K2's Implementing DLP For Better Security And Privacy

What About Randy?

- 40+ years of technology experience, top-rated speaker for almost 40 years
- Top 25 Thought Leaders in Accounting 2011-2024
- 2004-2023 Accounting Today 100 Most Influential in Accounting for twenty years
- Inducted Accounting Hall of Fame, Feb 2011
- Monthly columns on technology in CPAPractice Advisor, weekly podcasts on technology
- Published author of six books, From Hutchinson, KS
- randy@k2e.com or randyj@nmgi.com
- 620-664-6000 x 112

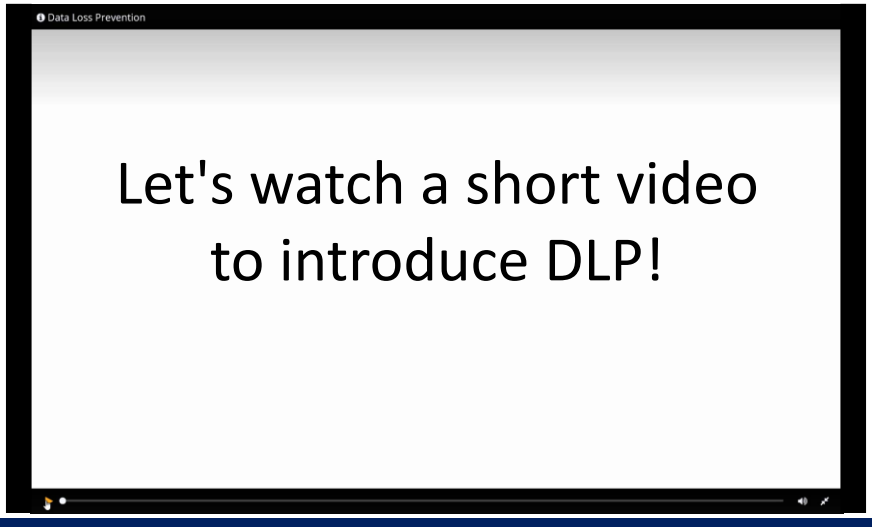
Learning Objectives

Upon completing this session, you should be able to:

- Define Data Loss Prevention (DLP)
- List examples of how DLP can enhance organizational security
- Name tools and services available that support DLP
- Identify the process for creating DLP rules in platforms such as Microsoft 365

WHAT IS DATA LOSS PREVENTION AND HOW DOES IT ENHANCE ORGANIZATIONAL SECURITY?

Introduction To DLP



What Is Data Loss Prevention?

- Data Loss Prevention (DLP) is a means of creating and enforcing security policies in an organization to reduce the risk of disclosing sensitive data, either accidentally or maliciously
- DLP can be applied at the network level, the application level, the endpoint level, or in a combination of levels
- When applied to a network, DLP tools analyze network traffic to detect potentially sensitive data
- When applied to endpoints, DLP tools can control data before it hits the network

Why Is DLP Necessary?

- Email is a notoriously insecure means of transmitting data
- Yet according to one report:
  - 56% have sent email to the wrong person
  - 53% have received unencrypted emails containing sensitive information
  - 21% have sent sensitive corporate information without encryption
  - 20% know of someone at their company who has been caught sending sensitive information without following established security protocol

Abigail Wang, *PC Magazine*

Why Is DLP Necessary?

- Consider Excel workbooks stored in a shared drive on a corporate server
- The workbook contains sensitive employee information, including Social Security numbers
- Should everyone who has access to that drive have access to the Social Security numbers?
- WellPoint exposed 128K customer medical records, including Social Security numbers, on an unsecured server for over a year

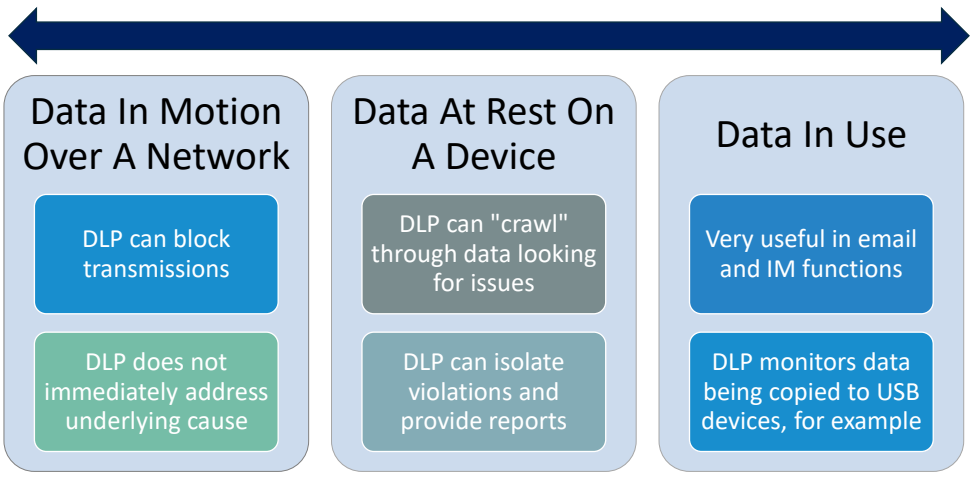
How Does DLP Enhance Security?

- DLP analyzes data in real-time, looking for patterns in the data that match specified characteristics
  - Social Security numbers and credit card numbers
- When DLP finds data that matches specified characteristics, it takes the action designated in the implemented policy
  - Sending a notification to the user and/or IT staff
  - Blocking the traffic altogether, with or without notifications to the user and/or the IT staff

Is DLP A Firewall?

- No! DLP and firewalls are fundamentally different technologies
- Firewalls serve as buffers between two networks, typically your local network and the Internet, blocking unauthorized access from one to the other
- Firewalls do not have content monitoring capabilities and do not analyze the data passing through as DLP does
- Both are necessary to help protect your systems and the sensitive data that resides on them

DLP Protects Across Three Fronts



DLP Must Have Features

- Cloud Support – must be flexible enough to support cloud, hybrid, and on-premise environments
- Advanced analytics – should expose insights on data usage, user behavior, and security risks in a way that allows anticipation of data vulnerabilities
- Data classification – ability to automatically scan information stacks to classify and tag data (possibly using AI/ML) as to risk or sensitivity
- Endpoint integration – must integrate seamlessly with servers, PCs, laptops, mobile devices, and peripherals

Before Rushing To Implement DLP

- Ensure that appropriate written policies are in place regarding the protection of sensitive data
- Educate team members on why DLP is important and how to handle matters regarding sensitive data
- How does a staff member handle a client request to email a document containing sensitive info?
  - Delicate balance between customer/client service and data/ information security

Before Rushing To Implement DLP

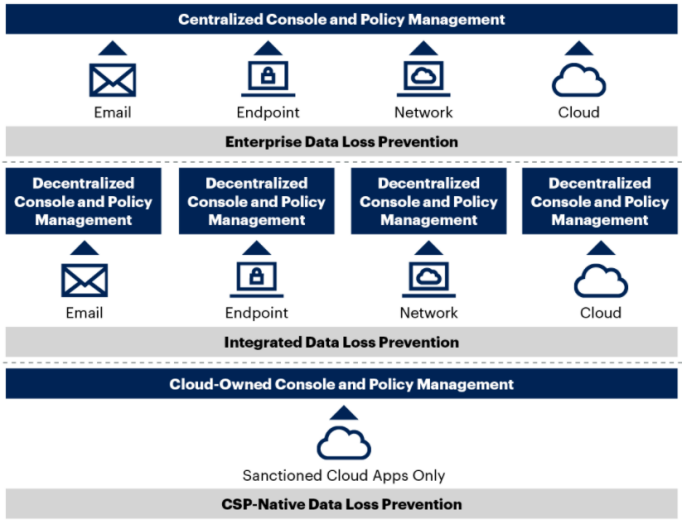
- Ensure that tools are in place to allow team members to respond to the requests and needs of clients and customers
  - Is a secure portal a viable option?
  - What about encrypted email?
  - What about simply encrypting a PDF document with a password?
  - What other options exist to satisfy the client or customer without unduly burdening your client or staff while providing exceptional service?

LEADING DLP TOOLS AND SERVICES

Three Classes of DLP Solutions

- Enterprise DLP – offer centralized policy management and reporting and generally incorporate advanced content inspection techniques
- Integrated DLP – are natively integrated within a service, such as secure email, web gateway, or endpoint protection, with generally limited policy and reporting capabilities
- Cloud Service Provider Native DLP – built in to provide data protection and visibility within a cloud ecosystem from a SaaS or IaaS provider

DLP Class Comparison



Gartner DLP Market Guide

Small and mid-size organizations tend to deploy DLP integrated within specific services (IDLP). CSP-Native DLP solutions offer capabilities much like those of EDLP vendors and are increasingly being chosen by organizations pursuing a cloud-first strategy.

Gartner DLP Market Guide

Some DLP Solutions

- Microsoft Purview Data Loss Prevention
- Forcepoint DLP
- Broadcom Symantec Data Loss Prevention
- Fortra Data Protection
- Trellix Data Loss Prevention Endpoint
- GTB Technologies DLP
- Proofpoint Enterprise Data Loss Prevention
- And many more on the Gartner DLP reviews site

Forrester Wave for Data Security Platforms, Q1 2023

- The DLP market has followed data into the cloud and most platforms run as a service against cloud data
- With many employees remaining either hybrid or remote, it is natural to migrate both applications and data protection to the cloud
- Significant threats to consider include leakage through the use of AI platforms like ChatGPT, collaboration platforms like Slack and Teams
- These threats are in addition to the standard threats such as unprotected web shares outside the organization and e-mail attachments

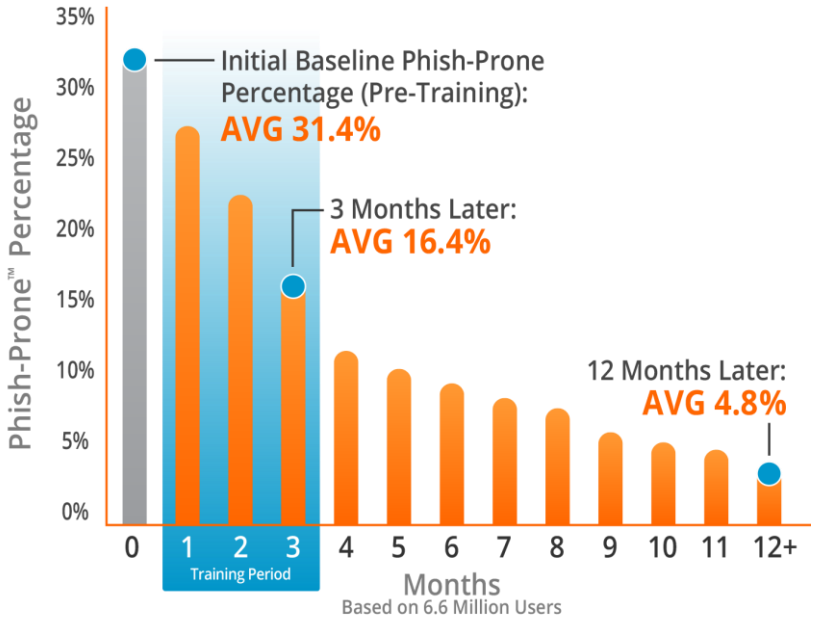
DLP In Context

- DLP is helpful for blocking inappropriate data sharing through email and other web platforms, but the real problem which must be addressed is user behavior
- While behavior cannot be changed overnight, a critical first step to any information protection initiative is to assess and enhance the organization's security awareness training
- Security awareness training from vendors like KnowBe4, SANS Institute, and others is just as important as DLP
- If users don't know what is acceptable/unacceptable, they are much more likely to engage in risky behavior

KnowBe4

Security Awareness Training

- **Train Your Users.** The world's most extensive library of security awareness training content. Automated training campaigns with scheduled reminder emails.
- **Phish Your Users.** Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.
- **See The Results.** Enterprise-strength reporting, showing stats and graphs for training and phishing, is ready for management. Show the great ROI!
- Learn more at https://www.knowbe4.com/

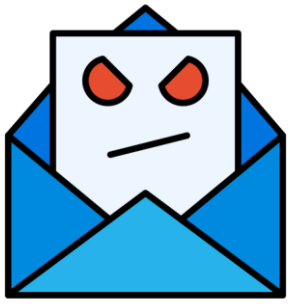


KnowBe4 Phishing Training Results

Go Phish

Open-Source Phishing Framework

- Gophish is a robust, open-source phishing framework that makes it easy to test your organization's exposure to phishing.
- Set Templates & Targets. Gophish makes it easy to create or import pixel-perfect phishing templates. Their web UI includes a full HTML editor, making it easy to customize your templates right in your browser.
- Launch the Campaign. Launch the campaign, and phishing emails are sent in the background. You can also schedule campaigns to launch whenever you'd like.
- Track Results. Detailed results are delivered in near real-time. Results can be exported for use in reports.
- Get started for free at https://getgophish.com/

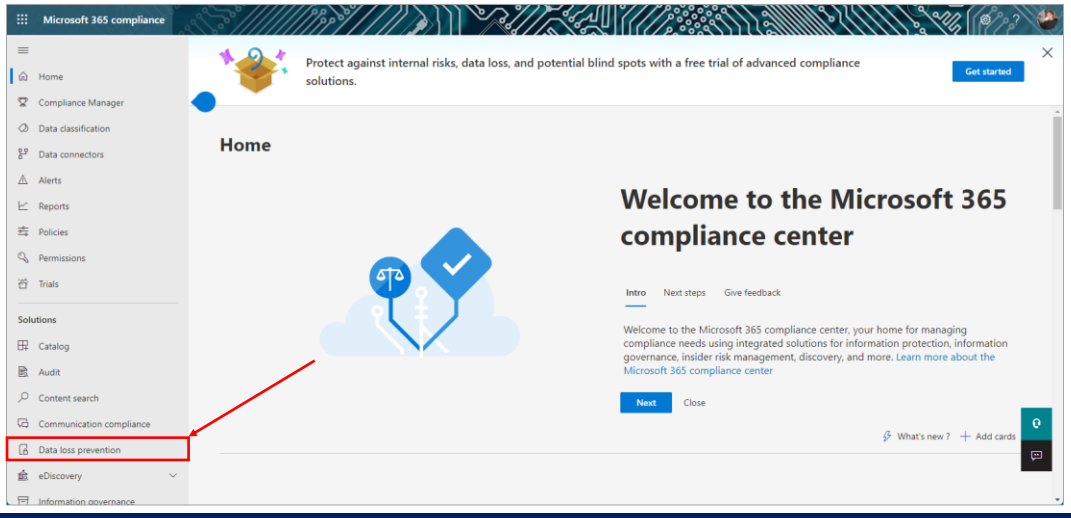


IMPLEMENTING DLP RULES TO PROTECT SENSITIVE DATA IN MICROSOFT 365

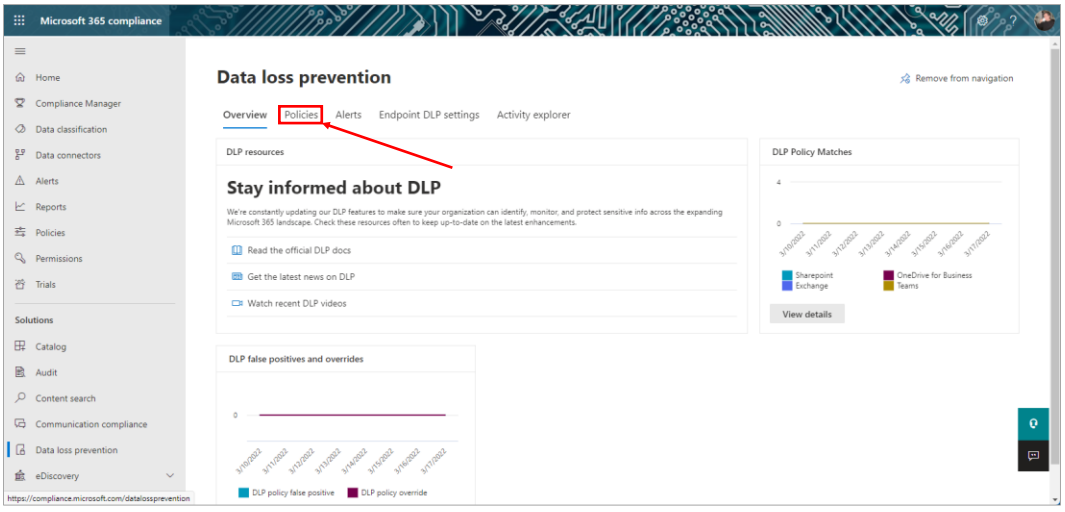
Implementing DLP In Exchange Online

- Many business professionals today have email provided through Exchange Online accounts, often as part of Microsoft Office 365 subscription
- Administrative users in Exchange Online can create and deploy DLP rules, provided the organization has a Plan 2 Exchange account, which includes Office 365 E3 and E5
- A good place to start is this TechNet article http://bit.ly/2lMnSGu

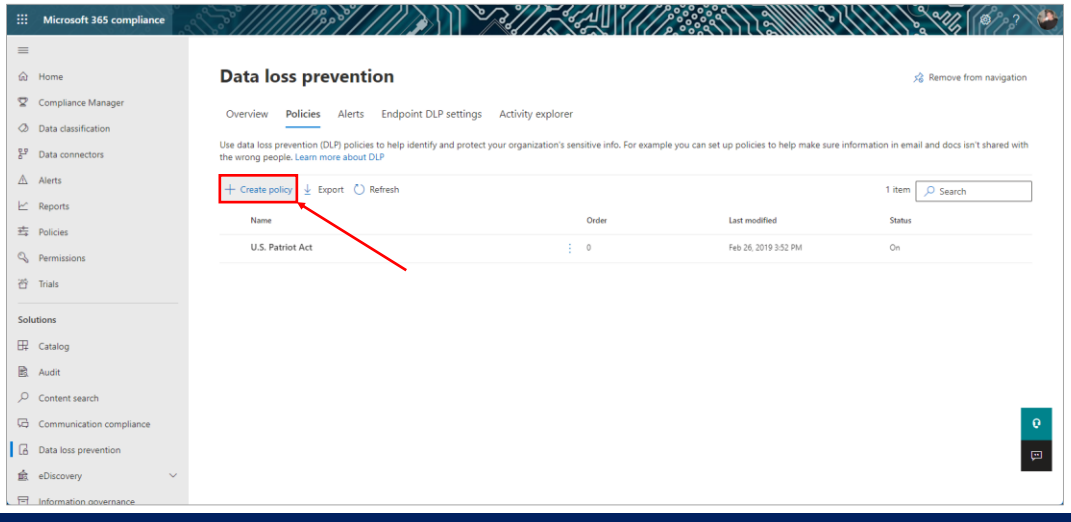
Open The 365 Compliance Center



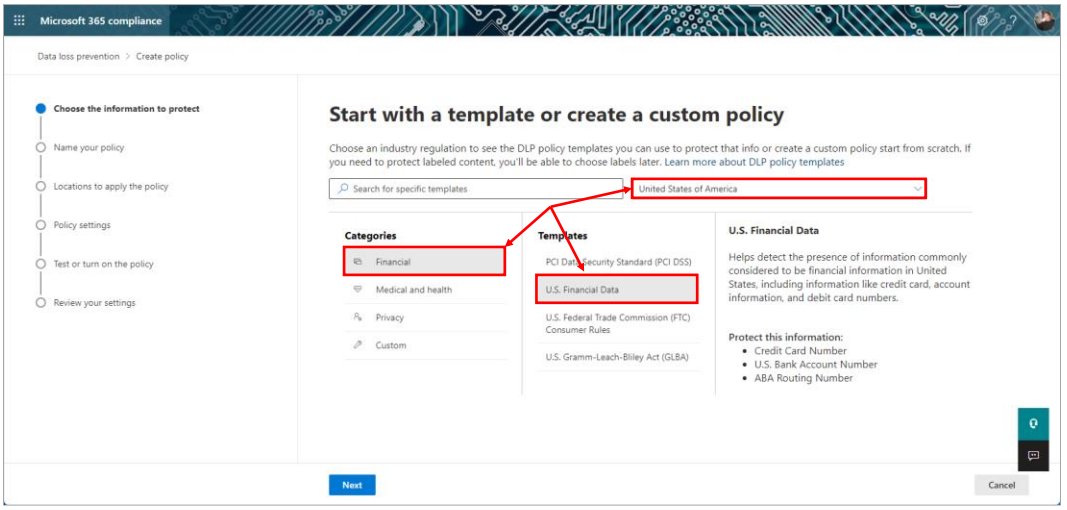
Click Policies



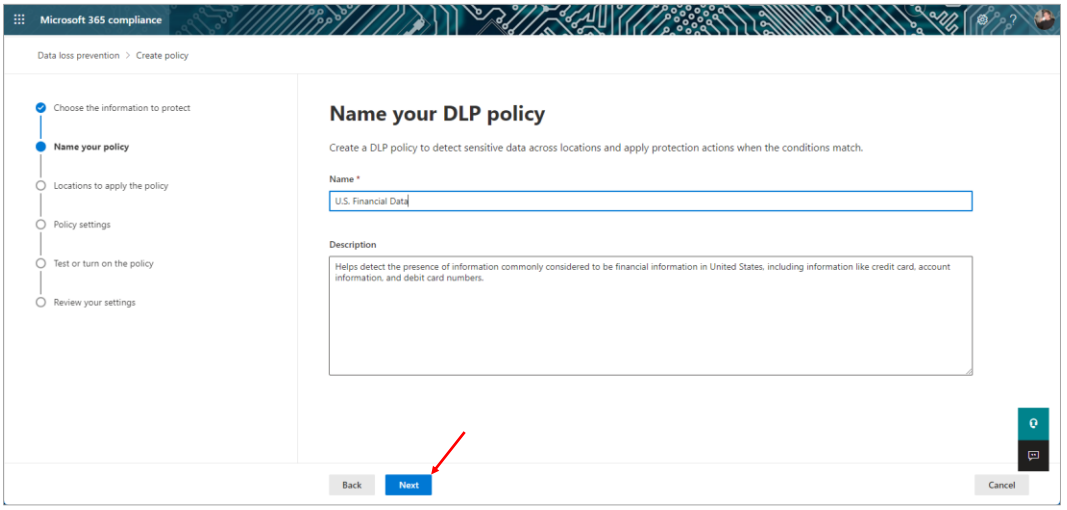
Click Create Policy



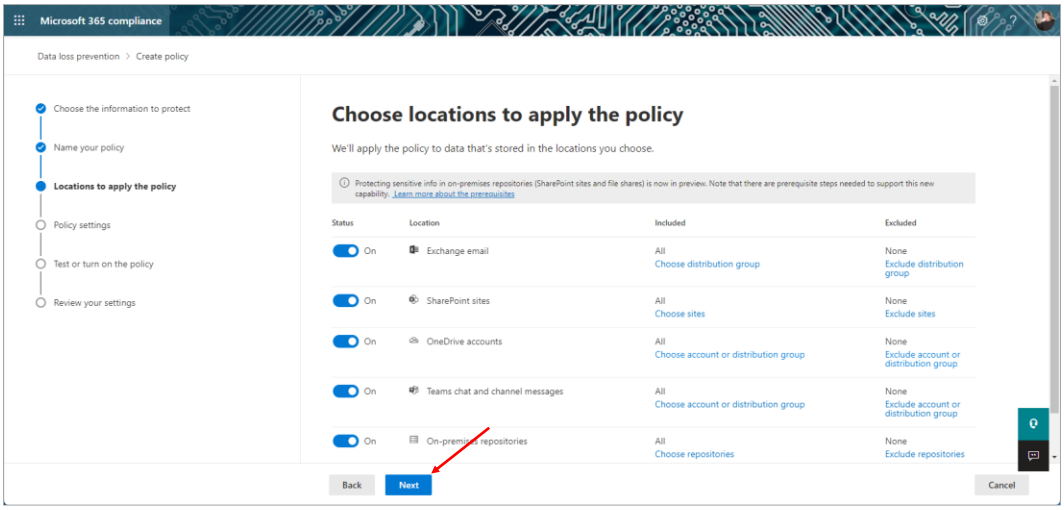
Select A Policy Template



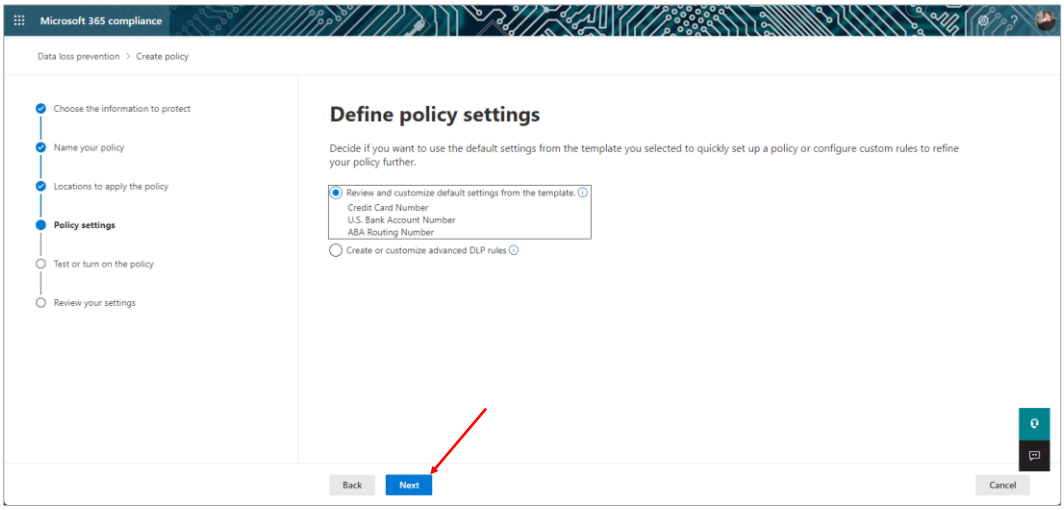
Use The Default Name



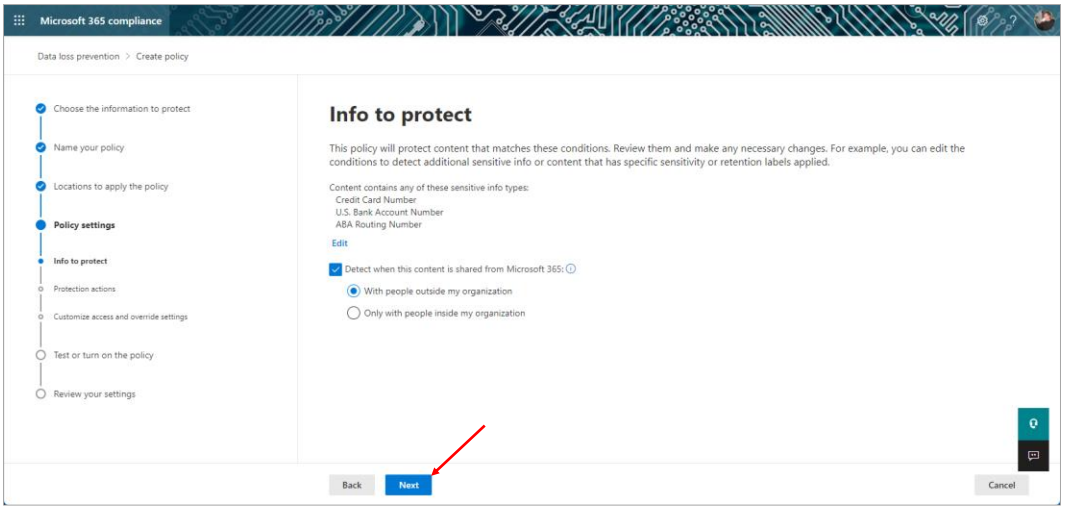
Choose Locations To Apply



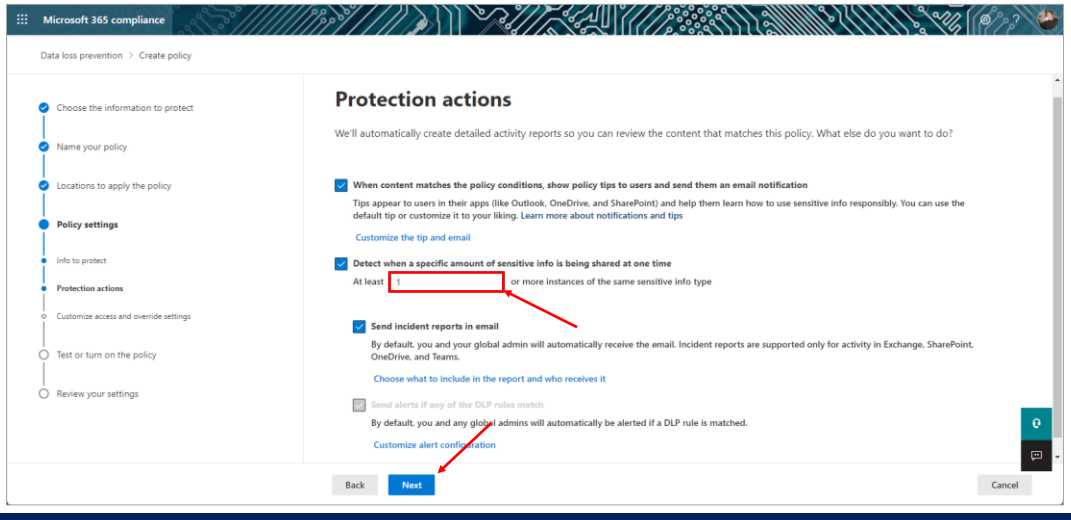
Click Next



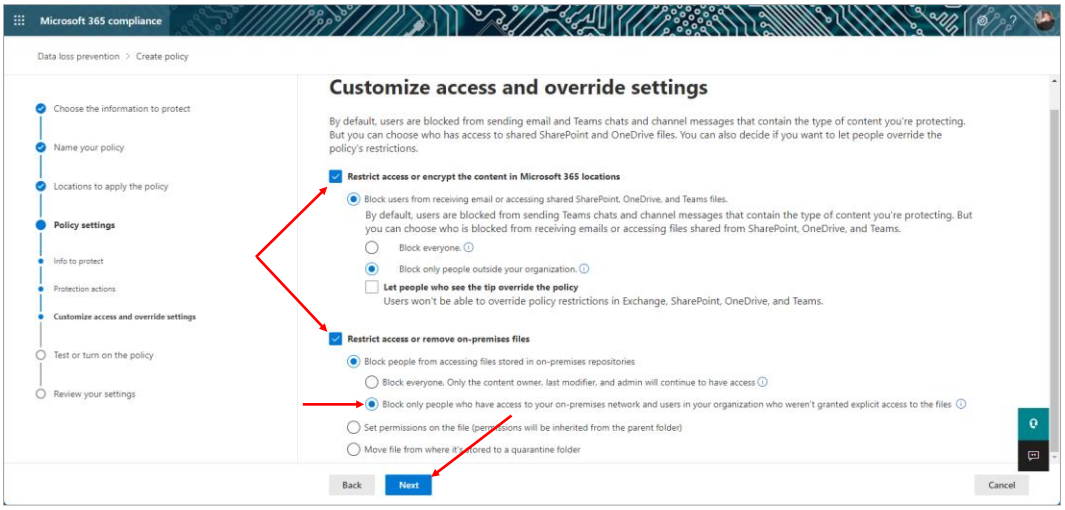
Identify Info To Protect



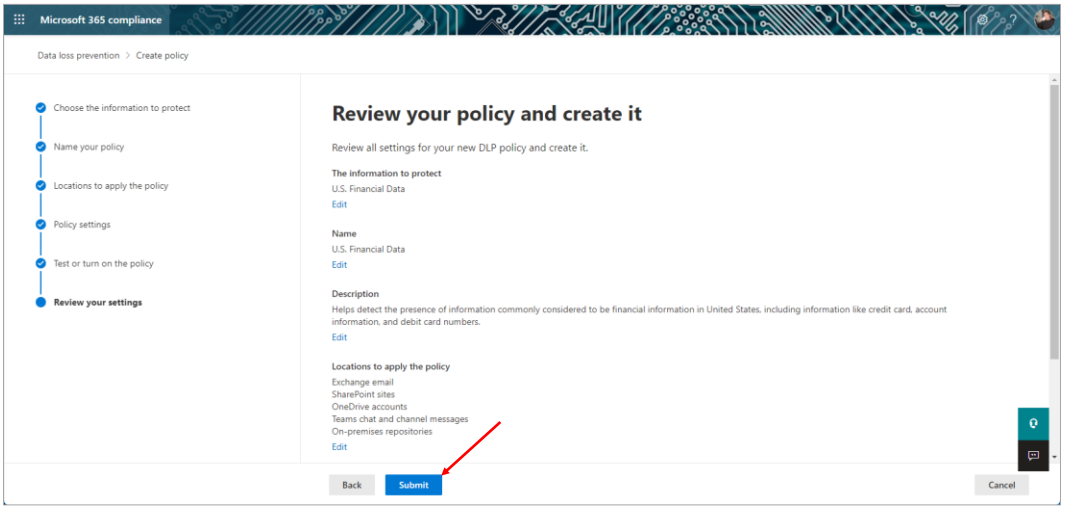
Select A Single Instance



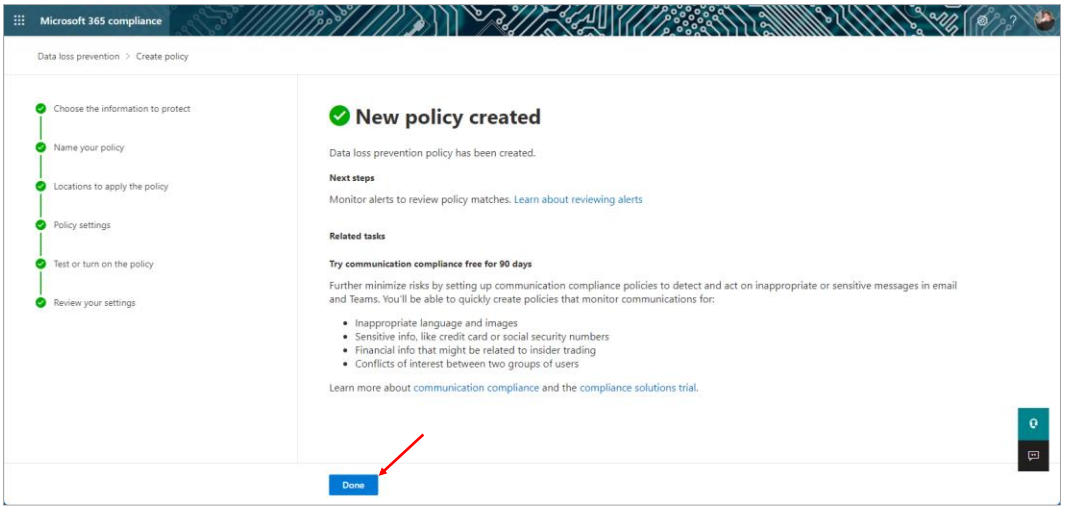
Customize Access And Override



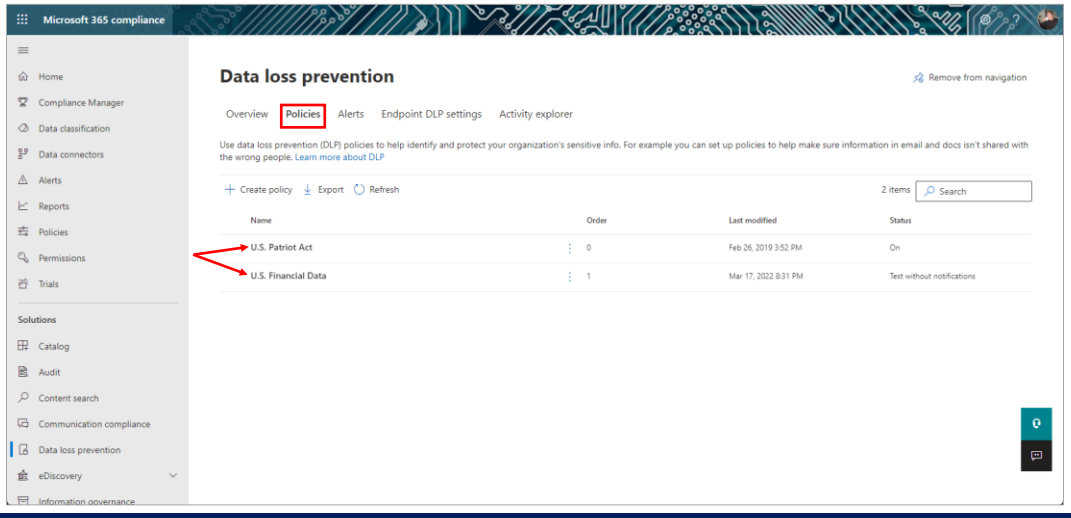
Create The Policy



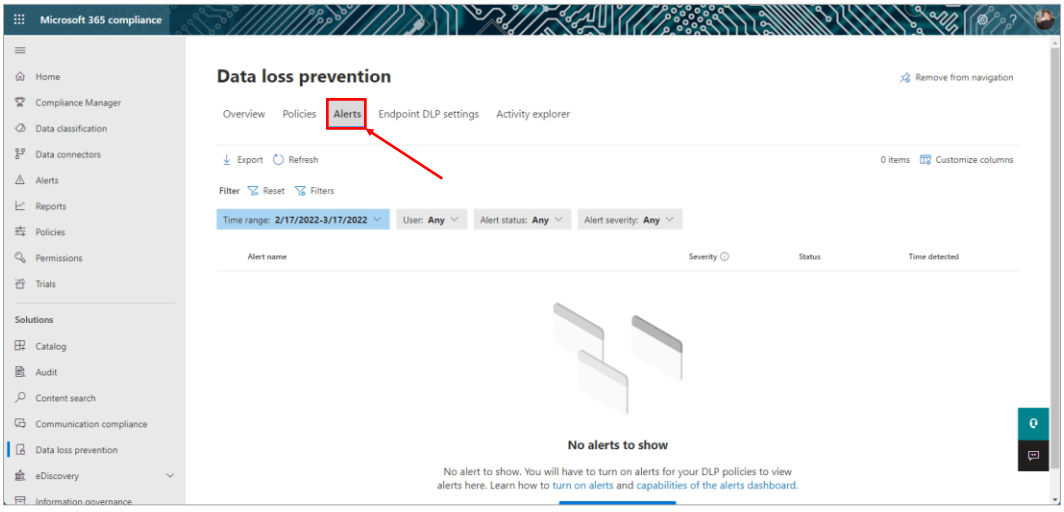
Confirm Policy Created



Return To DLP Compliance

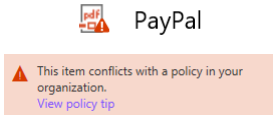


Violations Appear On Alerts Tab

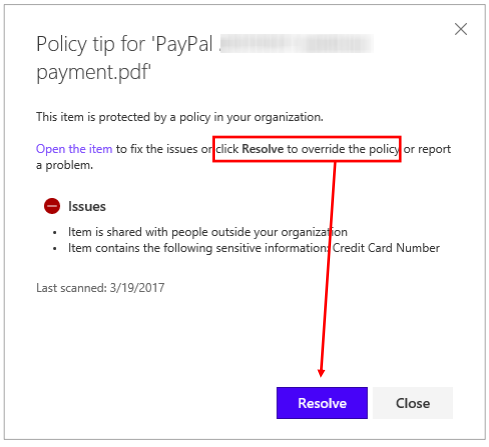


DLP SharePoint Policy Tip

Override Only Appears If You Chose To Allow Overrides



File Flagged in SharePoint Document Library



Take Aways

- Establishing policies and training end-users is still a vital aspect of information security
- Recognize the human element and understand that mistakes – some honest and some intentional – will compromise the security of sensitive data
- DLP provides an added layer of protection to block the outflow of sensitive data before we have a significant breach
- DLP has become a must-have technology in modern business

QUESTIONS?