A decorative graphic in the bottom left corner consisting of several overlapping geometric shapes in shades of blue, orange, and yellow.

NTT DATA, Data Classification and Protection Services for Microsoft Information Protection

June 2021

The Challenges with Data

The acceleration of the digital transformation has led to increase in volume of data generated

2.5

Quintillion bytes of data created everyday

163

Zettabytes of data to be stored by 2025

450B

Business transactions to happen every day by 2020

4B

Humans use internet with CAGR of 16.5%

Leading companies around the world are facing tough challenges with their data

Difficulty in implementing policy-based data protection



High investment in manpower to detect and respond to data breaches



Increased compliance requirements for data privacy



High dependence on manual processes for locating sensitive data



90% of corporate data is in office documents but there is an inability to protect that data easily

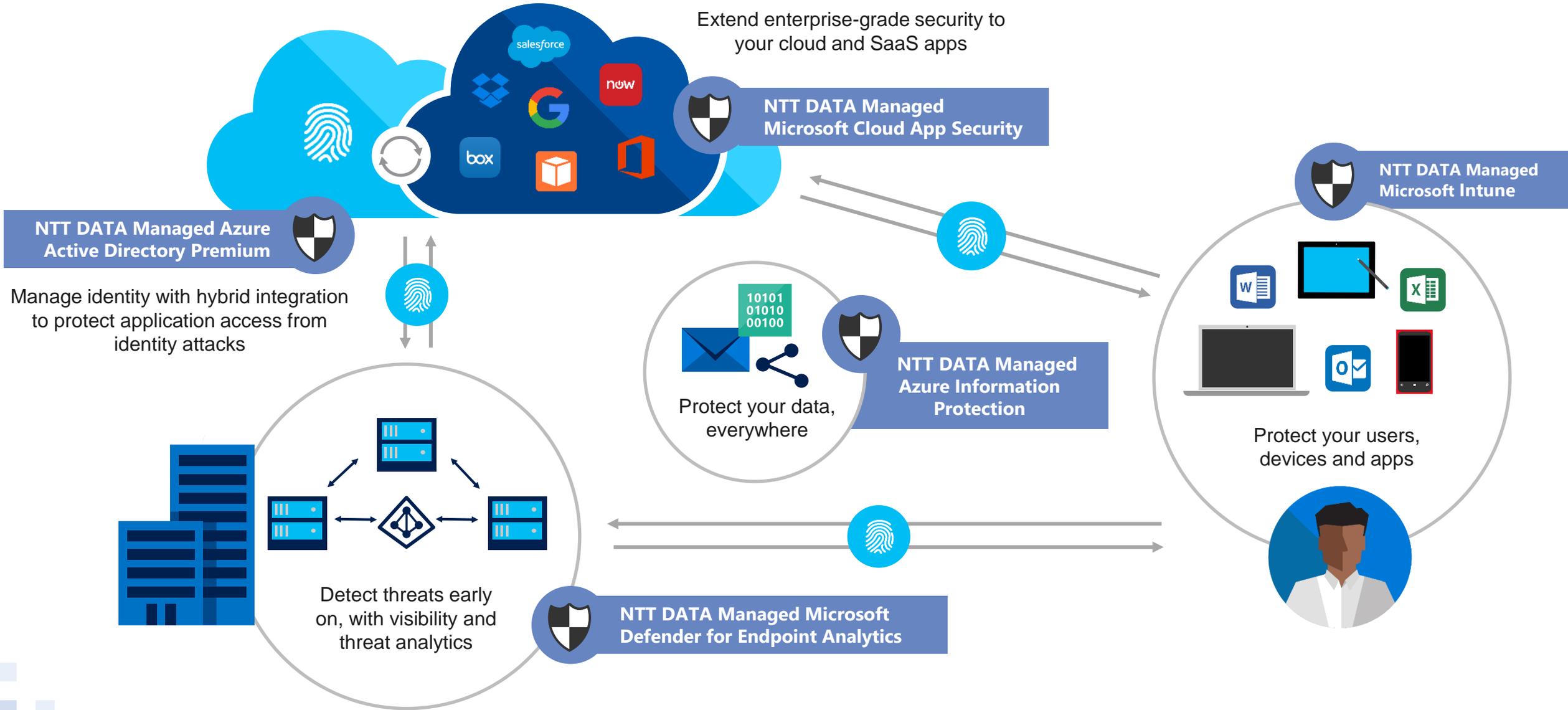


Inefficient document classification and overall labelling structure



It is imperative for all companies to invest in an improved data architecture and formulate a data security strategy

We deliver industry-best data governance solutions



Protect Your Data Across Different Environments



On-Premise

Classify and label data in on-prem repositories, including file servers and SharePoint



Office Apps Across Platforms

Label and protect Microsoft Office files natively across Windows, Mac, iOS, Android and Web Clients



SharePoint, Teams, Groups, PowerBI

Label and protect sensitive data manually and automatically across content and container



Exchange Online

Automatically label and protect sensitive emails in Exchange Online



Non-Microsoft Clouds and SaaS apps

Extend protection through Microsoft Cloud App Security to third party clouds and SaaS apps

Unified Label Management in Microsoft 365 Compliance center

Protect Your Data Using Sensitivity Labels

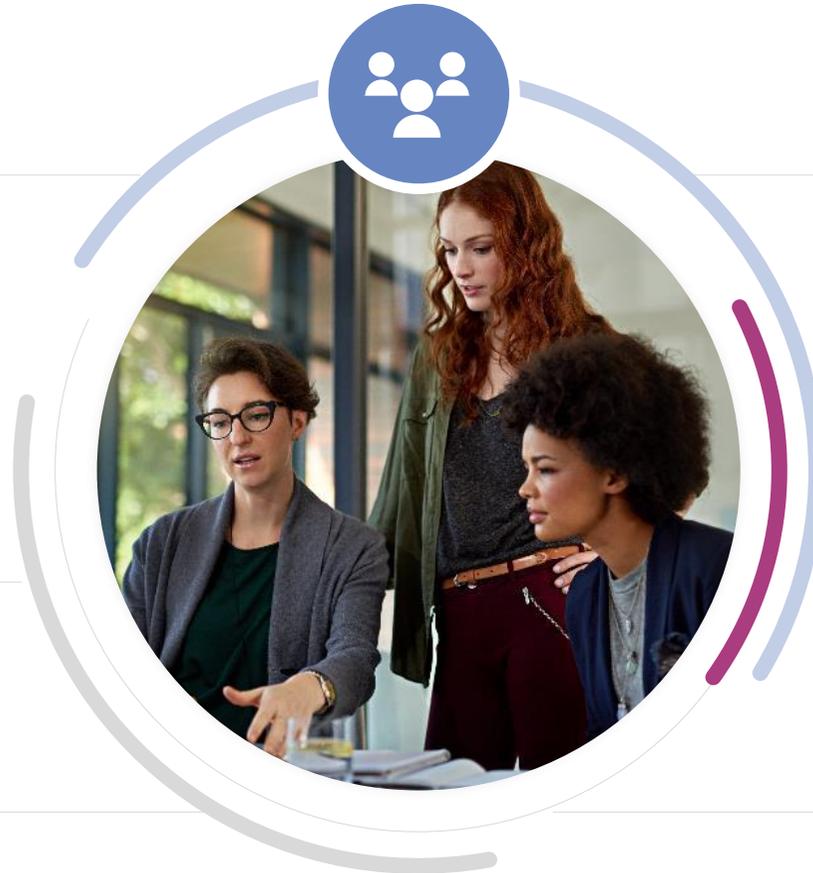
✔ Customizable

✔ Persist as container metadata or file metadata

✔ Readable by other systems

✔ Determine DLP policy based on labels

✔ Extensible to partner solutions



Manual or Automated Labels ✔

Apply to content or containers ✔

Label data at rest, data in use, or data in transit ✔

Enable protection actions based on labels ✔

Seamless end-user experience across productivity applications ✔

Defense in Depth – Securing your Data, Apps & Users

The challenge



Bad actors are using increasingly creative and sophisticated attacks



The digital estate offers a very broad surface area that is difficult to secure



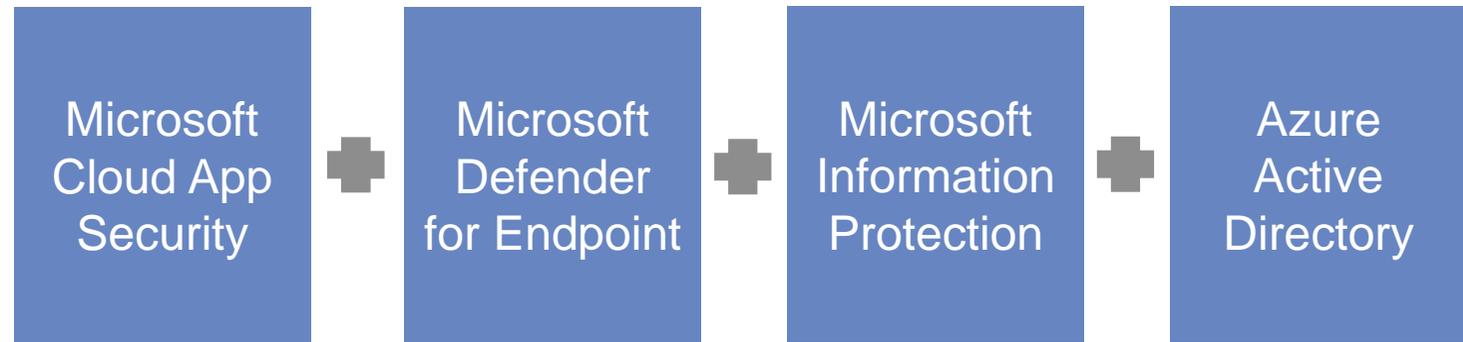
Data and users no longer reside behind your firewalls



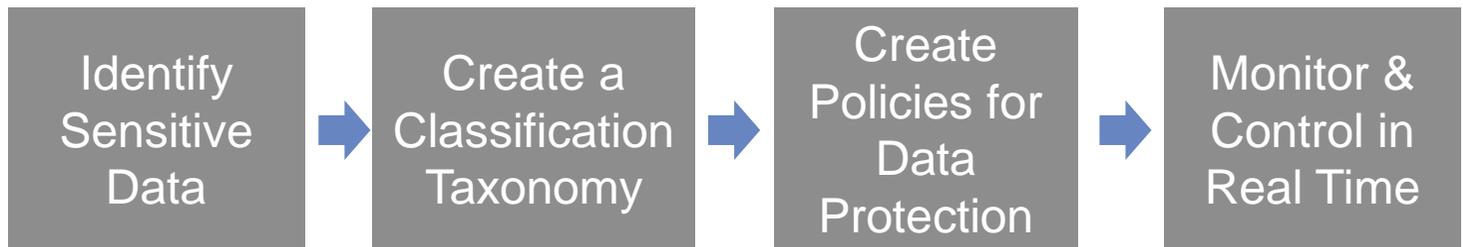
Intelligent co-relation of signals is difficult, time-consuming, and expensive

The solution

Better together – Microsoft Enterprise Mobility + Security products to protect your organization from threats



A strategic approach targeted to optimize your data security posture



A pragmatic and phased deployment will allow for the refinement of controls and best practices in a mindful manner

NTT DATA MIP Advisory Engagement Overview

Zero Trust Assessment

- Conduct a zero-trust assessment, and review high-level environment architecture and security solutions currently in place
- Discuss business concerns and requirements
- **Output** - a zero trust evaluation report and top-line objectives, concerns and requirements

Introduction to MIP

- Review MIP features and functionalities and how they can be used to protect data structures of your cloud environment
- Discuss how MIP capabilities can address your concerns and specific goals to accomplish
- **Output** – prioritized list of MIP objectives

Protect Your Information

- Identify parameters, policies, and integration points to meet your data protection objectives
- Discuss your data classification strategy and labeling taxonomy
- **Output** - defined policies that meet your data protection requirements and what actions will be taken should a policy be violated.

Integration with Apps & Tools

- Explore integration of MIP with other security tools to detect and prevent information loss
- Discuss how the labeling structure further prevents information loss against other critical apps
- **Output** - defined policies that meet your goals, as well as what actions will be taken for remediation

Monitoring & Controls

- Determine what actions should be taken to enable controls (i.e., preventing labeling misuse, document and file monitoring, etc.)
- Outline information protection policies for in-scope apps
- **Output** - defined policies that meet your goals, as well as what actions will be taken for remediation

Implementation (POC)

- Deliver a 3-5-day engagement for a high-level proof of concept to evaluate if MIP meets your business objectives
- Discuss preferred approach for enabling MIP controls to minimize production impact
- **Output** – the scope of work, and high-level requirements identification for MIP implementation

Controls Enablement

- Discuss the test plan process for enabling label/policy control across the environment and determine the preferred integration approach so that productivity is not disrupted
- **Output** – high-level implementation plan, targeted in scope apps, agreed-upon testing plan, deployment schedule and policies for MIP integration

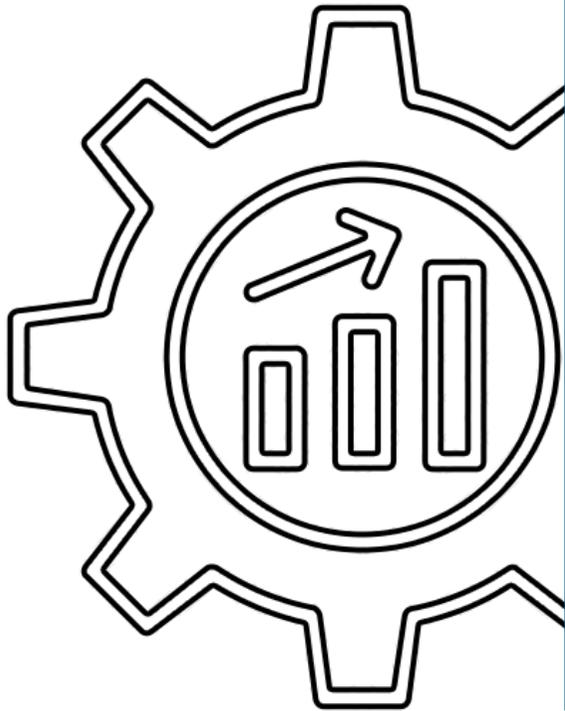
Architectural Vision

- Summarize all gathered intel & established parameters, configuration details and data
- **Output** – a collection of artifacts including architectural diagram, design guide, final implementation plan, and configuration set utilizing industry best practices

Overview of the Implementation Phase

Pilot

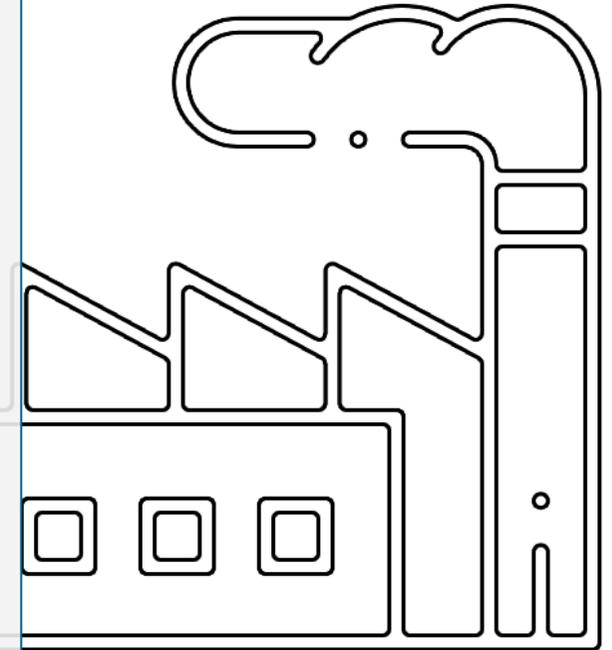
Apps are assessed to identify shadow IT and identify their risk levels



- Identify and discover sensitive data and implement policies for information protection
- Set up sensitive data types, policies and labels
- Deploy Microsoft Rights Management (RMS) and other connectors for information rights management of on-premise servers
- Roll out client-to-pilot group for proof-of-concept validation
- Collect feedback from pilot and refine classification taxonomy, sensitive data definitions and policies

Broad Rollout

Data protection is enabled to safeguard sensitive information



- Protect your information – Data classification and integration with Microsoft Teams, Office 365 and MCAS
- Detect & prevent threats – Anomaly and policy violation detection to identify and mitigate information loss
- Enable controls – Fine-tune policies and configurations that was set in earlier phases and enable policy automation
- Establish the process for periodic report delivery

Controls Enablement

Assess usage and performance patterns from the captured alerts established during the preceding phases to validate the controls meet the objectives. Configure governance controls based on required modifications as indicated during the testing process.

NTT DATA MIP Managed Services

Operational Support

Monitor alerts and provide escalation to mitigate risk exposure and ensure MIP is operating efficiently

- Monitor for abuse of defined policies as supported by MIP
- Investigate questionable usage, review and analyze data exposure, and review activity log of high-severity incidents
- Apprise audit trails of high-severity incidents and develop a proactive policy to prevent recurrence
- **Annual Platform review** may include activation of new features to be included in the service and discussion on the service alignment

For more active issues and responses, NTT DATA will support the following activities upon request, up to ten supported requests per month:

- Manage scanning parameters (MIP tool process) to:
 - Determine included or excluded file types
 - Inspect and label files
 - Identify and label files that can't be inspected

Optimization Support

Enable continual improvement efforts to enhance security posture

On a monthly basis:

- Remove and update policies at a rate of two policies per app
- Eliminate and manage labels and sub-labels. Manage the associated ownership tasks inline with the policy update process
- Assess the usage patterns and risk levels, determine points of concern and present findings for updates
- **Annual Platform review** may include activation of new features to be included in the service and discussion on the service alignment with the organizational business goals
- Identify automation opportunities, as supported by MIP, to reduce manual intervention based on the identified patterns every quarter

Audit Support

Support client-approved audit preparations for compliance or security program-related efforts

Audit assistance on a biannual basis to include:

- Deliver protection usage logs to support GRC requirements and additional usage insights
- Generate MIP data export upon request
- Provide detailed data usage reports
- Create off-band reporting on client requirements



NTT DATA'S Data Classification and Protection Solutions

Microsoft Cloud App Security

Provide visibility into cloud apps, including data access & usage and potential abuse

Conditional Access

Control access to files based on policy such as identity, machine configuration, geolocation, and more

Microsoft Defender for Endpoint

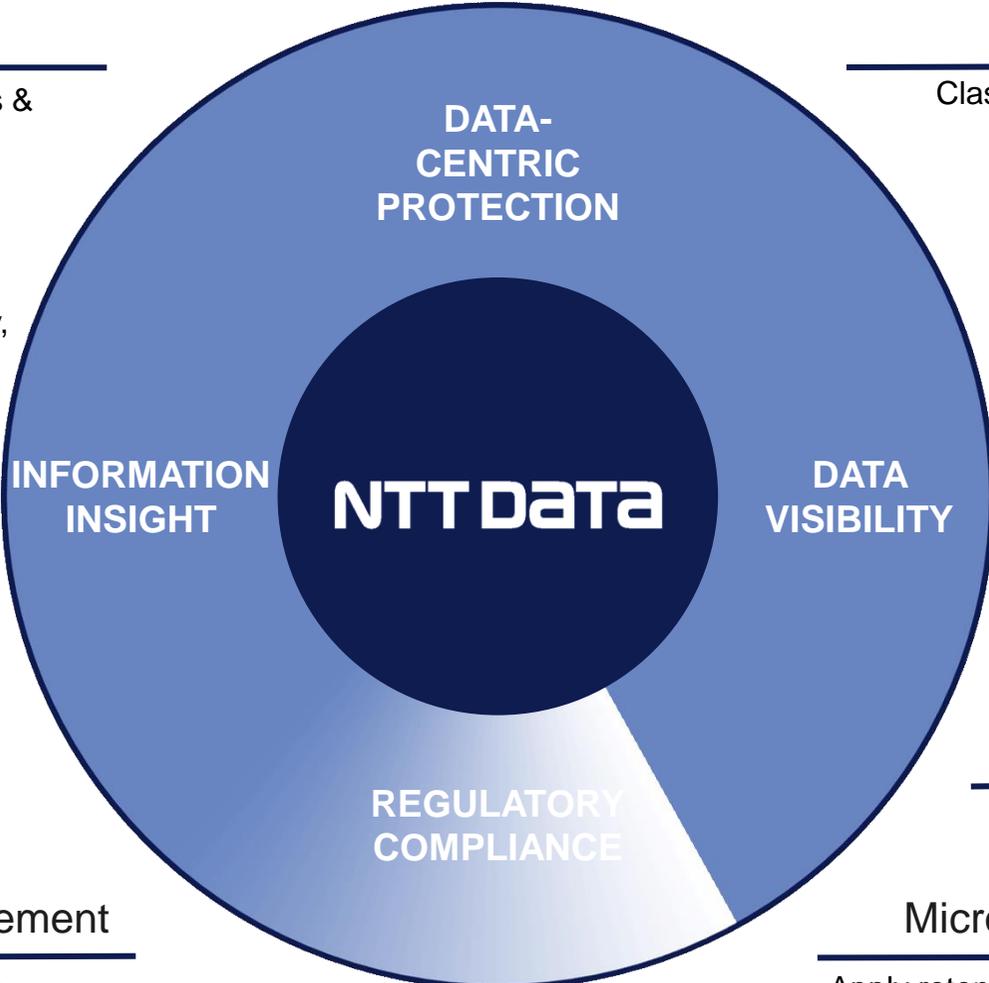
Prevent, Detect and Respond to advanced threats while minimizing your attack surface

Message Encryption

Send encrypted emails in O365 to anyone – inside or outside of the company

Microsoft 365 Advanced Security Management

Offer visibility into O365 apps usage and potential data abuse



Microsoft Information Protection

Classify, label and protect files both on-prem and in the cloud

Microsoft 365 DLP

Prevent data loss across Exchange online, SharePoint Online, OneDrive for Business

ISV Applications

Enable third-party supported data types to be protected, such as PDF files

Office Apps

Protect sensitive information while working in Excel, Word, PowerPoint, Outlook and Teams

SharePoint & Groups

Protect files in libraries and lists

Microsoft 365 Advanced Data Governance

Apply retention and deletion policies to sensitive and important data in O365

Why Partner With NTT DATA

Gold
Microsoft Partner
 Azure Expert MSP

Gold Cloud Platform
 SAP on Azure Advanced
 Specialization



A **Leader** in cyber resiliency (security consulting, strategy, incident response and business continuity)

NelsonHall, "NEAT report for Cyber Resiliency," June 6, 2019

Regulatory & Industry Compliance & Certifications







A **Leader** in the Gartner Magic Quadrant for Application Security Testing

Gartner, Inc. Magic Quadrant for Application Security Testing, April 29, 2020

- Microsoft Azure Expert MSP
- SAP on Azure Advanced Specialization
- 12 Gold Competencies, 4 Silver
- NTT & Microsoft Strategic Alliance
- CSA Corporate Member
- CNCF Silver member

- **3500** cloud architects & engineers
- **500+** cloud clients
- **5000+** cloud migrations
- **420+** Azure certifications
- **4300** experts on Microsoft technologies

3000+ security experts
6.1+ trillion logs analyzed annually
9 SOCs and **7** R&D centers
6.2 billion attacks defended annually
150+ million identities managed

A **Leader** in public cloud transformation, globally

ISG, "Provider Lens Quadrant Report for Cloud Transformation/Operation Services & XaaS 2020," November 2019

- Application Modernization:**
- **9500** app clients, globally
 - **1000+** DevOps build & release (CI/CD) engineers
 - **200+** Agile certified resources



NTT DATA

Trusted Global Innovator