netwrix

Netwrix Risk Insight

Security Guide

Version: 1.0
3/31/2021

Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

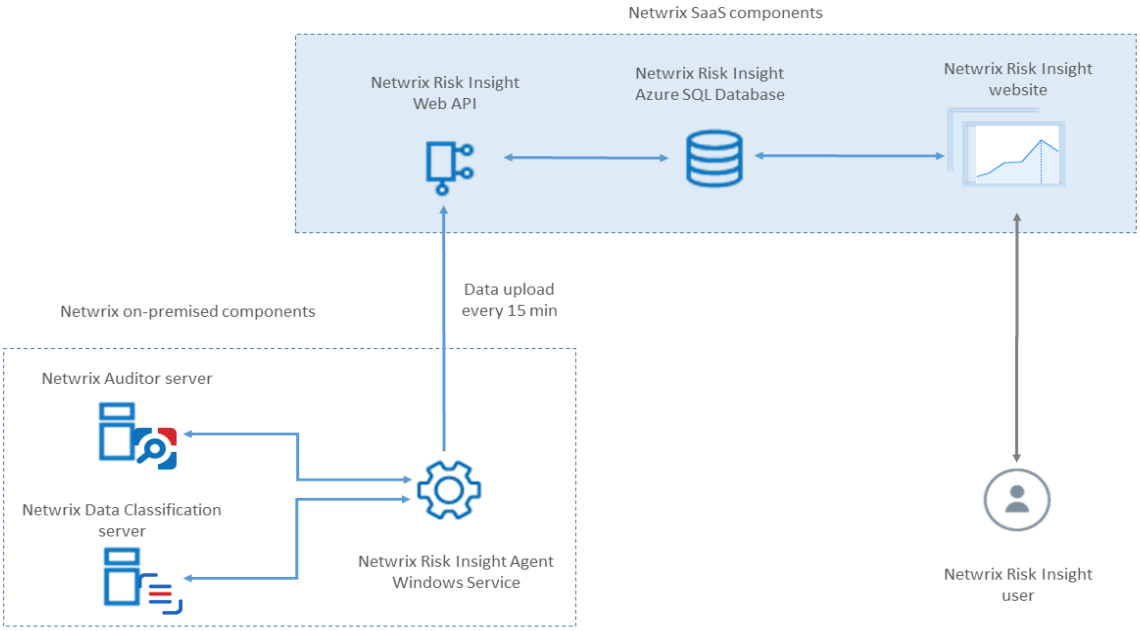
Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. How it works

Netwrix Risk Insight is a Microsoft Azure hosted, multi-tenant SaaS application that connects to one or more of a customer's on-premises Netwrix Auditor and/or Netwrix Data Classification installations. Solution architecture and components interactions are shown in the figure below.



Netwrix Risk Insight Agent is a lightweight Windows service which you deploy in your network. The agent collects aggregate data from your on-premises and/or Netwrix Data Classification servers and uploads the data to your Netwrix Risk Insight tenant via REST API calls over HTTPS every 15 minutes.

Netwrix Risk Insight Web API receives the data from **Netwrix Risk Insight Agent**. Token-based authentication is used for verification between the Web API and the agent. The service behind the API stores the data in the **Azure SQL Database**. The data is segregated by tenant (organization).

Netwrix Risk Insight Website is the presentation layer of the product that retrieves data from the Azure SQL database and presents it to users. Users can access this web portal with their corporate credentials using Azure AD Authentication (OAuth 2.0). Data is retrieved via API calls made on the user's behalf.

2. Physical security

Netwrix Risk Insight runs on Microsoft Azure infrastructure. Click here to learn more about Azure cloud security, or click here to view all Azure compliance certifications.

3. Network security

The Azure SQL database used to store the data is isolated from direct access. We use firewall rules that prevent database access to the API backend services running in Azure.

All API access happens on behalf of specific user accounts in Azure Active Directory. See Access Control section.

4. Data storage

Netwrix Risk Insight is a summary-level cloud-based dashboard application. It does not collect any specific events, objects, or their properties directly from your network or store. Instead, you configure a local agent that takes the aggregate risk counts of various kinds and sends these aggregate counts to the cloud to be displayed in the dashboards.

For example, Netwrix Risk Insight stores and reports the counts of User Accounts with Administrative Permissions, but not the names of these accounts.

Netwrix Risk Insight aggregates these counts by the corresponding Monitoring Plans that you have in your on-premises Netwrix Auditor. To accomplish this grouping, the names of the monitoring plans are also sent to the cloud. Thus, we recommend that you do not use sensitive or personal identifiable information (PII) for your monitoring plan names.

If you also decide to collect data from Netwrix Data Classification, Netwrix Risk Insight will reflect the count of Sensitive and Duplicate Documents by Taxonomy Name and by file share and SharePoint locations. Thus, in that case Taxonomy names and the names of your servers, shares, and SharePoint servers will be sent to the cloud along with the count of corresponding files located there. No filenames, content or any other information on specific files is ever sent to the cloud.

Finally, if you use Netwrix Risk Insight to display aggregate dashboards across multiple locations, the display names that you give to these locations will also be stored.

4.1. Data Collection

The following data is collected from on-premises :

Metric (count of)	Grouped by	Grouping example
Administrative Groups	Monitoring Plan Name	Windows Servers
Disabled Computer Accounts	Monitoring Plan Name	Active Directory
Empty Security Groups	Monitoring Plan Name	Active Directory
Inactive Computer Accounts	Monitoring Plan Name	Active Directory
Inactive User Accounts	Monitoring Plan Name	Active Directory

Metric (count of)	Grouped by	Grouping example
User Accounts with Administrative Permissions	Monitoring Plan Name	Active Directory
User Accounts with Password Never Expires	Monitoring Plan Name	Active Directory
User Accounts with Password Not Required	Monitoring Plan Name	Active Directory
Direct Permissions on Files and Folders	Monitoring Plan Name	HR Shares
File Names Containing Sensitive Data	Monitoring Plan Name	HR Shares
Potentially Harmful Files on File Shares	Monitoring Plan Name	HR Shares
Shares Accessible By Everyone	Monitoring Plan Name	HR Shares
AV Enablement	Monitoring Plan Name	Windows Servers
Admin Membership Blurring	Monitoring Plan Name	Active Directory
Applicable OS	Monitoring Plan Name	Windows Servers
Enabled Guest Accounts	Monitoring Plan Name	Active Directory
Under governed Windows Update Configurations	Monitoring Plan Name	Windows Servers
Anonymous SharePoint Shared Sites	Monitoring Plan Name	SharePoint Sites
Site Collections with Broken Inheritance	Monitoring Plan Name	SharePoint Sites
SharePoint Content Shared with Everyone	Monitoring Plan Name	SharePoint Sites
Site Collections with Share By Link Enabled	Monitoring Plan Name	SharePoint Sites

The following data is collected from Netwrix Data Classification:

Metric (count of)	Grouped by	Grouping example
Sensitive Documents by Taxonomy	Taxonomy Name	GDPR, PII, CCPA
Sensitive Documents	• SharePoint site collection • SharePoint Online site collection • File server name and share name • Box • Database • Dropbox • Exchange Mailbox • Exchange Server • Google Drive • Outlook Mail Archive	https://test.sharepoint.internal \\Server2\Docs
Duplicate Documents	• SharePoint site collection • SharePoint Online site collection • File server name and share name • Box • Database • Dropbox • Exchange Mailbox • Exchange Server • Google Drive	https://test.sharepoint.internal \\Server2\Docs

Metric (count of)	Grouped by	Grouping example
	• Outlook Mail Archive	

4.2. Data Processing

Your data is **only** used to perform the risk calculations based on the aggregate counts necessary to populate the Netwrix Risk Insight dashboards. Data is processed and analyzed on your premises by Netwrix Auditor and Netwrix Data Classification. The aggregate counts are sent to the cloud and presented in the Netwrix Risk Insight dashboards.

This enables Netwrix Risk Insight to summarize, for example:

- There are 3000 documents stored in the Southampton, UK location within the file share \\Server2\Docs
- There are 200 documents classified as GDPR in the Southampton, UK location within the SharePoint site https://test.sharepoint.internal

5. Data security

5.1. Data at rest

Data is persistently stored within the Azure SQL Database in the region you select when creating your account. All data stored in the database is encrypted with an AES 256-bit encryption algorithm.

5.2. Data in transit

Data will be transferred between the system components in a few different ways:

- Agent -> API
- API -> SQL Database
- SQL Database -> Application
- Application -> Browser (User)

Data is always encrypted in transit, and connections are made over HTTPS to prevent eavesdropping.

6. Access control

Netwrix Risk Insight is a multi-tenant cloud application. All data is segregated by tenants and access control is enforced.

Only the users who you explicitly add to your organization in Netwrix Risk Insight get to see your dashboards in the product. User access is set up using a customer Azure AD account. You can further protect access using Azure AD support for Multi-Factor Authentication (MFA). Thus, when users get deprovisioned from their corporate directories they also automatically lose access to Netwrix Risk Insight.

Netwrix employees who have administrative access to the Azure deployment to maintain the application only do so under their own Netwrix corporate accounts and all their activity is audited.

7. Customer data privacy

All customers access Netwrix Risk Insight via the same address:

- https://risk.netwrix.com

However, based on your selection at account signup / creation, your data is stored in one of the following Microsoft Azure regions:

- If you select the Americas, your data is stored in the Microsoft Azure region known as “West Central US”.
- If you select Europe/Africa, your data is stored in the Microsoft Azure region known as “West Europe”.

The region is selected by the user who is signing up for the product. We create a tenant for your organization in that region and guarantee that all your data always stays within that region.

If your company is split across multiple regions, you can select the region where the headquarters are located or, alternatively, have a separate tenant for each region. Please note that in this case Netwrix Risk Insight will not provide a company-wide risk score.

8. Compliance

Netwrix Risk Insight uses Azure datacenters in your region of choice. Microsoft provides the highest levels of security for these datacenters including compliance to the following standards: General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS.

For more information, visit https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/