

K2's Implementing DLP For Better Security And Privacy

Learning Objectives



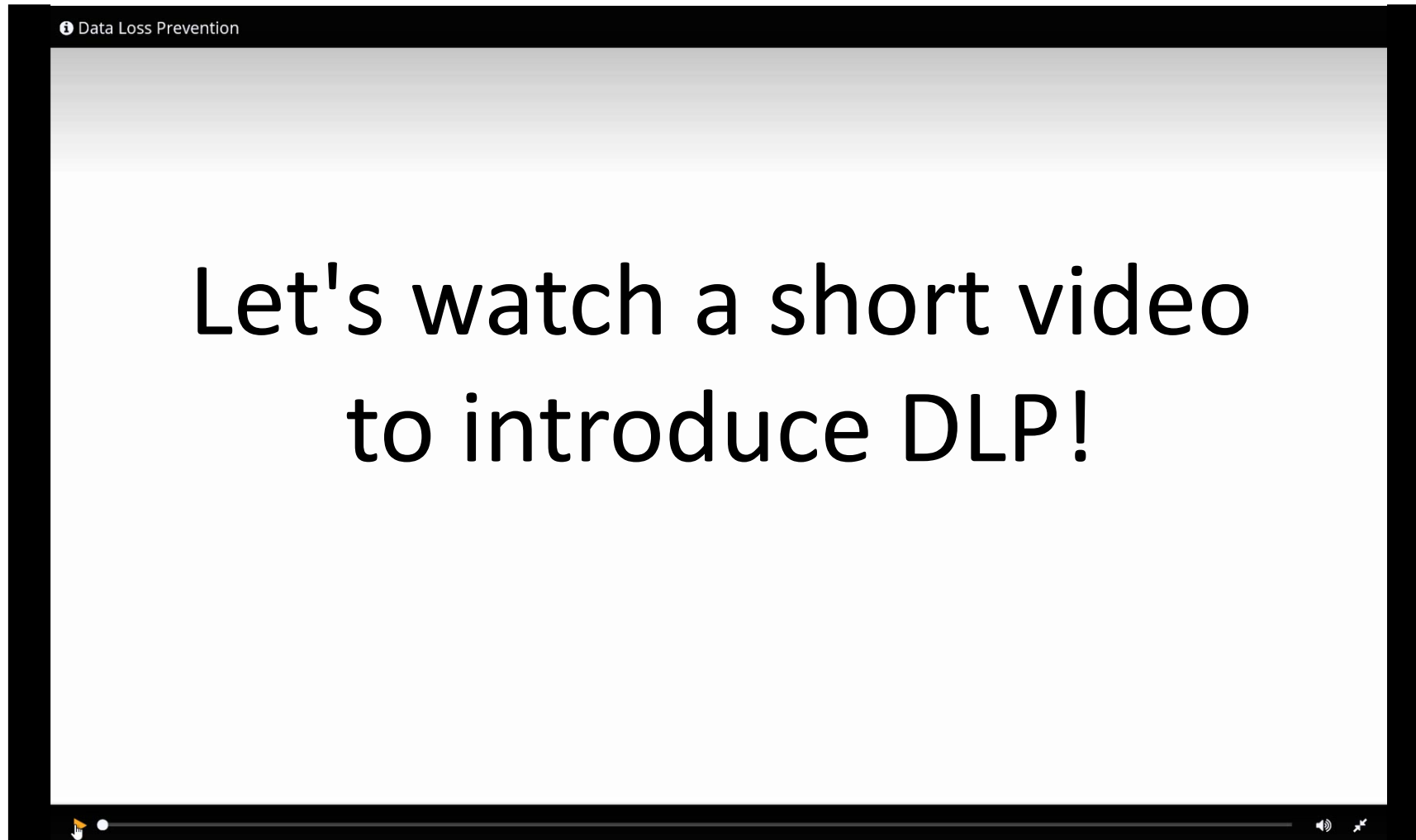
Upon completing this session, you should be able to:

- 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*, July 20, 2013

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?



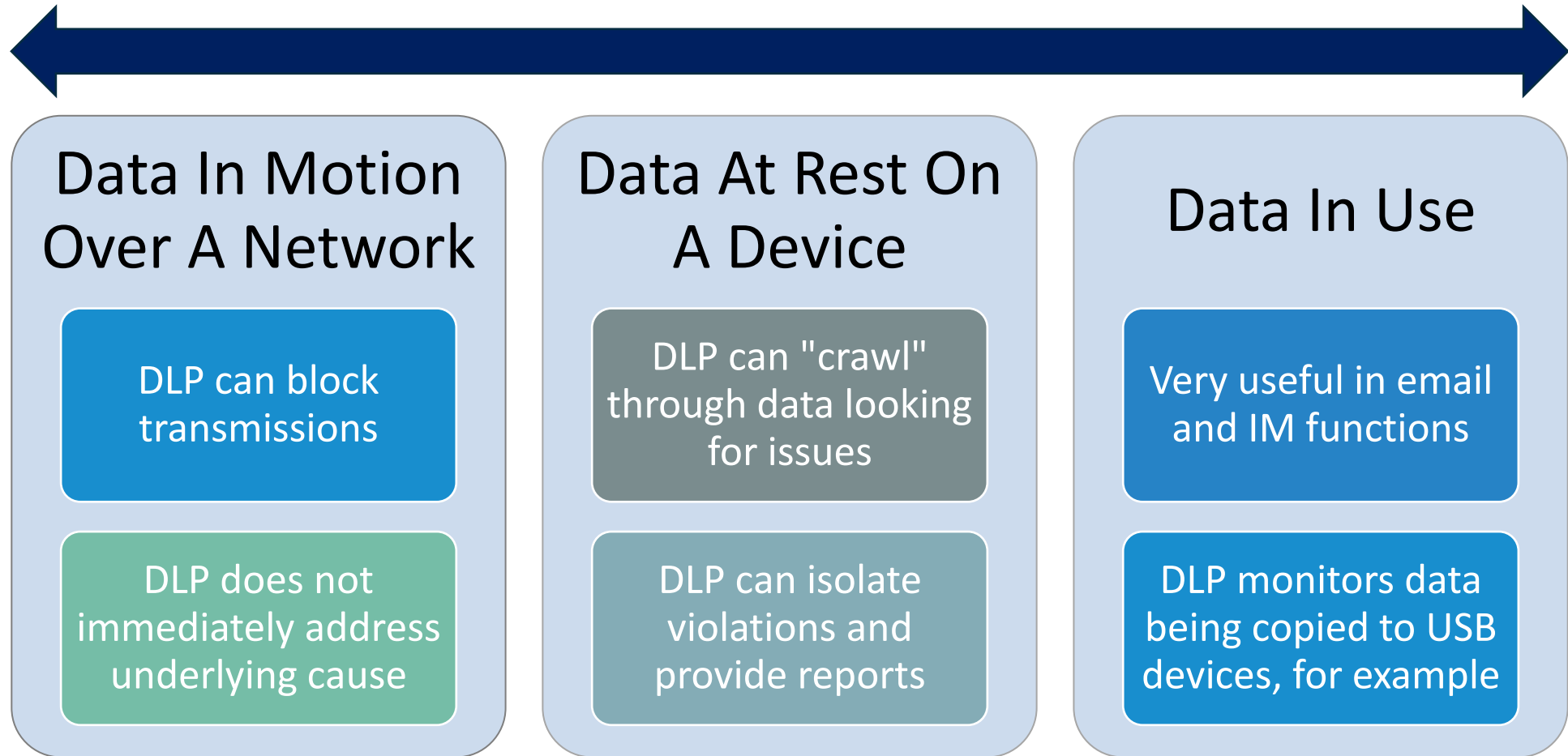
- DLP analyzes data in real-time, looking for patterns in the data that match specified characteristics
 - Social Security numbers and credit card numbers
- When DLP finds data that matches specified characteristics, it takes the action designated in the implemented policy
 - Sending a notification to 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?



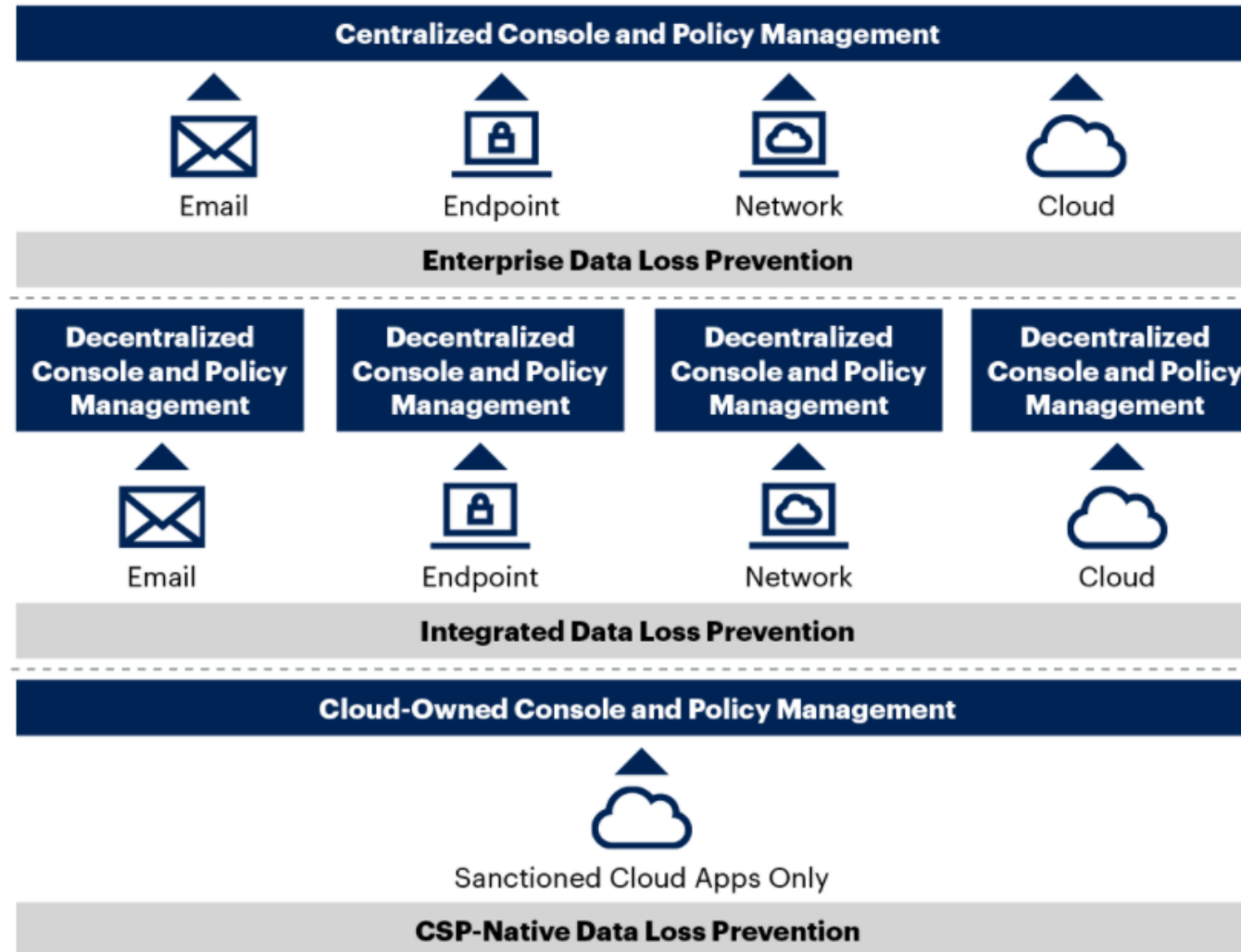
LEADING DLP TOOLS AND SERVICES

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



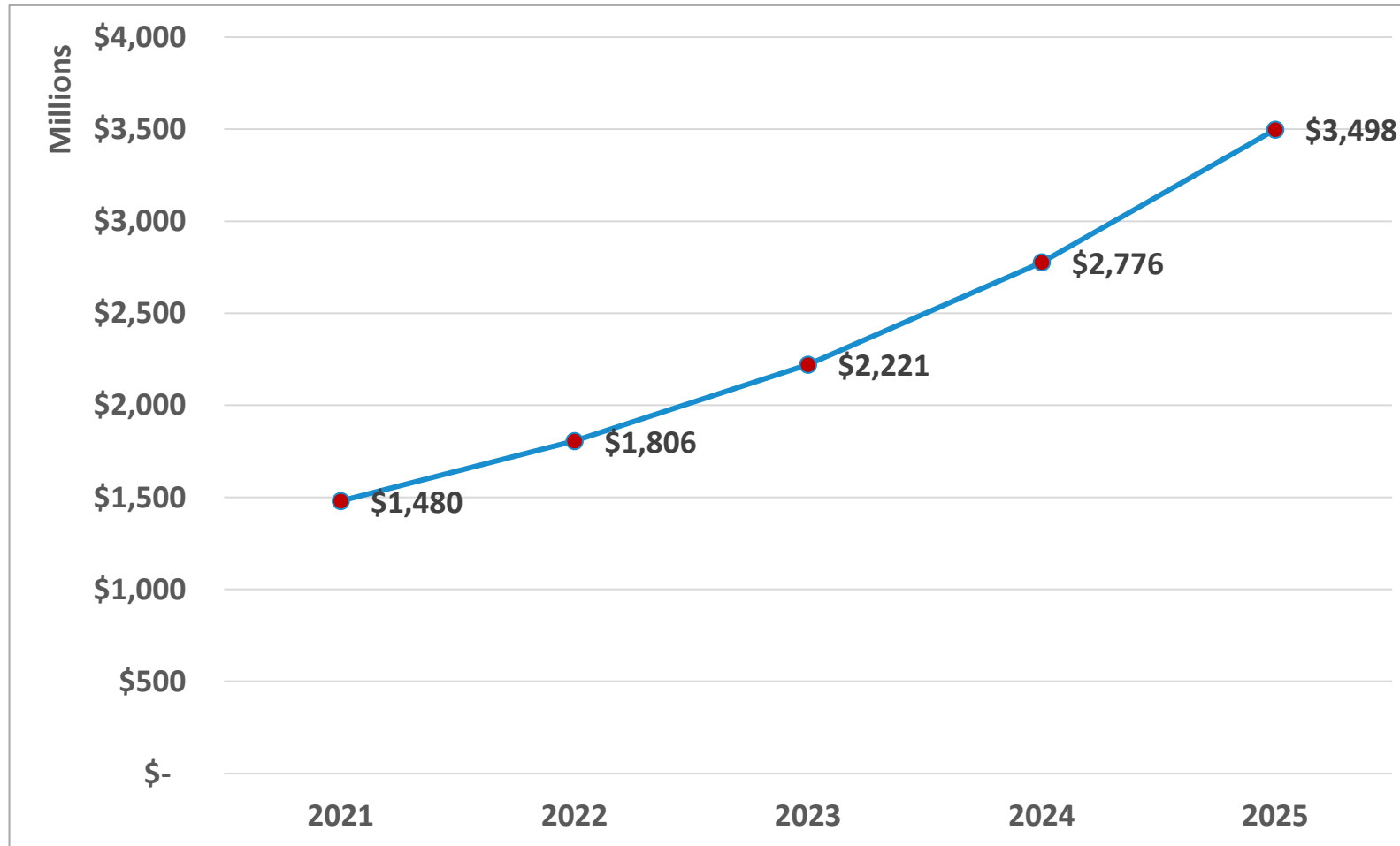
Gartner DLP Market Guide
June 2021



Small and mid-size organizations tend to deploy DLP integrated within specific services (IDL). 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 – June 2021

DLP Forecast Market Growth



Data from Radicati – Nov 2021

Leading DLP Solutions



- Gartner has not produced an updated version of their Magic Quadrant for DLP since 2016
 - Market has matured with only minor movements in the 2x2 matrix
 - Shift away from enterprise DLP to Secure Access Service Edge (SASE) data protection solutions



Gartner Magic Quadrant for DLP – Jan 2016

Leading DLP Solutions



- Similarly, Forrester has not produced an updated version of their Wave for DLP since 2016

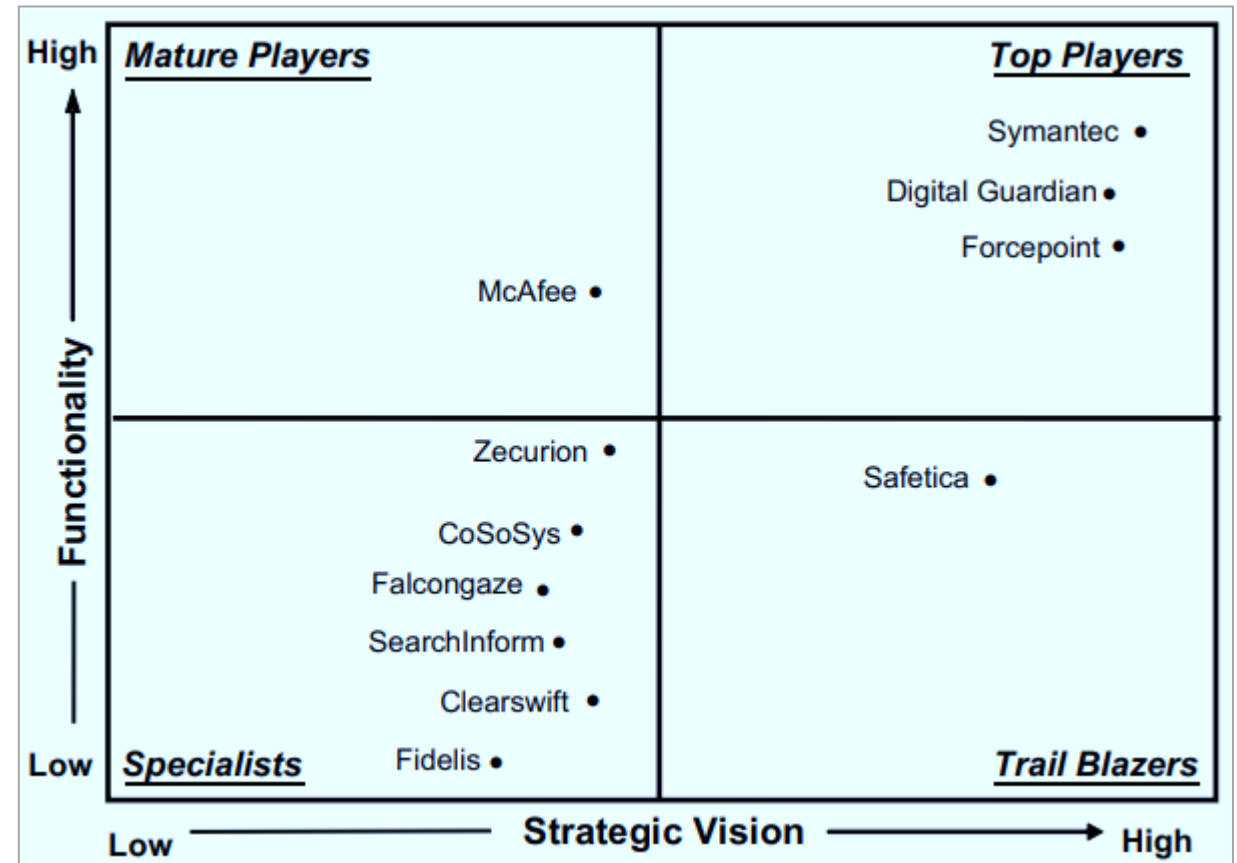


Forrester Wave for DLP – Q4 2016

Leading DLP Solutions



- Symantec
- Digital Guardian
- Forcepoint
- McAfee (Intel)
- Zecurion
- CoSoSys
- Falcongaze
- Clearswift
- Fidelis



Radicati DLP Market Quadrant – Nov 2021

Symantec



- Through acquisition of Vontu years ago, Symantec quickly became a leader in this field
- Symantec was acquired by Broadcom, Inc. in late 2019
- Today's solution from Symantec is one of the more robust enterprise tools available in the market
- Good fit for larger organizations and those requiring more advanced capabilities

Forcepoint



- In addition to traditional DLP, Forcepoint also incorporates analytics and insider threat detection into its tools
- Strong report-writing capabilities are also included
- Like Symantec, Forcepoint is probably best-suited for larger organizations and organizations with more complex security issues and requirements

Digital Guardian



- Historically, Digital Guardian's approach to DLP was largely through endpoint security
- However, with the 2015 acquisition of Code Green Networks, the company now has strong network DLP tools
- Supports complex use cases involving intellectual property and trade secret protection with both content and context awareness
- Can be implemented in the Cloud, on-premise, or in hybrid environments

McAfee Total Protection



- McAfee DLP fully integrates Onigma for endpoint DLP and Reconnex for network DLP
- Additional strength is provided by McAfee Web Gateway real-time inspection of inbound and outbound web content
- Solution is targeted to larger organizations

GTB Technologies



- GTB provides one of the most affordable solutions on the market and appears to have a niche with SMBs
- Simple solution to deploy that provides relatively easy on-going management
- Can be deployed in the Cloud, on premise, as a managed service, or in hybrid environments
 - Can be moved from one platform to another as needs change
- Majority of customers report positive ROI in one week to three months

Clearswift



- Recently acquired by RUAG, a Swiss holding company
- Strong email security and encryption capabilities provided in a very easy-to-manage suite
- Uses "adaptive reaction" to automatically remove sensitive data as it passes through the network
- Can sanitize incoming data, helping to protect from viruses and ransomware
- Clearswift can be used by organizations of all sizes

DeviceLock



- Acquired by Acronis in July 2020
- Very scalable solution that can be used by SMB through enterprise-class organizations
- Solution focuses on endpoint control
- Product is quick deployment enabled, often without the need for professional assistance



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/2IMnSGu>



Open The 365 Compliance Center



Microsoft 365 compliance

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Information governance

Protect against internal risks, data loss, and potential blind spots with a free trial of advanced compliance solutions. [Get started](#)

Home

Welcome to the Microsoft 365 compliance center

[Intro](#) [Next steps](#) [Give feedback](#)

Welcome to the Microsoft 365 compliance center, your home for managing compliance needs using integrated solutions for information protection, information governance, insider risk management, discovery, and more. [Learn more about the Microsoft 365 compliance center](#)

[Next](#) [Close](#)

[What's new?](#) [+ Add cards](#)

Click Policies



Microsoft 365 compliance

Data loss prevention Remove from navigation

Overview **Policies** Alerts Endpoint DLP settings Activity explorer

DLP resources

Stay informed about DLP

We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

- Read the official DLP docs
- Get the latest news on DLP
- Watch recent DLP videos

DLP Policy Matches

4

0

3/10/2022 3/11/2022 3/12/2022 3/13/2022 3/14/2022 3/15/2022 3/16/2022 3/17/2022

Sharepoint Exchange OneDrive for Business Teams

View details

DLP false positives and overrides

0

3/10/2022 3/11/2022 3/12/2022 3/13/2022 3/14/2022 3/15/2022 3/16/2022 3/17/2022

DLP policy false positive DLP policy override

<https://compliance.microsoft.com/datalossprevention>

Click Create Policy



Microsoft 365 compliance



Data loss prevention

Overview **Policies** Alerts Endpoint DLP settings Activity explorer

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

[+ Create policy](#) [↓ Export](#) [↻ Refresh](#) 1 item

Name	Order	Last modified	Status
U.S. Patriot Act	0	Feb 26, 2019 3:52 PM	On

Select A Policy Template



Microsoft 365 compliance

Data loss prevention > Create policy

Choose the information to protect

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

Search for specific templates

United States of America

Categories	Templates
Financial	PCI Data Security Standard (PCI DSS)
Medical and health	U.S. Financial Data
Privacy	U.S. Federal Trade Commission (FTC) Consumer Rules
Custom	U.S. Gramm-Leach-Bliley Act (GLBA)

U.S. Financial Data

Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Protect this information:

- Credit Card Number
- U.S. Bank Account Number
- ABA Routing Number

Next

Cancel

Use The Default Name



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy**
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *

Description

Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Back Next Cancel

Choose Locations To Apply



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories	None Exclude repositories

Back **Next** Cancel

Click Next



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings**
- Test or turn on the policy
- Review your settings

Define policy settings

Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further.

- Review and customize default settings from the template. ⓘ
 - Credit Card Number
 - U.S. Bank Account Number
 - ABA Routing Number
- Create or customize advanced DLP rules ⓘ

Back Next Cancel

Identify Info To Protect



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings**
- Info to protect**
- Protection actions
- Customize access and override settings
- Test or turn on the policy
- Review your settings

Info to protect

This policy will protect content that matches these conditions. Review them and make any necessary changes. For example, you can edit the conditions to detect additional sensitive info or content that has specific sensitivity or retention labels applied.

Content contains any of these sensitive info types:

- Credit Card Number
- U.S. Bank Account Number
- ABA Routing Number

[Edit](#)

Detect when this content is shared from Microsoft 365: ⓘ

- With people outside my organization
- Only with people inside my organization

Back Next Cancel

Select A Single Instance



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings**
- Info to protect
- Protection actions
- Customize access and override settings
- Test or turn on the policy
- Review your settings

Protection actions

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

- When content matches the policy conditions, show policy tips to users and send them an email notification**
Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)
- Detect when a specific amount of sensitive info is being shared at one time**
At least or more instances of the same sensitive info type
- Send incident reports in email**
By default, you and your global admin will automatically receive the email. Incident reports are supported only for activity in Exchange, SharePoint, OneDrive, and Teams.
[Choose what to include in the report and who receives it](#)
- Send alerts if any of the DLP rules match**
By default, you and any global admins will automatically be alerted if a DLP rule is matched.
[Customize alert configuration](#)

Back Next Cancel

Customize Access And Override



Microsoft 365 compliance

Data loss prevention > Create policy

Customize access and override settings

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

- Restrict access or encrypt the content in Microsoft 365 locations**
 - Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.
 - Block everyone. ⓘ
 - Block only people outside your organization. ⓘ
 - Let people who see the tip override the policy**
Users won't be able to override policy restrictions in Exchange, SharePoint, OneDrive, and Teams.
- Restrict access or remove on-premises files**
 - Block people from accessing files stored in on-premises repositories
 - Block everyone. Only the content owner, last modifier, and admin will continue to have access ⓘ
 - Block only people who have access to your on-premises network and users in your organization who weren't granted explicit access to the files ⓘ
 - Set permissions on the file (permissions will be inherited from the parent folder)
 - Move file from where it's stored to a quarantine folder

Back Next Cancel

Create The Policy



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings**

Review your policy and create it

Review all settings for your new DLP policy and create it.

The information to protect
U.S. Financial Data
[Edit](#)

Name
U.S. Financial Data
[Edit](#)

Description
Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.
[Edit](#)

Locations to apply the policy
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
On-premises repositories
[Edit](#)

[Back](#) [Submit](#) [Cancel](#)

Confirm Policy Created



Microsoft 365 compliance

Data loss prevention > Create policy

- Choose the information to protect
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

✔ New policy created

Data loss prevention policy has been created.

Next steps

Monitor alerts to review policy matches. [Learn about reviewing alerts](#)

Related tasks

Try communication compliance free for 90 days

Further minimize risks by setting up communication compliance policies to detect and act on inappropriate or sensitive messages in email and Teams. You'll be able to quickly create policies that monitor communications for:

- Inappropriate language and images
- Sensitive info, like credit card or social security numbers
- Financial info that might be related to insider trading
- Conflicts of interest between two groups of users

Learn more about [communication compliance](#) and the [compliance solutions trial](#).

Done



Return To DLP Compliance



Microsoft 365 compliance

Data loss prevention

Overview **Policies** Alerts Endpoint DLP settings Activity explorer

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

+ Create policy ↓ Export ↻ Refresh 2 items

Name	Order	Last modified	Status
U.S. Patriot Act	0	Feb 26, 2019 3:52 PM	On
U.S. Financial Data	1	Mar 17, 2022 8:31 PM	Test without notifications

Note: Red arrows point to the 'U.S. Patriot Act' and 'U.S. Financial Data' rows in the table.

Violations Appear On Alerts Tab

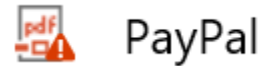



The screenshot displays the Microsoft 365 compliance center interface. The left-hand navigation pane includes sections for 'Solutions' and 'Data loss prevention'. The 'Alerts' tab is selected and highlighted with a red box, with a red arrow pointing to it. The main content area is titled 'Data loss prevention' and contains sub-tabs for 'Overview', 'Policies', 'Alerts', 'Endpoint DLP settings', and 'Activity explorer'. Below the sub-tabs are options for 'Export', 'Refresh', and 'Customize columns'. A filter section shows 'Time range: 2/17/2022-3/17/2022', 'User: Any', 'Alert status: Any', and 'Alert severity: Any'. A table header is visible with columns for 'Alert name', 'Severity', 'Status', and 'Time detected'. The table is currently empty, displaying a message: 'No alerts to show. No alert to show. You will have to turn on alerts for your DLP policies to view alerts here. Learn how to [turn on alerts](#) and [capabilities of the alerts dashboard](#).' The 'Alerts' tab in the left navigation pane is highlighted with a blue bar.

DLP SharePoint Policy Tip



**Override Only
Appears If You
Chose To Allow
Overrides**




 This item conflicts with a policy in your organization.
[View policy tip](#)

File Flagged in
SharePoint
Document Library

Policy tip for 'PayPal [REDACTED] payment.pdf' ✕

This item is protected by a policy in your organization.

[Open the item](#) to fix the issues or **click Resolve to override the policy** or report a problem.

 **Issues**

- Item is shared with people outside your organization
- Item contains the following sensitive information: Credit Card Number

Last scanned: 3/19/2017

[Resolve](#) [Close](#)

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



E-mail:

randy@k2e.com

brian@k2e.com

QUESTIONS?

