proximus enterprise

Consulting services: Security

Sensitive Data Assessment

Do you know where your data resides?

By 2024, the volume data consumption per year is expected to grow to 149 zettabytes (ZB), representing a doubled increase from the amount of data consumption in 2021*. In the past, organizations primarily dealt with documents and emails. Now they are also dealing with instant and text messaging, video files, and images. The internet of things, or IoT, will only add to this explosion in data.

Protecting information is critical to ensure trust but also to meet internal and external regulatory requirements. Protecting data has become more challenging as people work in new ways, creating and sharing data across boundaries. While mobility and cloud services have helped users become more productive and collaborative, securing and monitoring the data has become harder. Companies now need to protect sensitive information across devices, SaaS applications, and cloud services in addition to on-premises environments.

Before an organization can protect its data, they first must know where it resides, how it is being used and shared, what the associated privacy and regulatory risks are, and even if the data is still needed.

Get to know your data

The Sensitive Data Assessment is a customer engagement delivered by Proximus that scans organizational data for privacy and regulatory risks. In addition to scanning organizational data for privacy and regulatory risks, the Sensitive Data Assessment also includes an activity to assess the customer's Microsoft 365 environment (including Teams, Sharepoint, Exchange…) against the Data Protection Baseline. This assessment leverages Microsoft Compliance Manager and provides insight into how your organization is performing relative to key data protection standards and regulations and is used to calculate an initial Compliance Score. Proximus will also suggest improvement actions for the company to undertake.

Ultimately, the Sensitive Data Assessment will help you understand how to mitigate and protect against privacy and regulatory risks discovered during the engagement.

From the start, Proximus will guide you through the entire workshop and implementation, making sure the effort is closely aligned with your business needs and strategy.

* source: Finances Online "How much data is created every day"

Sensitive Data Assessment

Service Description
This engagement leverages a subset of Microsoft 365 products, services, and features to gain visibility over existing, and sometimes hidden, privacy and regulatory risks that may exist in the data that resides in the customer's Microsoft 365 cloud environment and optionally on the customer's premises. The outcome and findings of the Data Risk Check serves as input to the overall workshop and will be used to create awareness and recommendations to address the discovered risks.

Scope
- Data Risk Check
  - Optional: On-premises data stores
  - Optional: Windows 10 Endpoints
- Compliance Manager Tenant Assessment
- Recommendations and next steps session

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Kick-off meeting	Setup trial license	Setup and Configure	Analyze Automated Discovery findings	Delivery and Presentation of Report	Decommission trial license

Deliverables
The findings of the Data Risk Check Automated Discovery and the Compliance Manager Tenant Assessment will be collected, analyzed, and mapped to Microsoft solutions for risk mitigation. During a workshop, the findings and identified privacy and regulatory risks will be discussed, possible solutions for mitigation will be presented and a roadmap with actionable next steps and recommendations will be created. This Roadmap will include for each recommendation the Microsoft Purview tools the customer already owns and develop next steps to guide the customer through a broader Microsoft Purview rollout.

- Activities
- Lead-time
- Resource capabilities
- Technological capabilities (solutions) if applicable
- Budget

64% of data theft incidents could be prevented with Data Loss Prevention.[1]

85% less time spent by organizations identifying, calssifying, and labeling sensitive data with automation and AI.[2]

1. McAfee: "Grand Theft Data: Data exfiltration study: Actors, tactics, and detection", 2017
2. Forrester Consulting, "The Total Economic Impact Of Microsoft 365 E5 Compliance", June 2021, commissioned by Microsoft.

Why Proximus?
- More than **15 years of experience in cybersecurity and running a security operations center**
- Experience **in all sectors**: services, industry, finance, government, …
- A **Microsoft Gold Partner for Security**, which means that you are always guaranteed the best service and the best advice
- Advanced specialization in **Threat Protection** and **Identity and Access Management**
- Unburdening support in everything from **assessment, architecture**, and **implementation** up to **managed services**

Find out more?
Contact your Proximus contact person or talk to an expert:
proximus.be/securitycontact