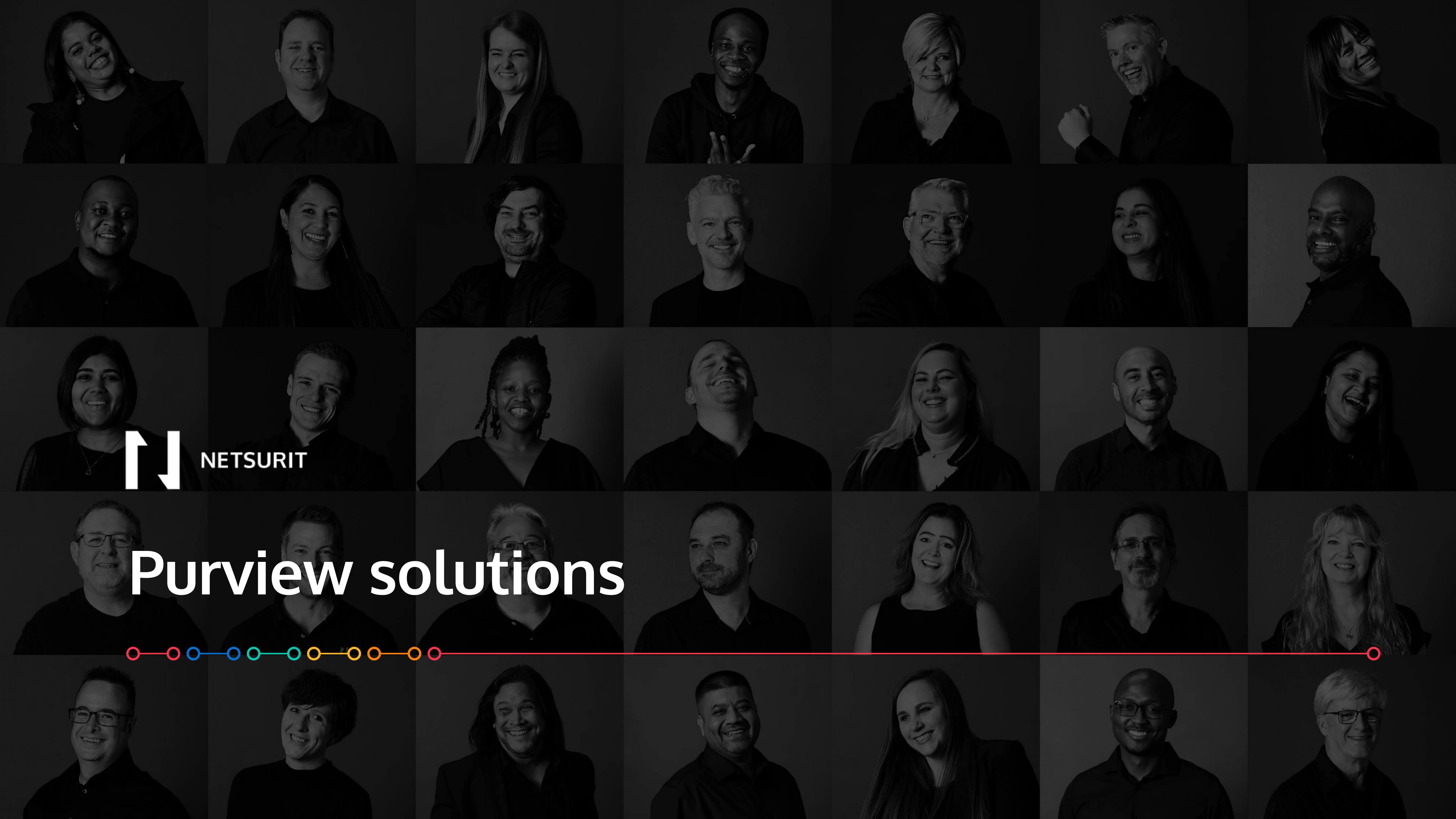


NETSURIT

Purview solutions

Who is Netsurit?

PROVEN EXPERTISE

28 YEARS IN OPERATION

23 YEARS AS MICROSOFT GOLD PARTNER

- Preferred Microsoft Solutions Partner
- 6 Microsoft Advanced Specializations
- Extensive AI and Enablement experience
- Member of Microsoft Intelligent Security Association (MISA)

TRUSTED PROVIDER

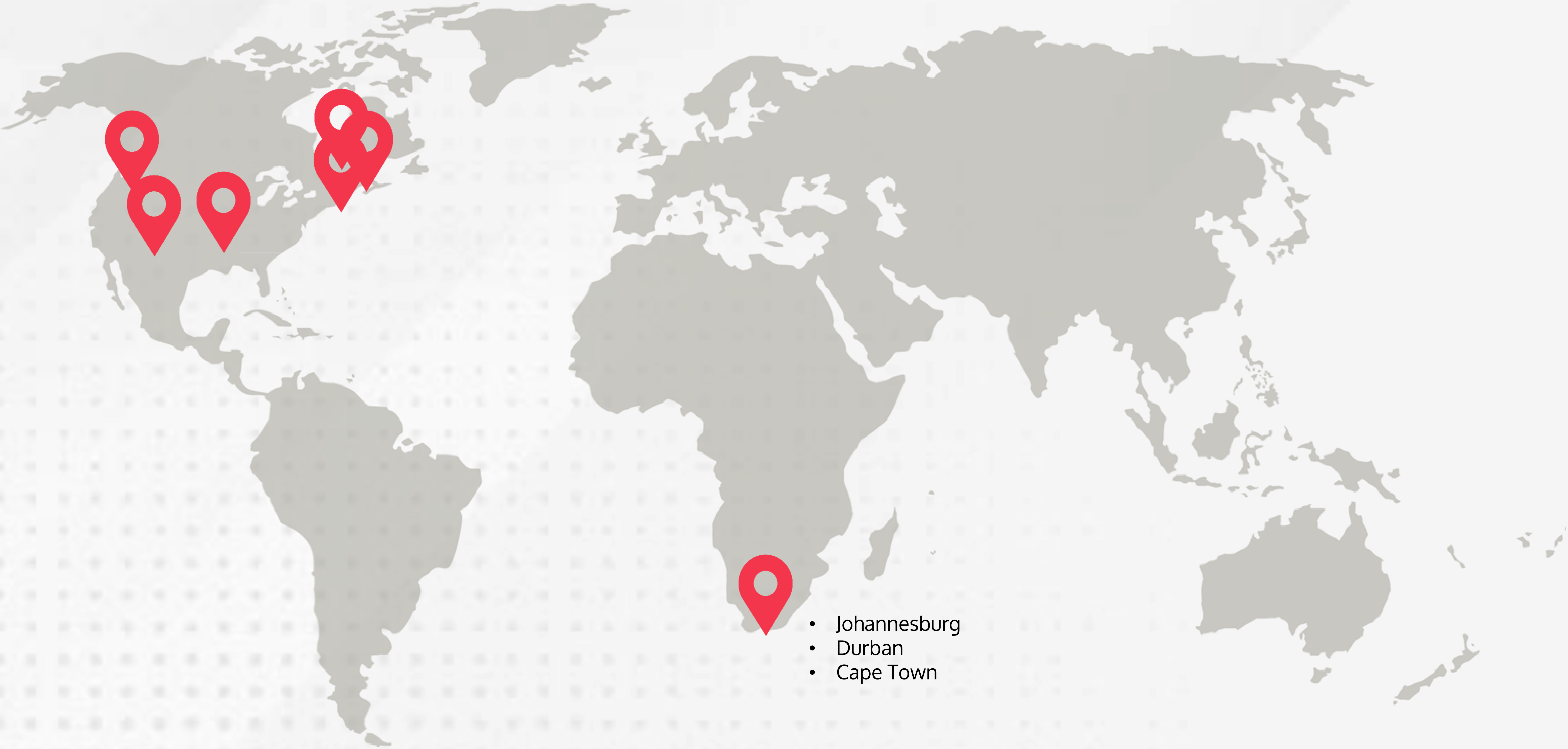
+450 elite
IT professionals worldwide

+600
clients in United States and South Africa

14 years
Global Top Managed Service Provider

INC 5000
fastest growing company

Netsurit – Where we are



- Johannesburg
- Durban
- Cape Town

Trusted by +600 satisfied global customers

peopleUSA

novo nordisk®

Adviceworx

AMARO FOODS

fuel

Komati FRUIT

GT's

MANGOS Outsourcing & Offshoring Partners

JETS.COM

Bidvest Automotive

CAPE TOWN HOLLOW BOUTIQUE HOTEL

DMS POWDERS

Universal Healthcare

WM PARTNERS LP

freshpet

VALUEWORKS

GALDERMA

Gordon Verhoef & Krause BUILDING & RENOVATION

KAIZER CHIEFS

lanham-love service::success::matters

MOSTERT OPPERMAN GOODBURN INCORPORATED

CANI

Standard Bank

isto BIOLOGICS

LEARNING sandbox

LIONS

LIBSTAR

Premier Fishing & Brands Limited The First Choice

fundamental

ALLANGRAY

REDTAIL CAPITAL MARKETS™

NESPRESSO

NEDBANK

Premier

Standard Bank

SafetySA

absa

RUSK RENOVATIONS INC

WestStar MORTGAGE CORPORATION

PRESIDENT Hotel

PWM PRIVATE WEALTH MANAGEMENT

R&H Rail (Pty) Ltd

THE HYDRO STELLENBOSCH

ALLANGRAY

NETSURIT

Microsoft Partnership

Microsoft Partner
Microsoft

Microsoft
Solutions Partner
Security

Microsoft
Solutions Partner
Modern Work

Microsoft
Solutions Partner
Infrastructure
Azure

Microsoft
Solutions Partner
Digital & App Innovation
Azure

Microsoft
Solutions Partner
Data & AI
Azure

Specializations
Microsoft Partner
Microsoft

Cloud Security
Threat Protection
Identity and Access Management
Information Protection and Governance
Endpoint Management
Infra and Database Migration

Microsoft Intelligent Security Association
Microsoft

Microsoft Verified
Managed XDR Solution

NETSURIT suite of solutions

NETSURIT
Managed Services (MSP)

Reliable and scalable IT infrastructure solutions, ensuring seamless operations and minimal downtime.

NETSURIT
Productivity Enablement

Unlock your company’s potential through workshops, custom training platforms, and strategic roadmaps designed to enhance efficiency and productivity.

NETSURIT
Professional Services

Tailored on-demand projects to drive digital transformation, enhance security, and modernize workplaces through specialized Microsoft implementations

NETSURIT
Secure

Advanced cybersecurity solutions to protect your digital assets, ensuring robust security and peace of mind.

NETSURIT
AI Enablement

Empower your business with AI and Machine Learning capabilities through specialized workshops, implementation roadmaps, and custom training platforms.

NEW

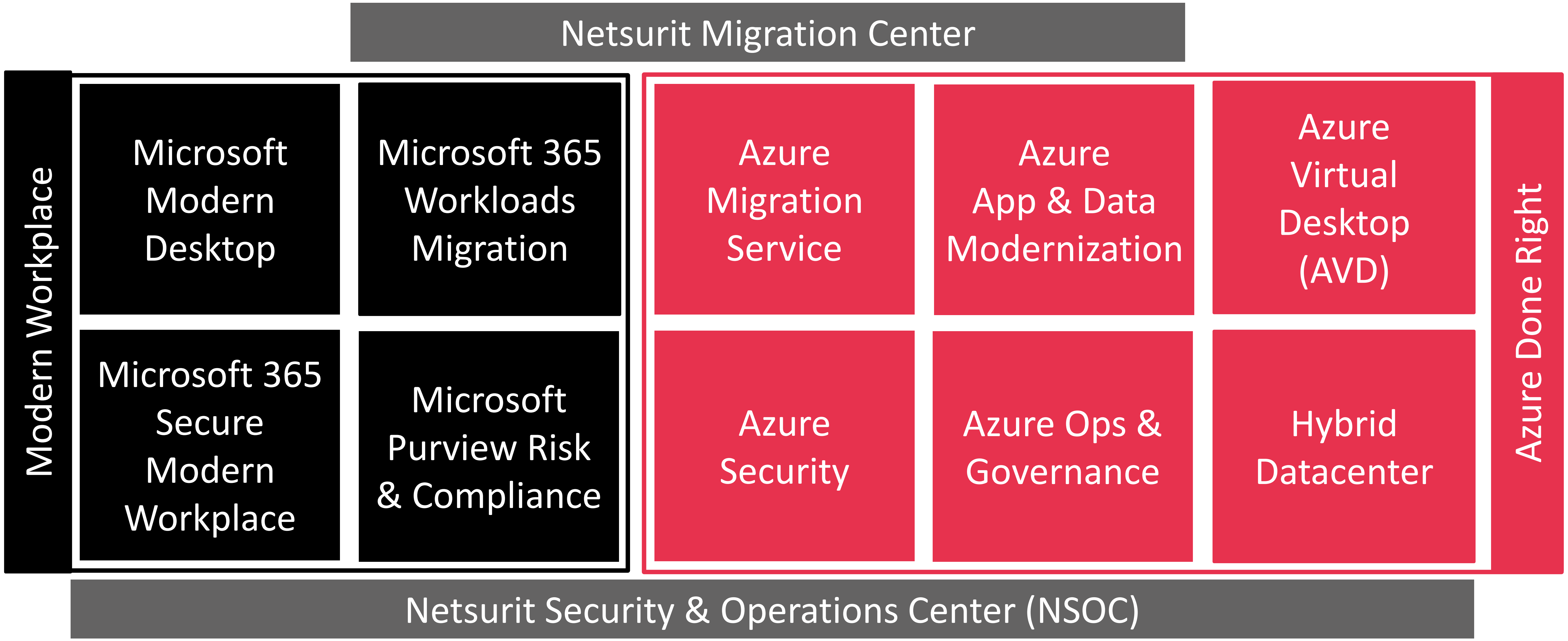
NETSURIT
InnovateX

Access to an Intelligence Office and corresponding capabilities for actionable insights and technology implementation, ensuring proactive support for growth and modernization.

NETSURIT

NETSURIT
Professional Services

Tailored on-demand projects to drive digital transformation, enhance security, and modernize workplaces through specialized Microsoft implementations



Netsurit Migration Center

Modern Workplace

- Microsoft Modern Desktop
- Microsoft 365 Workloads Migration
- Microsoft 365 Secure Modern Workplace
- Microsoft Purview Risk & Compliance

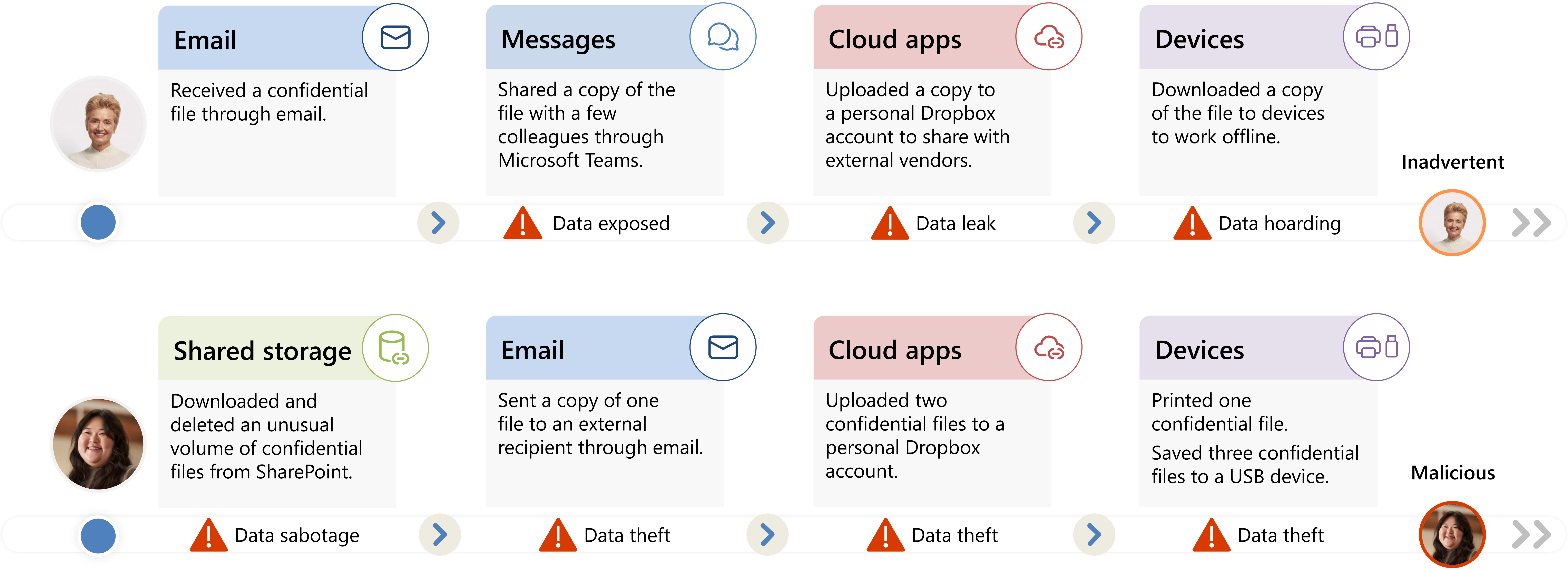
Azure Done Right

- Azure Migration Service
- Azure App & Data Modernization
- Azure Virtual Desktop (AVD)
- Azure Security
- Azure Ops & Governance
- Hybrid Datacenter

Netsurit Security & Operations Center (NSOC)

Data security incidents can happen anytime anywhere

Data doesn't move itself; people move data



Email

Received a confidential file through email.

Messages

Shared a copy of the file with a few colleagues through Microsoft Teams.

⚠ Data exposed

Cloud apps

Uploaded a copy to a personal Dropbox account to share with external vendors.

⚠ Data leak

Devices

Downloaded a copy of the file to devices to work offline.

⚠ Data hoarding

Inadvertent

Shared storage

Downloaded and deleted an unusual volume of confidential files from SharePoint.

⚠ Data sabotage

Email

Sent a copy of one file to an external recipient through email.

⚠ Data theft

Cloud apps

Uploaded two confidential files to a personal Dropbox account.

⚠ Data theft

Devices

Printed one confidential file.

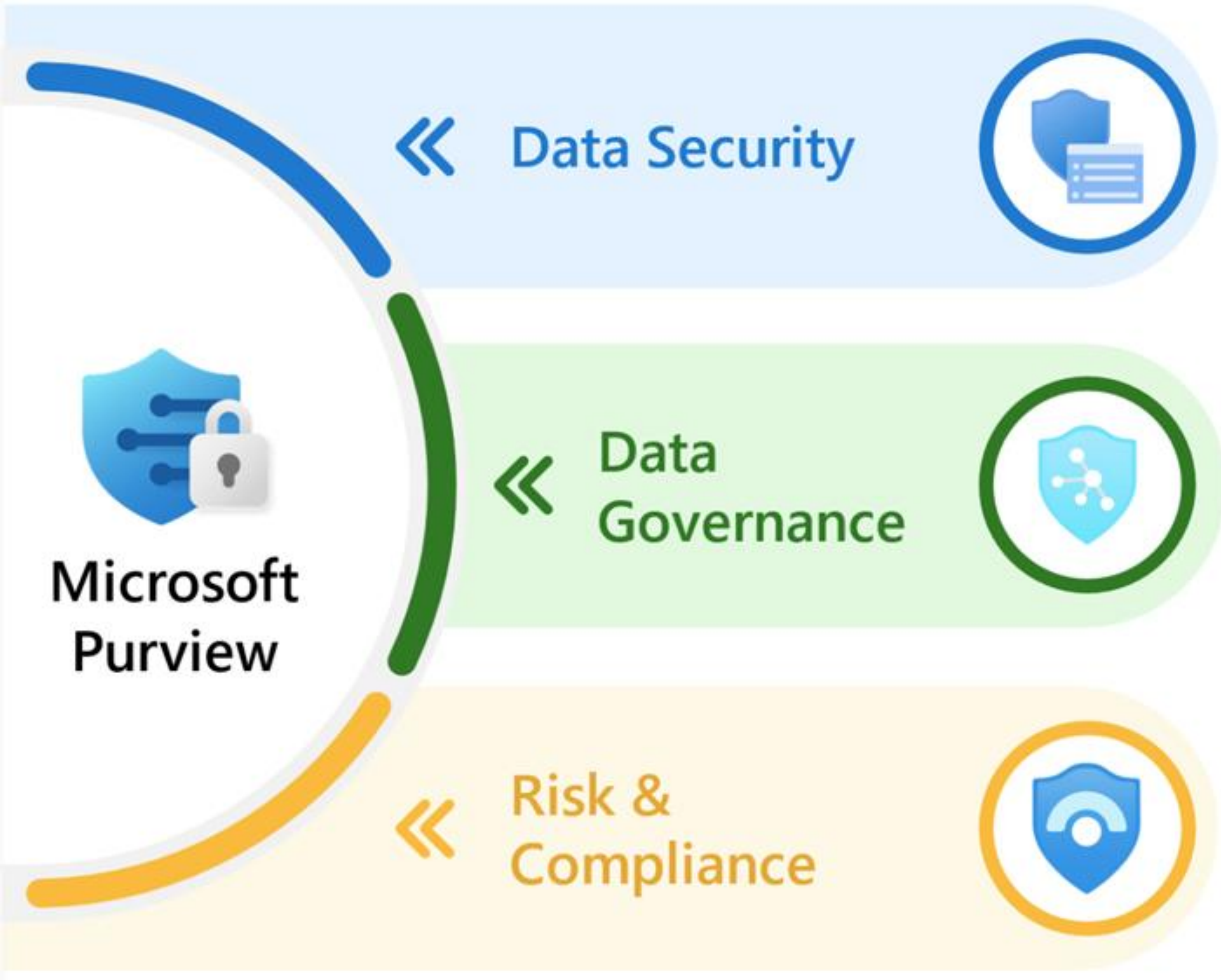
Saved three confidential files to a USB device.

⚠ Data theft

Malicious

NETSURIT

Microsoft Purview Solutions



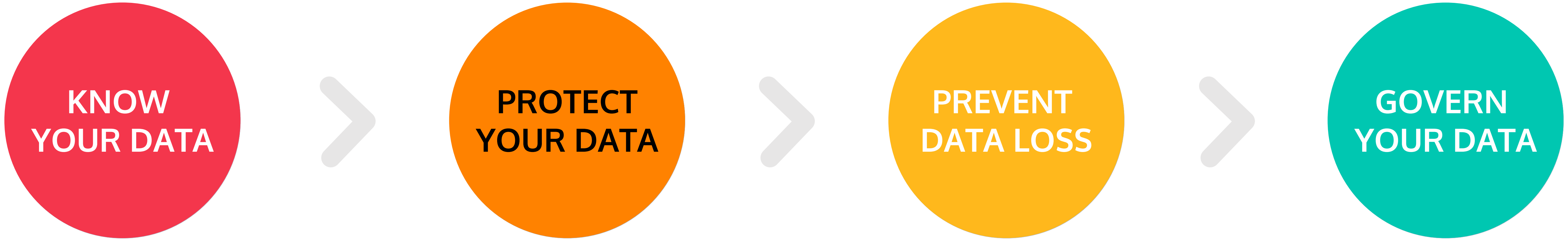
Microsoft Purview Data Loss Prevention
Microsoft Purview Information Barriers
Microsoft Purview Information Protection
Microsoft Purview Insider Risk Management

Microsoft Purview Data Catalog
Microsoft Purview Data Estate Insights
Microsoft Purview Data Map
Microsoft Purview Data Policy
Microsoft Purview Data Sharing

Microsoft Purview Audit
Microsoft Purview Communication Compliance
Microsoft Purview Compliance Manager
Microsoft Purview Data Lifecycle Management
Microsoft Purview eDiscovery

Microsoft Purview Information Protection & DLP

Protect and govern data wherever it lives



KNOW YOUR DATA: Understand your data landscape and identify important data across your hybrid environment

PROTECT YOUR DATA: Classify data with sensitivity labels, apply flexible protection, encryption, access restrictions and visual markings

PREVENT DATA LOSS: Prevent unauthorized or accidental sharing, transfer, or use of sensitive data with policies

GOVERN YOUR DATA: Automatically retain, delete, and store data and records in a compliant manner

POWERED BY AN INTELLIGENT PLATFORM
Unified approach to automatic data classification, policy management, analytics, and APIs

Devices

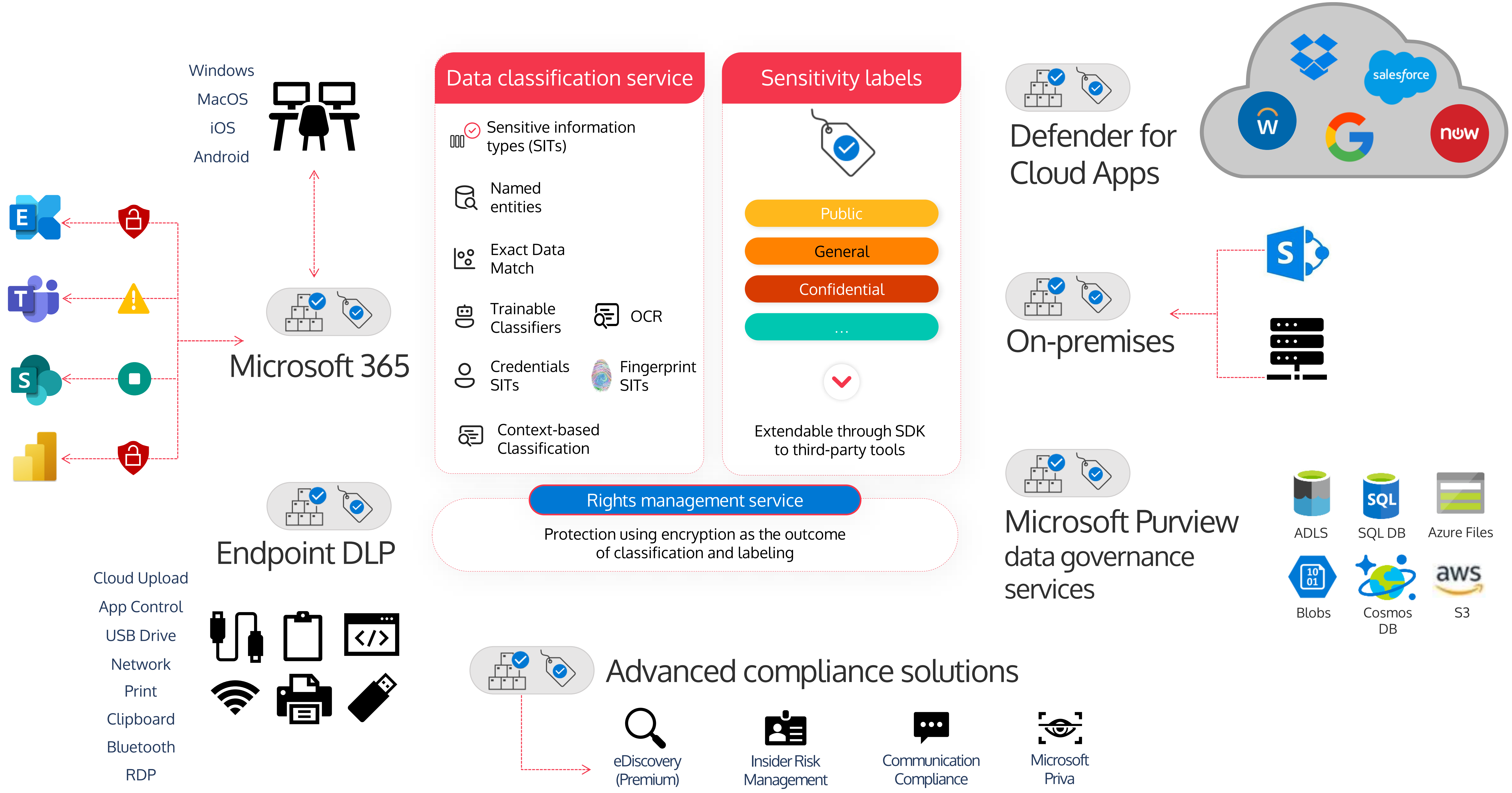
Apps

Cloud services

On-premises

ISV/3rd party

Microsoft Purview Information Protection & DLP



Windows
MacOS
iOS
Android

Microsoft 365

Endpoint DLP

Cloud Upload
App Control
USB Drive
Network
Print
Clipboard
Bluetooth
RDP

Data classification service

- Sensitive information types (SITs)
- Named entities
- Exact Data Match
- Trainable Classifiers
- OCR
- Credentials SITs
- Fingerprint SITs
- Context-based Classification

Sensitivity labels

- Public
- General
- Confidential
- ...

Extendable through SDK to third-party tools

Rights management service

Protection using encryption as the outcome of classification and labeling

Defender for Cloud Apps

On-premises

Microsoft Purview data governance services

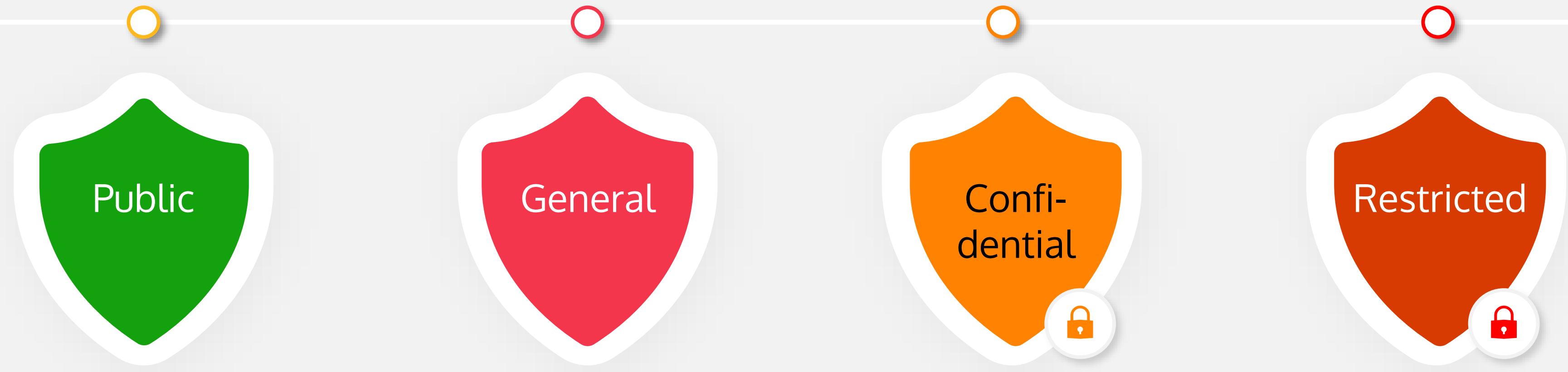
Advanced compliance solutions

- eDiscovery (Premium)
- Insider Risk Management
- Communication Compliance
- Microsoft Priva

NETSURIT

Sensitivity labels

- Span your entire data estate
- They are a representation of your information taxonomy.
- They describe the priority assigned to your categories of sensitive information.



Content labels

Applied To: Office apps, Power BI reports, Azure Data

Protections: Encryption and visual markings

Automation: Can be applied either manually by users or automatically based on classification

Container labels

Applied To: SharePoint sites, Teams channels, Microsoft 365 groups

Protections: Access control, privacy settings, conditional access

Automation: Can be applied manually by site/Team or group owners

Powerful controls that ensure labels are applied where needed

Apply labels by default, make them mandatory, prevent label downgrades

NETSURIT

Purview classification technologies

Sensitive info types

Over 200 out-of-the-box information types like Social Security and credit card numbers

Clone, edit, or create your own

Supports regular expressions (regex), keywords, and dictionaries

AVAILABLE TODAY

Named entities

Over 50 entities covering person name, medical terms, and drug names

Best used in combination with other sensitive information types

AVAILABLE TODAY

Exact data match

Provides a lookup to exactly match content with unique customer data

Supports 100 million rows and multiple lookup fields

AVAILABLE TODAY

OCR

Expanded OCR for Exchange Online, SharePoint Online, OneDrive for Business, Teams, and endpoint devices

Supports over 150 languages

Supports image files and images embedded in PDFs

AVAILABLE TODAY

Trainable classifiers

Over 35 pre-trained ready-to-use trainable classifiers

Create your own classifier based on business data

AVAILABLE TODAY

Credentials SITs

42 new SITs for digital authentication credential types

Use in auto-labeling and DLP policies to detect sensitive credentials in files

AVAILABLE TODAY

Fingerprint SITs

Detect exact or partial matching of sensitive intellectual property

Use in Exchange Online, SharePoint Online, Microsoft Teams, and devices

Note: Available in Purview DLP

AVAILABLE TODAY

Context-based classification

SharePoint and OneDrive default site label

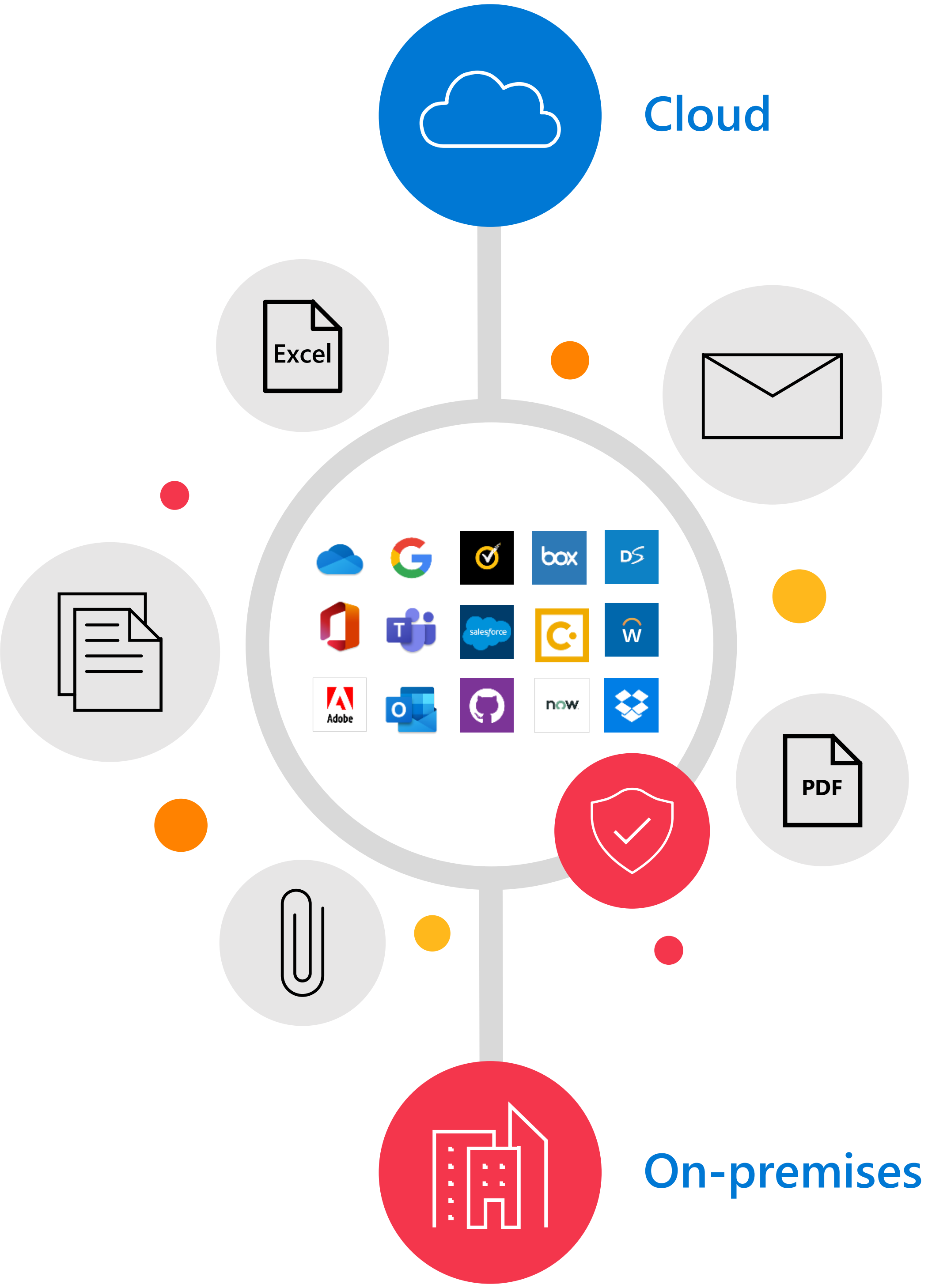
Service-side auto-labeling

- File extension
- Document name contains word
- Document property is
- Document size greater than
- Document created by

ROADMAP ITEM

Microsoft Purview Information Protection

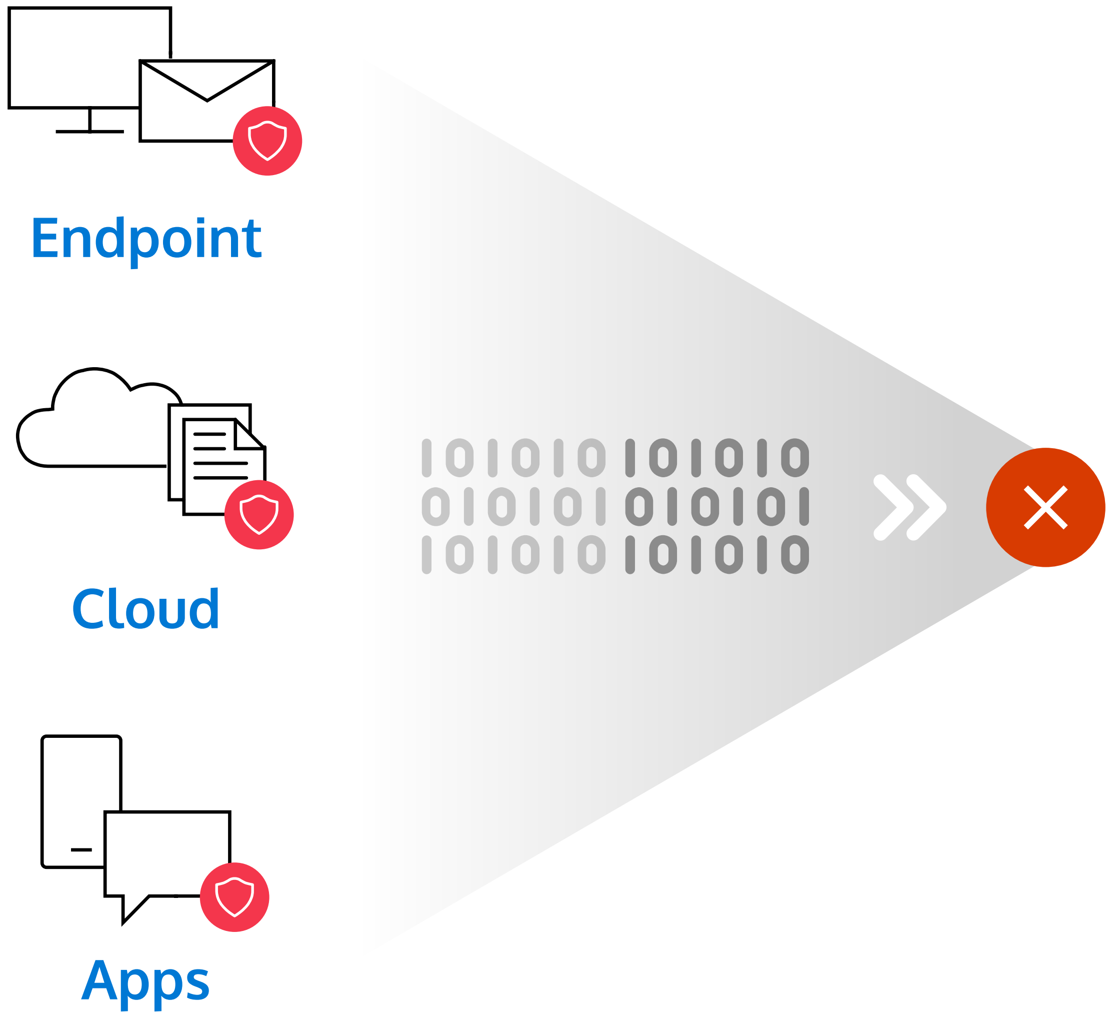
An intelligent, built-in, and extensible solution to know and protect sensitive data



- → Discover and classify data at scale using automation and machine learning
- → Built-in labeling and protection
- → Platform extends the protection experience
- → Encryption built into Microsoft 365: at rest, in transit, and in use
- → Labels define WHO has access to the content and HOW they can use with the content

Microsoft Purview Data Loss Prevention

Prevent accidental or unauthorized sharing of sensitive data



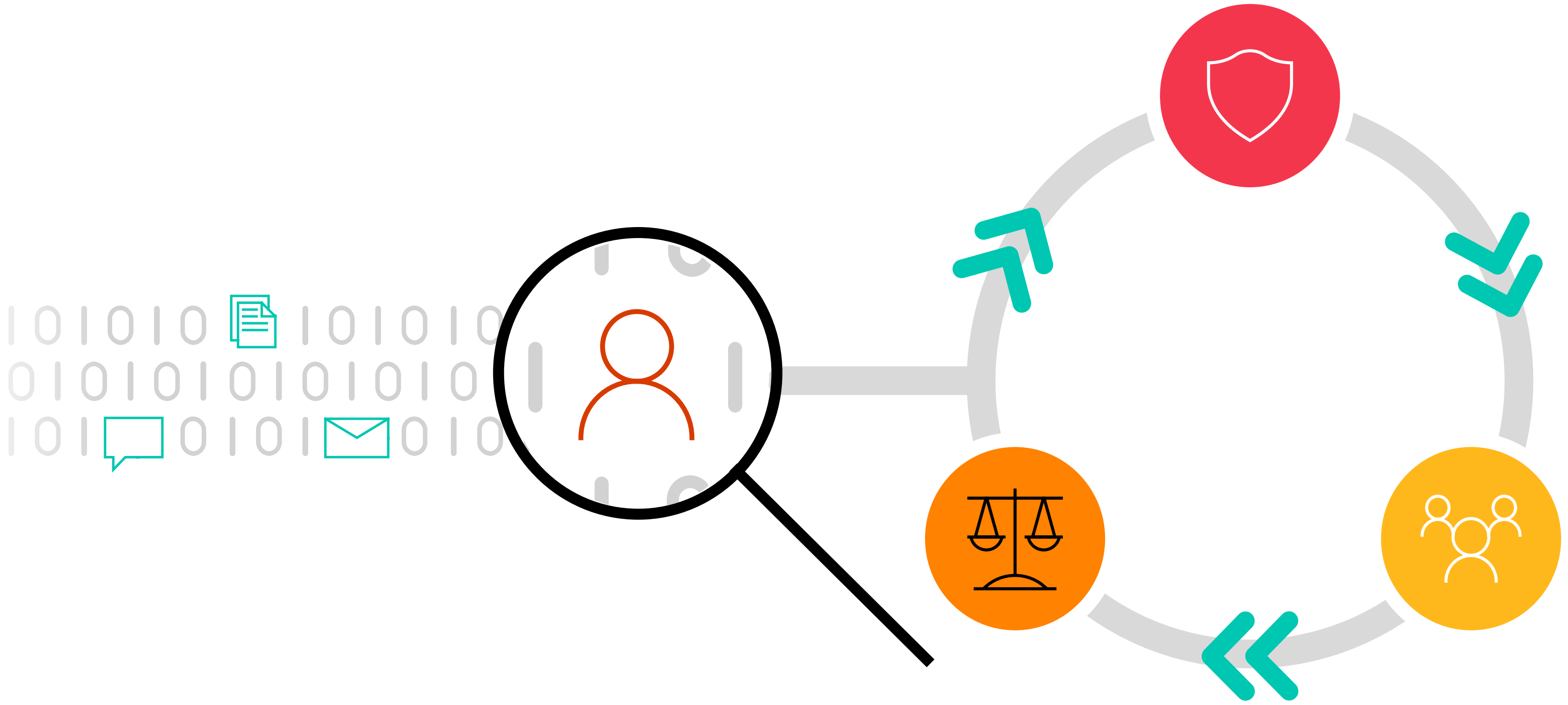
- Automatically enforce compliance with regulations and internal policies across cloud and on-premises
- Extend DLP policy to both Microsoft and non-Microsoft endpoints, on premises file shares, user apps, browsers, and services
- Apply flexible policy administration to balance user productivity

NETSURIT

Microsoft Purview Insider Risk Management

Identify and act on insider risks with an integrated end-to-end approach

- Identify risky activity and hidden risks with customizable templates and contextual insights
- Maintain user privacy with built-in controls that keep user data anonymous
- Enable collaboration across security, HR, and legal with integrated investigation workflows

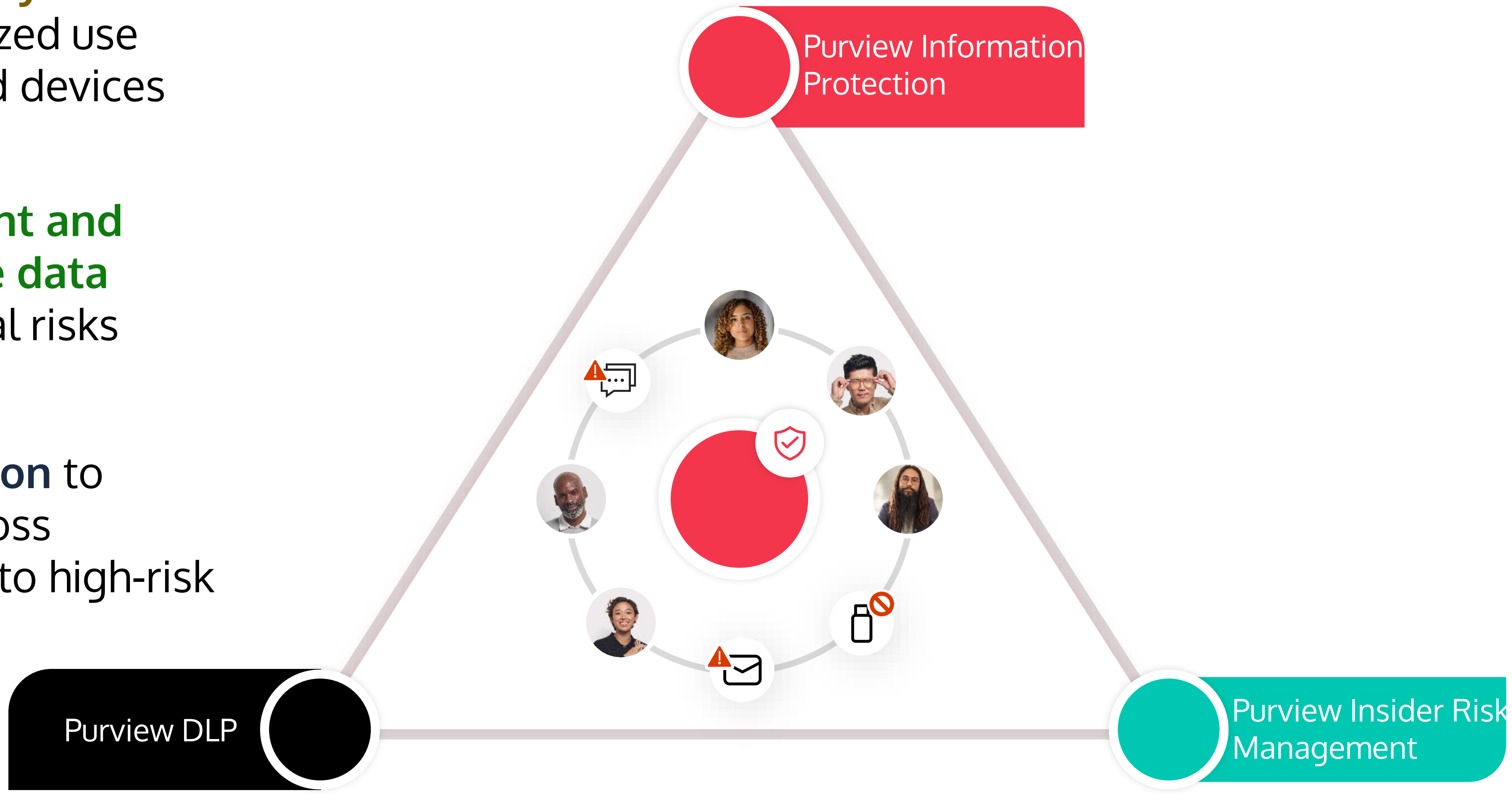


Fortify data security with an integrated approach

Discover and auto-classify data and prevent it from unauthorized use across apps, services, and devices

Understand the **user intent and context around sensitive data** to identify the most critical risks

Enable **Adaptive Protection** to assign appropriate data loss prevention (DLP) policies to high-risk users


Purview Information Protection
Purview DLP
Purview Insider Risk Management

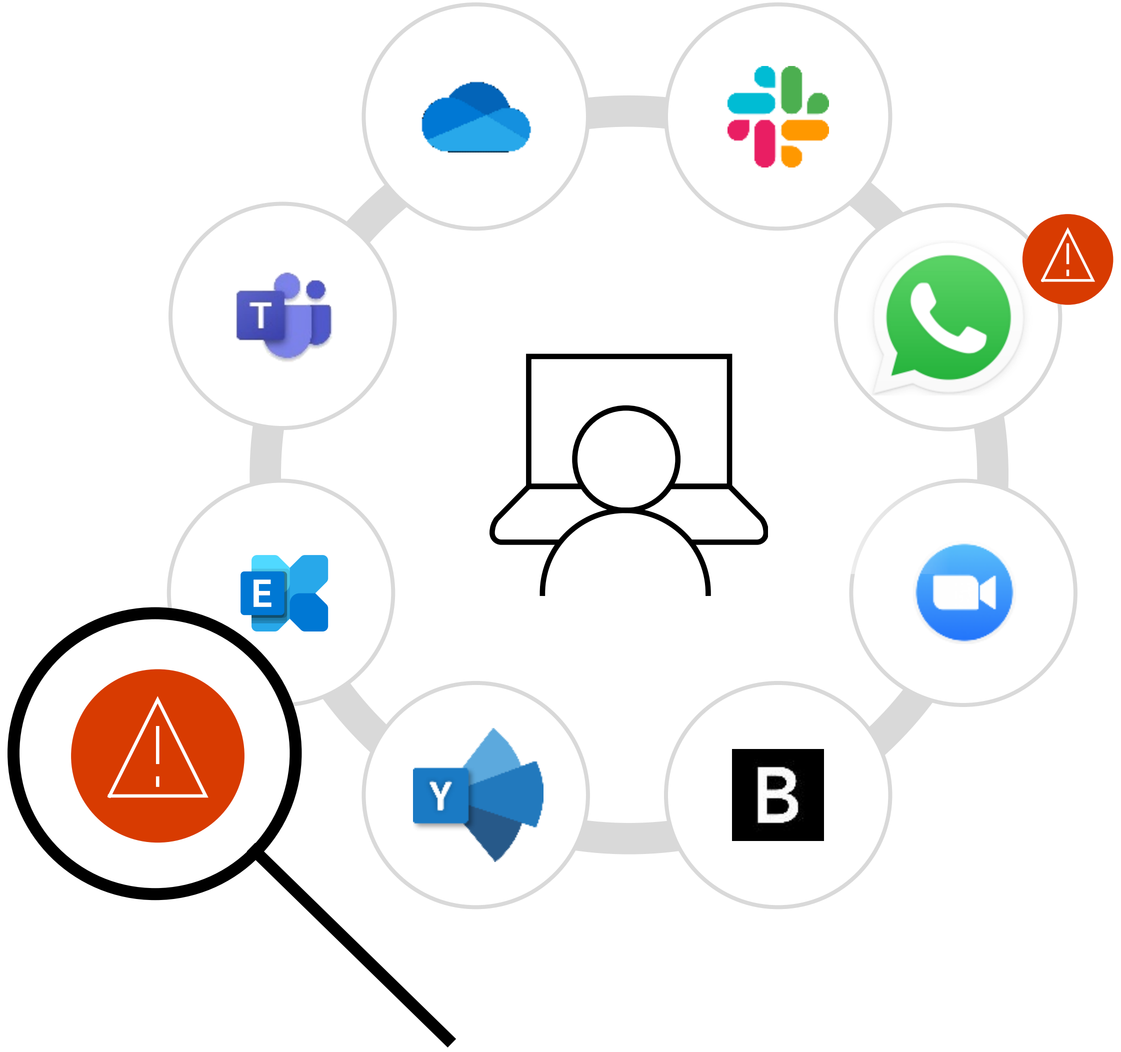
Support for multi-cloud, hybrid, and software-as-a-service (SaaS) data | Partner ecosystem

NETSURIT

Microsoft Purview Communication Compliance

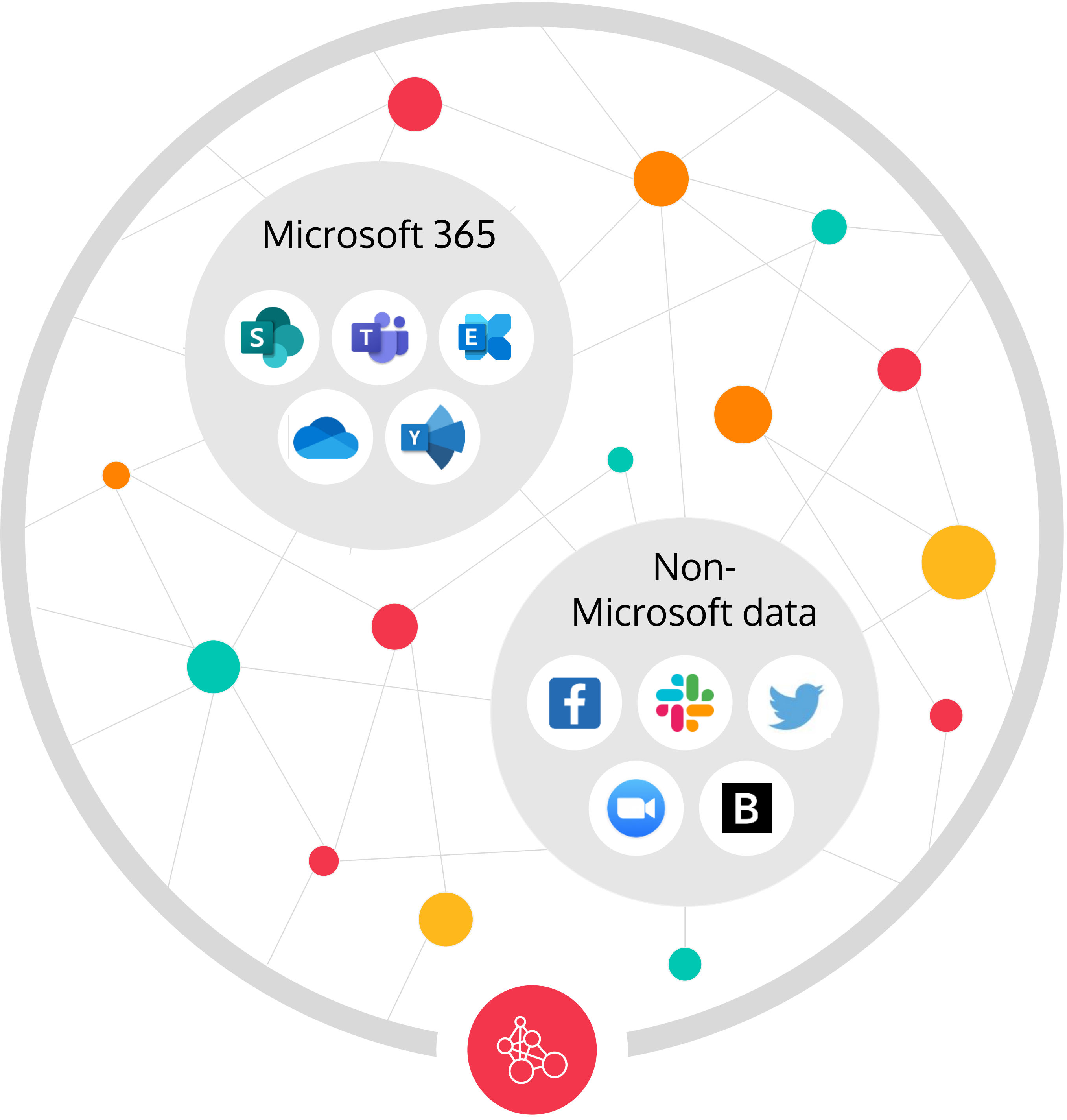
Quickly identify and act on code-of-conduct policy violations

- Intelligent customizable playbooks detect violations across Teams, Exchange, and third-party content
- Flexible remediation workflows enable quick action on violations, like remove incriminating messages on Teams
- Identify and investigate communications risks while maintaining end-user privacy



Microsoft Purview Data Lifecycle Management

Classify and govern data at scale



Powered by an intelligent platform

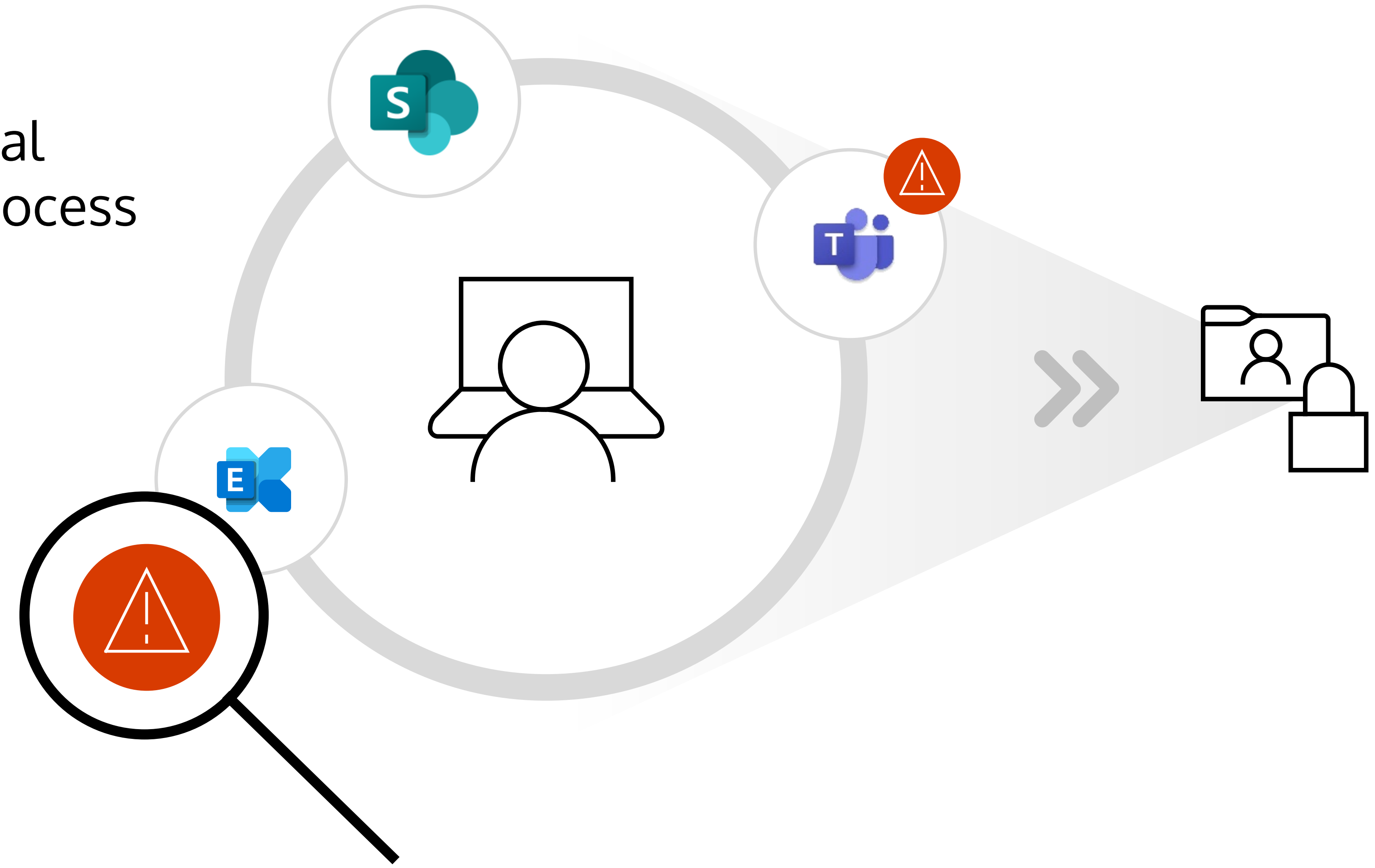
- Retain or delete data and manage records where users collaborate to manage risk and prevent productivity loss
- Demonstrate compliance with label analytics insights, defensible disposal, and rich audit trails
- Manage non-Microsoft data import with pre-built data connectors*

*Pre-built data connectors include connectors built by Microsoft and by partners – Veritas, Telemessage, CellTrust and 17a-4 LLC. Except for Veritas, Telemessage, CellTrust and 17a-4 LLC, Microsoft does not have direct relationships with the data source companies in bringing these data connectors to the platform.

Microsoft Purview eDiscovery

Discover, preserve, collect, process, cull, and analyze your data in place

- Preserve content by custodian, send hold notifications, and track acknowledgements
- Review and manage static sets of documents within a case, that can be independently searched, analyzed, shared, and acted upon
- Near duplicate detection, email threading, themes, and ML models to identify potential high value content and make the review process more efficient

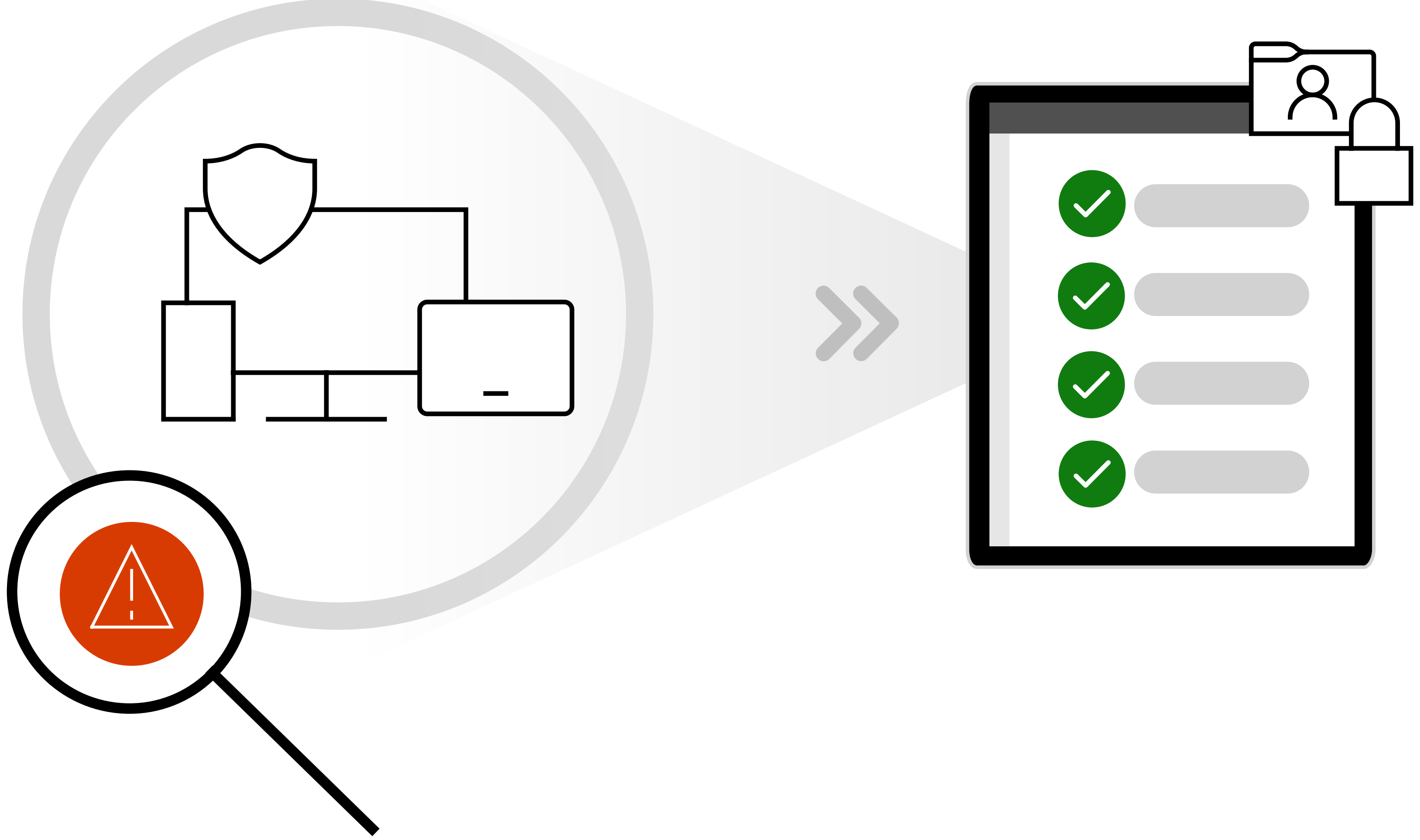


NETSURIT

Microsoft Purview Audit

Power your forensic and compliance investigations

- Tap into additional events that are important for forensic investigations (e.g. mail items accessed, mail send, user search)
- Preserve audit logs for up to a year, with option for 10-year retention add-on
- High bandwidth access to data with ~2x the baseline



NETSURIT

Purview reference customers

NEDBANK

absa

FNB

Standard Bank

ENS africa | Africa's largest law firm

aurex

Constructors

PWM PRIVATE WEALTH MANAGEMENT

datasciences corporation

enX GROUP

Adviceworx

Professional Financial Advice

Premier

VAT IT

Microsoft Purview implementation phases

Phase
Phase 1 - Assessment and planning
Phase 2 - Core DLP implementation
Phase 3 - Core information protection implementation
Phase 4 - Core Insider Risk Management implementation
Phase 5 - Expanded DLP & information protection implementation
Phase 6 - Expanded Purview Data Management implementation
Phase 7 - Core Communications Compliance & Information Barriers implementation
Phase 8 - Expanded Insider Risk Management implementation
Phase 9 - Expanded Communications Compliance & Information Barriers implementation
Ongoing Operations - Ongoing operations and solution expansion

Microsoft Purview implementation phases

Phase	Focus/objectives
Phase 1 Assessment and planning	Initial requirements analysis. Initial sensitive information discovery. Identify initial data classification requirements.
Phase 2 Core DLP solution implementation	Initial implementation of core Microsoft Purview Data Loss Prevention (DLP) functionality. This will include DLP policy enforcement for transactions on Office 365 services, on-premises file servers, Windows 10/11 client computers and web service connections. Develop initial data classification taxonomy. Implement initial solutions for selected high priority use cases in the business. Perform initial compliance training for compliance officer and other stakeholders. Create and document DLP policies, processes, and procedures.
Phase 3 Core information protection implementation	Initial implementation of core Microsoft Purview information protection and governance functionality, including Microsoft Information Protection (MIP), Data Lifecycle Protection and eDiscovery. Implement initial solutions for selected high priority use cases in the business. Perform initial compliance training for compliance officer and other stakeholders. Create and document information protection policies, processes, and procedures.
Phase 4 Core Insider Risk management implementation	Implement core Insider Risk Management Functionality including Data Security Posture Management (DSPM) for AI.

Microsoft Purview implementation phases

Phase	Focus/objectives
Phase 5 Expanded DLP & information protection implementation	Expand the solution to more parts of the business. Expanded requirements analysis. Additional sensitive information discovery. Expand the data classification taxonomy. Expand the implementation of core Microsoft Purview compliance functionality, including Data Loss Prevention (DLP), Microsoft Information Protection (MIP), Data Lifecycle Protection, eDiscovery. Implement information protection solutions for additional use cases in the business. Perform additional compliance training for compliance officer and other stakeholders. Create and document additional compliance policies, processes and procedures. Expand operational processes for compliance management.
Phase 6 Expanded Purview Data Management implementation	Implement granular data lifecycle management using retention labels and retention label policies to accommodate advanced requirements. Expand audit log retention Implement comprehensive eDiscovery processes for forensic investigations.
Phase 7 Core Communications Compliance & Information Barriers implementation	Implement core Communications Compliance & Information Barriers Functionality.

Microsoft Purview implementation phases

Phase	Focus/objectives
Phase 8 Expanded Insider Risk Management implementation	Implement additional Insider Risk Management Functionality including Data Security Posture Management (DSPM) for AI.
Phase 9 Expanded Communications Compliance & Information Barriers implementation	Implement additional Communications Compliance & Information Barriers functionality.
Ongoing Compliance Operations	Ongoing operations and solution expansion.

Ongoing compliance operations

1. Periodic compliance reviews (using Compliance Manager).
2. Updating classifications of sensitive information.
3. Updating data labels.
4. Updating Purview Information Protection configuration, labels, policies, and templates.
5. Updating DLP sensitive information classifications and rules.
6. Configuring rights protected libraries in SharePoint Online.
7. Updating transport rules in Exchange Online.
8. Reviewing and updating permission assignments and roles in Office 365 services.
9. Reviewing and updating sharing configuration in Office 365 services.
10. Periodically scanning cloud and on-premises repositories for unclassified sensitive information.
11. Review and update retention settings and policies.
12. Perform content searches and investigations using eDiscovery.
13. Respond to audit events and alerts.
14. Monitor in scope systems to detect potential compliance violations.
15. Investigate and respond to potential compliance violations.
16. Respond to formal Data Subject Requests (DSR).
17. Monthly report
    - Summary of compliance operations performed by Netsurit team for the month.
    - State of Purview compliance, based on Compliance Manager, including Compliance Secure Score.
    - Digest of Purview operational reports for the month.
    - Summary of risks and issues identified.
    - Recommendations for future changes.

Case Study

ENSafrica | Africa's largest law firm

- Select a case study and describe the scenario.
- Explain the situation assessment process.
- Explain the threat analysis conducted by the team.
- Outline the solution architecture developed.
- Discuss the progress of the implementation.

ENSafrica Case Study

ENSafrica | Africa's largest law firm

- Biggest Law firm in Africa
- 1250 active employees
- “All documents are sensitive”
- Legal Regulations
- Comply with South Africa POPIA regulation
- At the start had M365 E3 plus E5 Security add-on licenses

Situation Assessment

- Gain visibility into hidden data security risks in the Microsoft 365 Cloud environment in use by the customer.
- Enable the Automated Discovery service to search for:
  - Data that contains one or more sensitive information types
  - Stale data
  - Suspicious and unusual activities
- Help the customer understand how Microsoft Purview products and services can help mitigate and protect against the data security risks that were identified over the course of the engagement.
- Enable Microsoft 365 services used by the Data Security Check Automated Discovery process:
  - Content Search
  - Data Loss Prevention
  - Insider Risk Management
  - Microsoft Purview Information Protection
  - Audit

NETSURIT

Threat Analysis

- Identify all hidden data risks
- Identify the know your data within environment
- Identify threat actors

Solution Architecture

- Purchase and assign M365 E5 Compliance Add-on (Later Full M365 E5)
- Assist client to build Document taxonomy
- Use Out-Of-Box and Custom classifiers to identify the sensitive information
- Use Data Loss Prevention with defined processes
- Use information protection
  - Manual Process – For applying User Assigned Permissions
  - Automatic – Data at rest and while working on documents
- Insider Risk Management
- Compliance Manager
  - Process to implement improvement Actions
- Configure Retention Labels and Policies