VOTIRO

Votiro SaaS 23.06.11

Release Notes

June 2023

Copyright Notice

The material herein is proprietary to Votiro CyberSec Ltd. This document is for informative purposes. Any unauthorized reproduction, use or disclosure of any part of this document is strictly prohibited.

Votiro CyberSec's name and logos are trademarks of Votiro CyberSec Ltd., its subsidiaries or affiliates. All other company or product names are the trademarks of their respective holders.

www.votiro.com

Contents

1   Introduction

We are very pleased to announce the latest release of Votiro SaaS version 23.06.11. This version contains important enhancements to our product!

2 New Features

The following new features and improvements are added to this version of Votiro SaaS.

2.1 MSSP Capabilities

Our product now supports MSSP (Managed Security Service Provider) use cases.

Some of the prominent MSSP use cases that are supported:

- Ability for the MSSP admin to create new customers and assign licenses.

- Use the MSSP dashboard to see/filter all the MSSP customers' data.
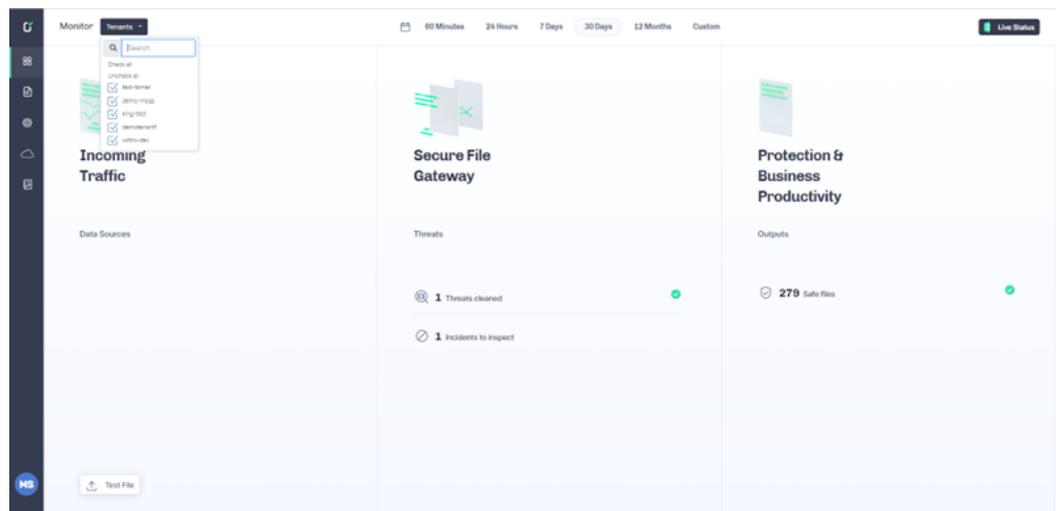
- Use the MSSP incidents to see/filter all the MSSP customers' incidents data.
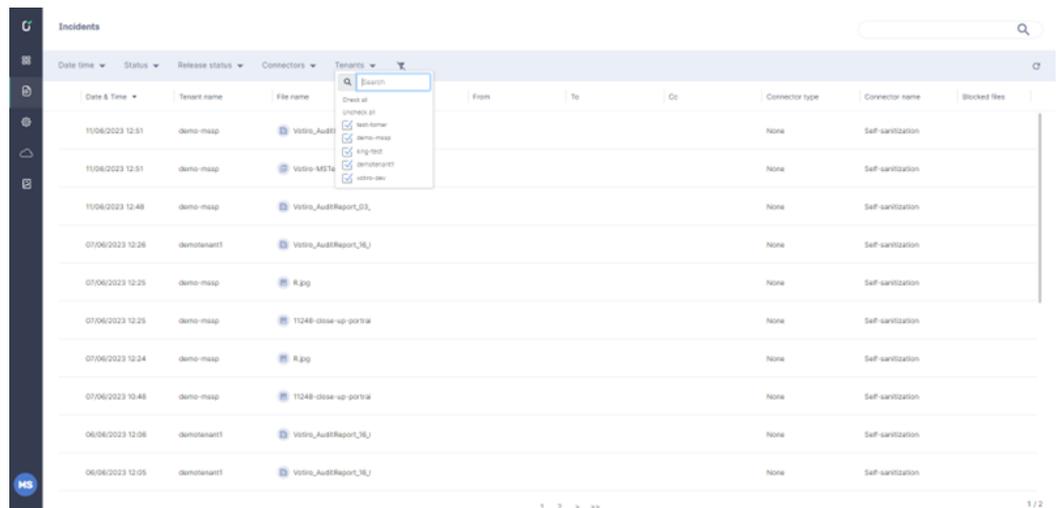
- Ability to create reports on each MSSP customer's data.

2.2 URL Protection

The product now includes improved protection against the usage of malicious URLs.

The URL protection includes the following features:

■ Remove malicious URL in the email body - the link will be removed once a suspicious link is detected in the email body.

■ High-performance rate - the URL protection architecture supports a high-performance rate by reducing response time.

■ License flag - URL protection capabilities can be turned on/off by license.

■ Different file types - URL protection can be applied to the following file types:

♦ PDF

♦ Word (Doc, DOCX)

♦ Excel (XLSX)

♦ Email

2.3 Bitdefender anti-malware protection

Our product now includes one of the best anti-malware engines in the market (Bitdefender SDK) that will scan any file before sanitization.

This will add protection for malicious executable files and other file types that cannot undergo sanitization.

This new engine will also be used for our retrospective detection.

2.4 New AI detection for malicious Office Macros

After a few months of testing and tuning, our AI detection for malicious office Macro becomes GA.

This is a new AI module that we trained on over 1 million samples to make it accurate as possible.

The new AI module will improve our office macro detection in the following aspects:

■ Increase the detection rate of malicious macros.

■ Reduced false positives.

■ Provide us a confidence level of the detection to be able to tag a macro as malicious or suspicious.

3   Resolved Issues

The following open issues have been resolved in this latest version release:

- Resolved an issue where some CSV files were detected as Unknown.

- Resolved an issue where the incident sanitization log contains "_blocked.pdf" in the original file name.

- Resolved an issue where large file sanitization using our AWS S3 connector failed.