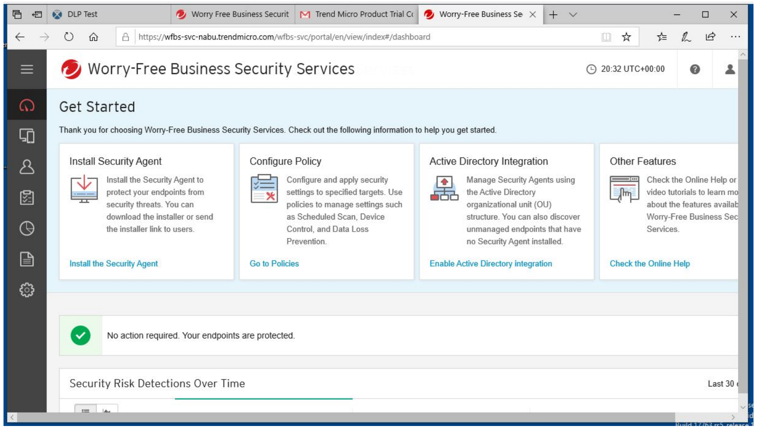
● Anyone who uses this computer (all users)

○ Only for me (IEUser)

Installation for all users requires Administrator privileges.

Nullsoft Install System v3.04

Trend Micro Install



https://wfbs-svc-nabu.trendmicro.com/wfbs-svc/portal/en/view/index#/dashboard

Worry-Free Business Security Services

20:32 UTC+00:00

Get Started

Thank you for choosing Worry-Free Business Security Services. Check out the following information to help you get started.

Install Security Agent

Install the Security Agent to protect your endpoints from security threats. You can download the installer or send the installer link to users.

Install the Security Agent

Configure Policy

Configure and apply security settings to specified targets. Use policies to manage settings such as Scheduled Scan, Device Control, and Data Loss Prevention.

Go to Policies

Active Directory Integration

Manage Security Agents using the Active Directory organizational unit (OU) structure. You can also discover unmanaged endpoints that have no Security Agent installed.

Enable Active Directory integration

Other Features

Check the Online Help or video tutorials to learn mo about the features availab Worry-Free Business Sec Services.

Check the Online Help

No action required. Your endpoints are protected.

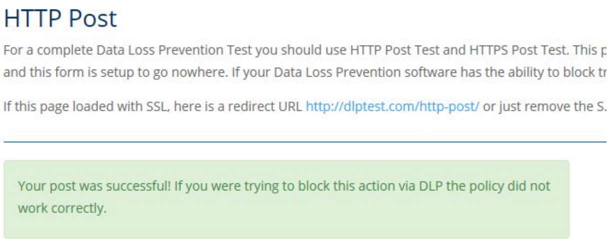
Security Risk Detections Over Time

Last 30

Part 2: Baseline Evaluation

On DLP Test perform the following tests to establish a baseline configuration:

- HTTP POST
    - ○ Test one sample SSN or CCN file



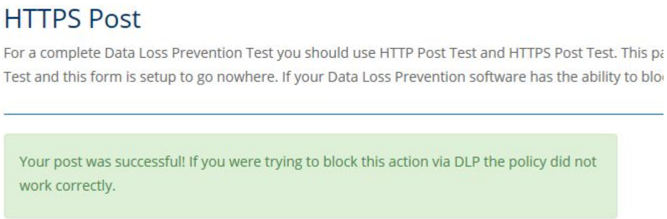
HTTP Post

For a complete Data Loss Prevention Test you should use HTTP Post Test and HTTPS Post Test. This p
and this form is setup to go nowhere. If your Data Loss Prevention software has the ability to block tr

If this page loaded with SSL, here is a redirect URL http://dlptest.com/http-post/ or just remove the S.

Your post was successful! If you were trying to block this action via DLP the policy did not work correctly.

- HTTPS POST
    - ○ Test one sample SSN or CCN file

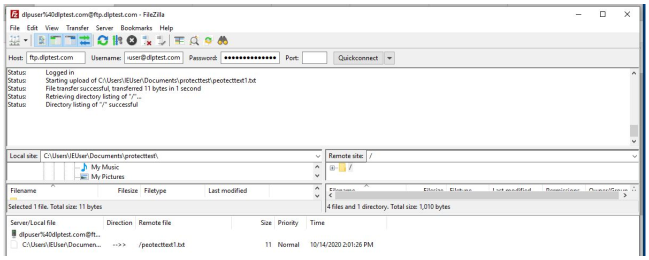


HTTPS Post

For a complete Data Loss Prevention Test you should use HTTP Post Test and HTTPS Post Test. This pa
Test and this form is setup to go nowhere. If your Data Loss Prevention software has the ability to blo

Your post was successful! If you were trying to block this action via DLP the policy did not work correctly.

- FTP Test using FileZilla
    - ○ Test all sample SSN and CCN files



dlpuser%40dlptest.com@ftp.dlptest.com - FileZilla

Host: ftp.dlptest.com Username: user@dlptest.com Password: •••••••••••••• Port:

```
Status:     Logged in
Status:     Starting upload of C:\Users\IEUser\Documents\protecttest\peotecttext1.txt
Status:     File transfer successful, transferred 11 bytes in 1 second
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
```

Local site: C:\Users\IEUser\Documents\protecttest\

Remote site: /

Filename	Filesize	Filetype	Last modified

Selected 1 file. Total size: 11 bytes

4 files and 1 directory. Total size: 1,010 bytes

Server/Local file	Direction	Remote file	Size	Priority	Time
dlpuser%40dlptest.com@ft...					
C:\Users\IEUser\Documen...	-->>	/peotecttext1.txt	11	Normal	10/14/2020 2:01:26 PM

The data types to test include:

- Social Security Number (SSN)
- Credit Card Number (CCN)
- Date of Birth (DoB)

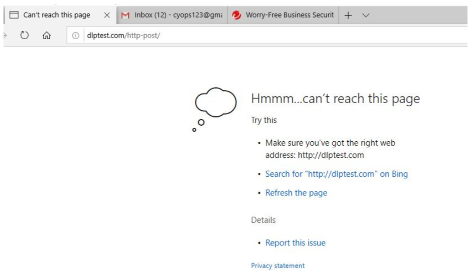
Part 3: Endpoint DLP Policy Implementation with Trend Micro

The next step will be configuring DLP settings in Trend Micro to match our needs. Today we're focusing on achieving PCI-DSS compliance, so configure a policy accordingly.

Once your agent is updated with a DLP policy, test its efficacy on DLP Test perform the following tests to establish a baseline configuration:

- HTTP POST
  - Test one sample SSN or CCN file
- HTTPS POST
  - Test one sample SSN or CCN file
- FTP Test using FileZilla
  - Test all sample SSN and CCN files

Micro trend results



dlptest.com/http-post/

Hmmm...can't reach this page

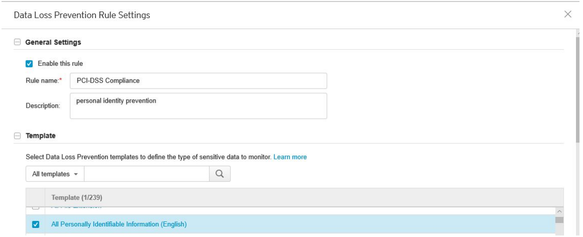
Try this

- Make sure you've got the right web address: http://dlptest.com
- Search for "http://dlptest.com" on Bing
- Refresh the page

Details

- Report this issue

Privacy statement


Data Loss Prevention Rule Settings

General Settings

☑ Enable this rule

Rule name:* PCI-DSS Compliance

Description: personal identity prevention

Template

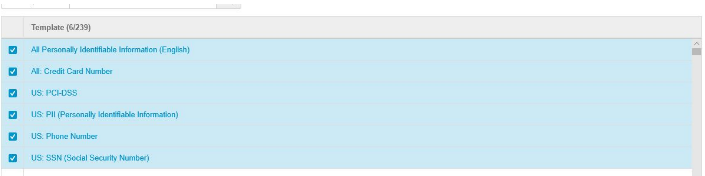
Select Data Loss Prevention templates to define the type of sensitive data to monitor. Learn more

All templates

Template (1/239)

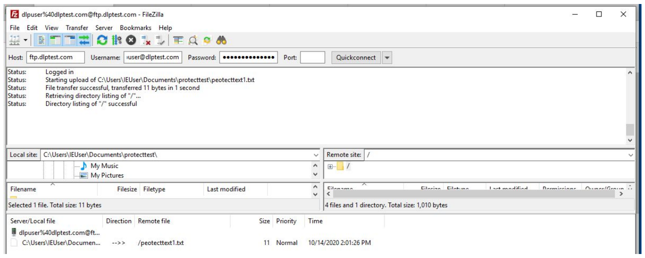
☑ All Personally Identifiable Information (English)

DPL Policy Settings


Template (6/239)

☑ All Personally Identifiable Information (English)
☑ All: Credit Card Number
☑ US: PCI-DSS
☑ US: PII (Personally Identifiable Information)
☑ US: Phone Number
☑ US: SSN (Social Security Number)

FTP



dlpuser%40dlptest.com@ftp.dlptest.com - FileZilla

Host: ftp.dlptest.com Username: ›user@dlptest.com Password: •••••••••••••• Port:

```
Status:     Logged in
Status:     Starting upload of C:\Users\IEUser\Documents\protecttest\peotecttext1.txt
Status:     File transfer successful, transferred 11 bytes in 1 second
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
```

Local site: C:\Users\IEUser\Documents\protecttest\

My Music
My Pictures

Remote site: /

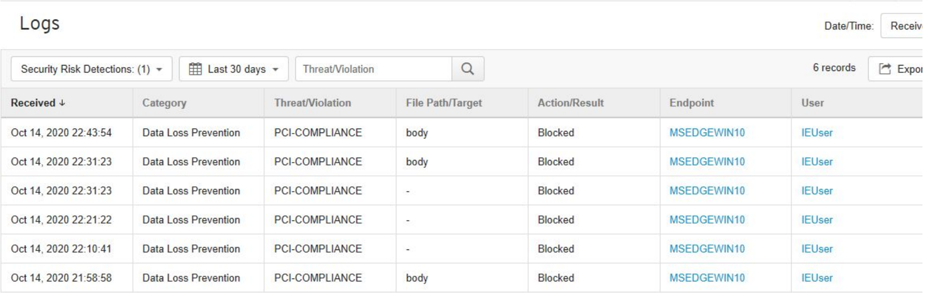
Filename Filesize Filetype Last modified

Selected 1 file. Total size: 11 bytes

4 files and 1 directory. Total size: 1,010 bytes

Server/Local file	Direction	Remote file	Size	Priority	Time
dlpuser%40dlptest.com@ft...					
C:\Users\IEUser\Documen...	-->>	/peotecttext1.txt	11	Normal	10/14/2020 2:01:26 PM

Blocked Micro


Logs

Date/Time: Receiv

Security Risk Detections: (1) | Last 30 days | Threat/Violation

6 records

Expor

Received ↓	Category	Threat/Violation	File Path/Target	Action/Result	Endpoint	User
Oct 14, 2020 22:43:54	Data Loss Prevention	PCI-COMPLIANCE	body	Blocked	MSEDGEWIN10	IEUser
Oct 14, 2020 22:31:23	Data Loss Prevention	PCI-COMPLIANCE	body	Blocked	MSEDGEWIN10	IEUser
Oct 14, 2020 22:31:23	Data Loss Prevention	PCI-COMPLIANCE	-	Blocked	MSEDGEWIN10	IEUser
Oct 14, 2020 22:21:22	Data Loss Prevention	PCI-COMPLIANCE	-	Blocked	MSEDGEWIN10	IEUser
Oct 14, 2020 22:10:41	Data Loss Prevention	PCI-COMPLIANCE	-	Blocked	MSEDGEWIN10	IEUser
Oct 14, 2020 21:58:58	Data Loss Prevention	PCI-COMPLIANCE	body	Blocked	MSEDGEWIN10	IEUser

Part 4: Policy Change Proposal

Now that you've modeled a DLP solution to address the security audit, compose a revision to company policy that addresses the classification of the included data types.

- Using the Data Policy Classification Template, compose and submit a policy document that accounts for the requested data types PII and PCI for Globex.
    - Purpose
    - Scope
    - Roles and Responsibilities
    - Data Classification Procedure
    - Data Classification Guideline
    - Impact of Level Determination
    - Appendices
        - Include your baseline & DLP policy test findings here.
            - Test finding proved successful with HTTP transfer but although all same parameters were set within the Micro Trend, the setting did not prevent personal data from being transferred through FTP or HTTPS.
    - Revision History

Globex DLP Policy