Strategic roadmap to ensure

Exchange security

ManageEngine

Exchange Reporter Plus

Strategic roadmap to ensure Exchange security

With the quantum leap in the adoption of remote work environments, many security vulnerabilities have opened up. Protecting remote connections is becoming increasingly difficult as hacking techniques have become more sophisticated and tricky. An estimated two billion email addresses and 21 million passwords were exposed during a single data breach in 2019, according to a State of Security report. Phishing email attacks reached 241,324 incidents in 2020, a surge of more than 125,000 over the previous year, the FBI observed.

The White House's Office of Management and Budget revealed that 74 percent of federal agencies are either in a Risk or High risk category, for cyberattacks. Across the globe, vital national and international information has been compromised. The most common source of all cyberattacks is email. Apart from the usual spam, virus and phishing attacks, new techniques like ransomware and crypto malware attacks are becoming common.

Email bombing is an increasingly popular form of spam, and it uses spam emails as a Trojan horse, according to the State of Security report. 83 percent of organizations across the world have recently experienced phishing attacks. Each year, more than 10 million malware attacks are reported, a figure that has increased each year. 79 percent of IT leaders believe employees put the organization's data at risk accidently or knowingly. In about 47 percent of the data breaches, the consequences are severe.

Importance of safeguarding your Exchange environment

Individuals at most organizations communicate through emails, and since there are often thousands of mailboxes in an organization, the scope of an email attack is wide. With the exposure rate being high and without any proper security settings, emails have become the most common and simple pathway for an attack. One can easily hack into a mailbox using methods, like key logging or brute-force attacks, to extract vital information like bank account numbers, major transactions, business confidential data, and more. Emails are also the most preferred medium for launching internal attacks. It is easier to access an email account than hack into a sophisticated firewall protected server. Hence, it is vital to safeguard your email accounts and data accessed by users.

What is a strategic roadmap?

A major mistake organizations often commit while dealing with anomalies is to try and use many methods to resolve the issue. This causes confusion and IT admins can lose track of what to monitor and how to manage to prevent the issue from appearing again. A systematic, step-by-step approach is required to fortify your Exchange environment completely. Taking one step at a time and leaving no space for loopholes is vital.

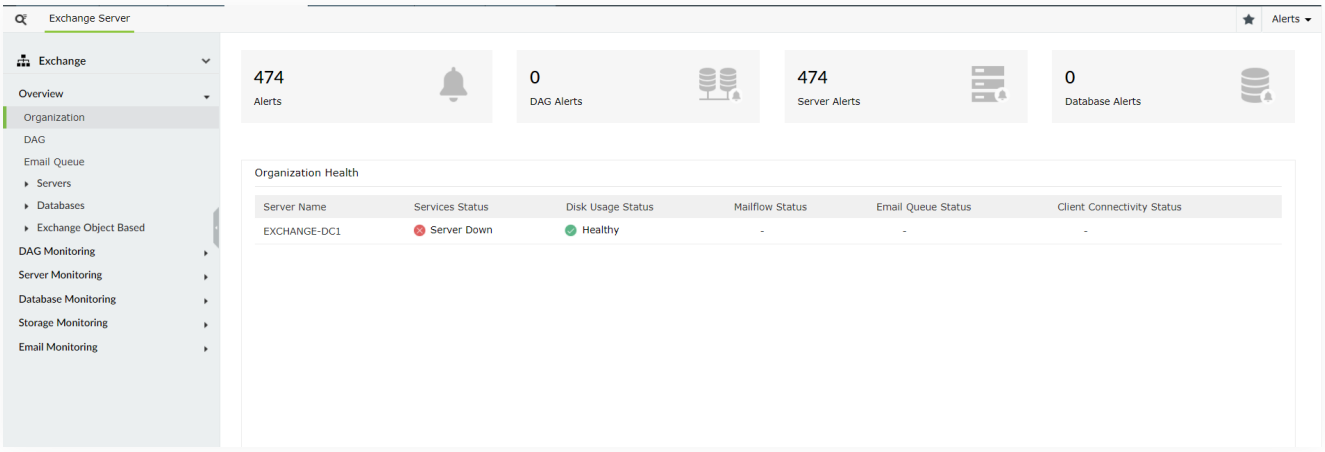
This e-book presents seven steps to help you ensure Exchange security. We also discuss how Exchange Reporter Plus, a reporting, auditing, monitoring, and content search solution for Exchange Server, Exchange Online, and Skype for Business, enables you to perform these steps and manage your organization's email environment.

1. Detecting anomalies before they occur
2. Auditing user activities
3. Fetching regular reports and updates
4. Going beyond what the native tool offers
5. Keeping a check on the mailbox content
6. Assigning granular technician roles
7. Creating alert profiles for immediate notifications and taking preventive actions
8. without any time delay.

1. Detecting anomalies before they occur

No attack is random. While backtracking, you can uncover a series of events that have opened up vulnerabilities. For example, frequent issues in client connectivity, or any other Exchange service, foreshadows future network issues. Unplanned mailbox exports can indicate an intruder is trying to tamper with the organization's mailboxes. All attacks follow a pattern and can be predicted. It is vital to detect this pattern and check for issues in your organization regularly. That way, you can stop a potential attack before it happens. This saves time and resources for your organization.

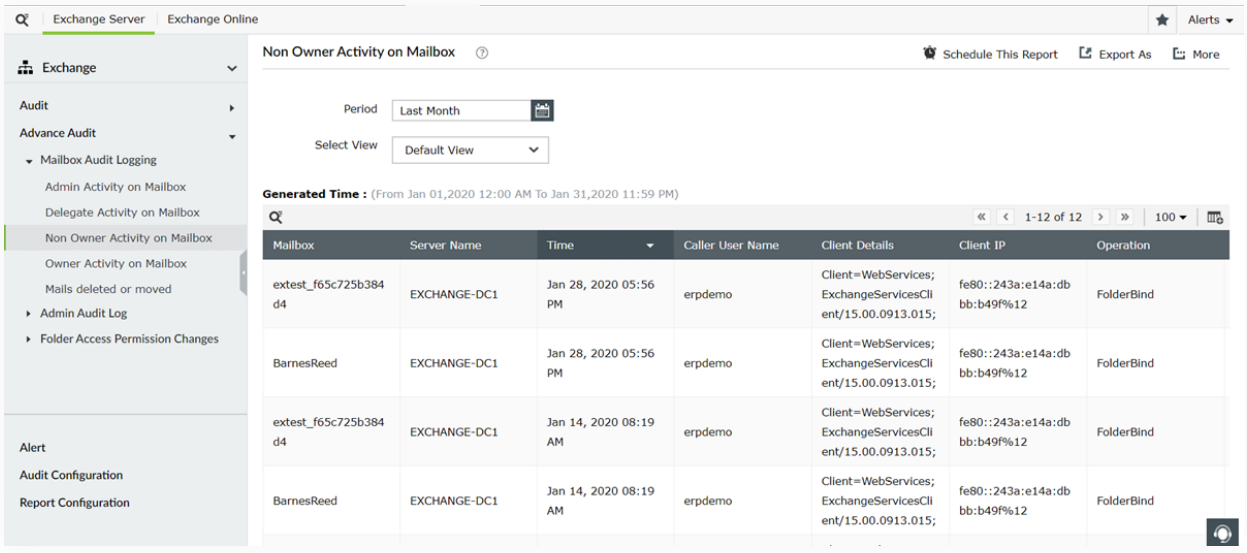
Using Exchange Reporter Plus, you can audit Exchange Online and Exchange Server, as well as monitor your Exchange Server services and endpoints 24/7. This ensures you stay informed about any major changes. While monitoring your organization's servers, Exchange Reporter Plus triggers red flags whenever an abnormality is formed. By checking these red flags, you might note frequently occurring errors and detect related issues. You can also view the status of your organization's Exchange servers using the monitoring dashboard. This effectively reduces the daily time necessary to check the health of every component or service in your Exchange environment.



2. Auditing user activities

Once you confirm the proper functioning of your Exchange environment by monitoring the services and endpoints, you need to proceed to track the user activities in your organization. A large amount of sensitive data is often accessible to your organization's staff. A few impostors might try to misuse permissions, such as Send As, or Send on Behalf, to access important mailboxes, steal vital information, or communicate false information. You need to keep a close watch on the mailbox and folder permission changes that occur.

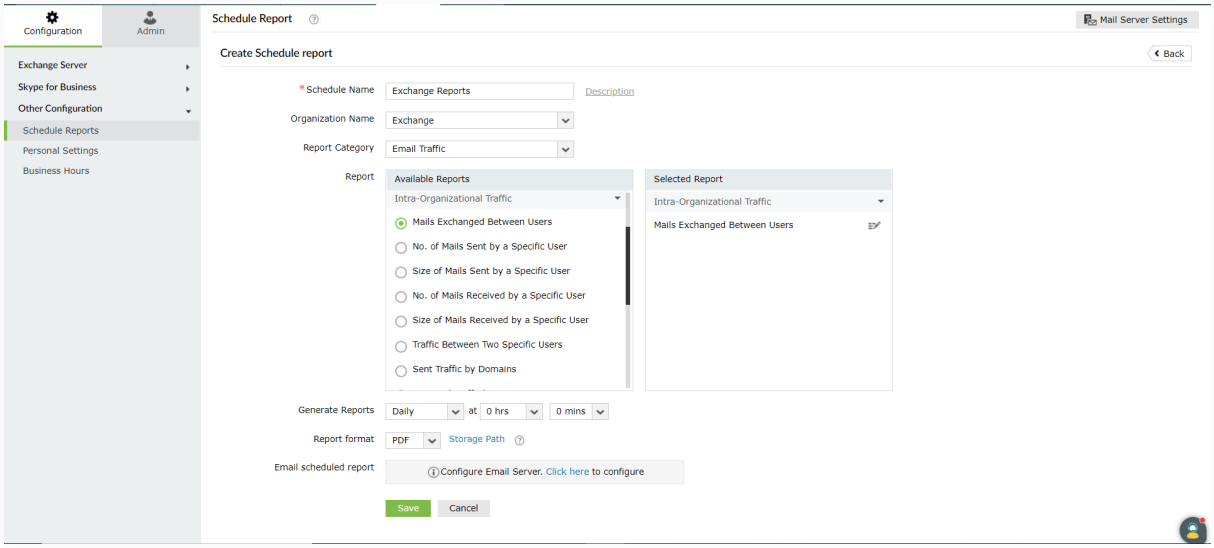
If there are any mismatches in the assigned permissions, or if some users are found to possess excess permissions, Exchange Reporter Plus' advanced auditing capabilities lets you know immediately. You can track of all user actions, including the admins, owners, delegates, and non-owners of a mailbox. The native tool does not offer granular reporting to this level, so that you can keep track of every small and big detail, like the time of change or the client IP from which the change was made.



3. Fetching regular reports and updates

It is important to devise strategies to fortify Exchange in your organization, but it is equally as important to be consistent in these efforts. Many organizations and IT administrators plan to use various defensive strategies, like using patches, frequent troubleshooting, running diagnostics, and others. However, if they experience a period of no visible signs of trouble, they tend to bypass established procedures. That is when major issues result. Implementing complex PowerShell codes and native tool diagnostics to search each day for abnormalities is tedious.

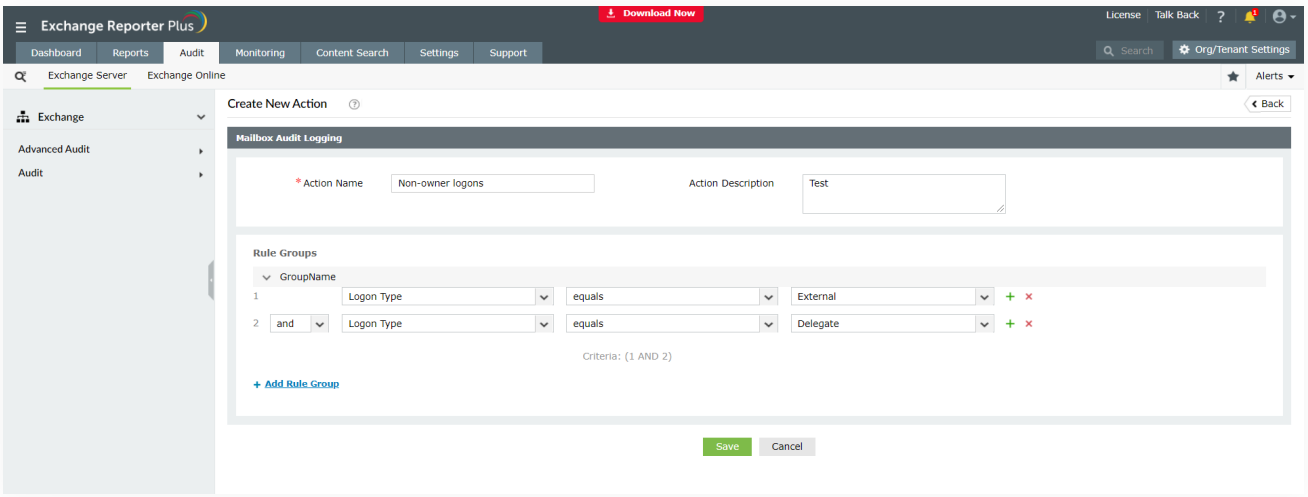
Consistently and constantly fetching reports, monitoring, and auditing your environment is vital. Oversight of a single action can wreck havoc in your environment within hours. Exchange Reporter Plus provides a reliable solution. This tool delivers regular updates about every aspect of Exchange, including its health, status, major changes, and more. This enables you to implement an established routine that ensures malicious activities are efficiently detected. You can easily schedule and generate reports that are automatically sent to stakeholders. Reports can be exported in four formats: HTML, XLS, CSV and PDF, and can also be used for compliance purposes.



4. Going beyond what the native tool offers

The generic reporting, auditing and monitoring functionalities offered by native tools can be bypassed easily, given the sophisticated level of data theft techniques utilized today. In Exchange servers you have to use Windows PowerShell to get even basic details, like the server health, client connectivity, email queues, and more. Apart from being complex and time-consuming, this can introduce other issues that might go unnoticed. But using cmdlets, like Search-MailboxAuditLogs, each time you need to work with the audit logs for a specific mailbox can be mind-numbing.

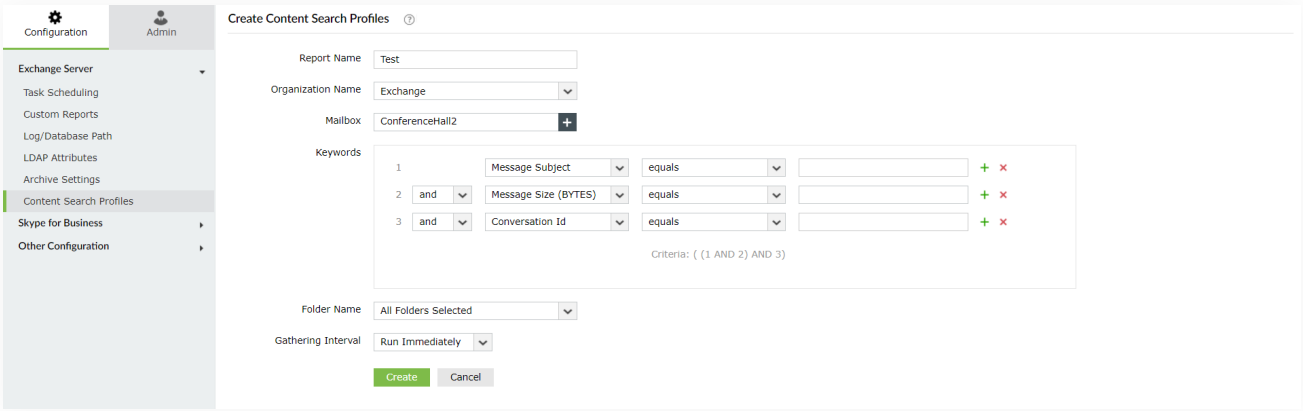
Exchange Reporter Plus equips you to develop your own defenses. Create customized reports and using the audit action configuration option to configure personalized audit actions. Custom reports, easily tailored to your organization's needs, help you scrutinize every aspect of your Exchange environment, especially areas unnoticed by native tools. For example, you can configure actions as granular as non-owner mailbox logon audits, and use rule groups to set criteria to scrutinize logs in greater depth, as shown in the image below.



5. Keeping a check on the mailbox content

Another major shortcoming of the native Exchange tool is that its eDiscovery feature is not very helpful. Although you can track and spot specific content based on keyword searches, you cannot see the entire email and the context of the information, and you cannot download attachments directly. Also, the keywords-based search is not open-ended. In case of internal data theft or insider attacks, at risk is information like bid quotations, transaction details, business confidential information and blueprints, which are shared via email. You need to stay vigilant about the kind of content that is shared by the employees. An Exchange administrator cannot possibly check every mailbox. A specialized tool is needed.

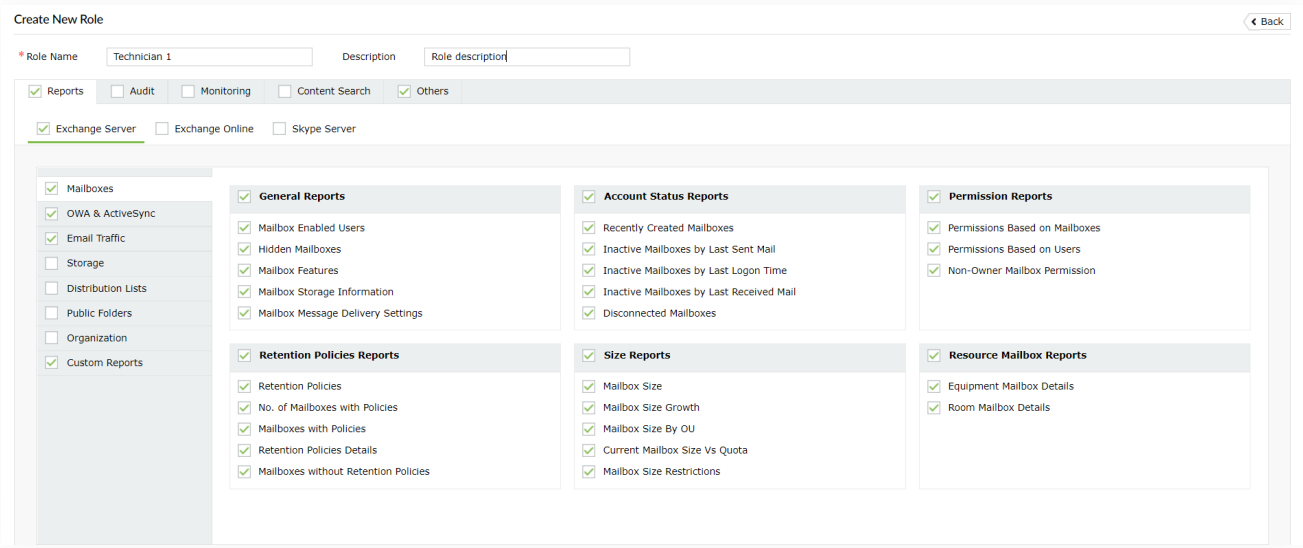
Exchange Reporter Plus enables you to perform keyword, attribute, and pattern-based searches in your organization's mailboxes. It can search a single mailbox, as well as multiple or all mailboxes at once. You can create content search profiles that scrutinize mailboxes using various condition filters, and that automatically generate and email details to stakeholders. The tool also enables you to view the content in HTML format and isolate questionable attachments so you can review them for security reasons.



6. Assigning granular technician roles

Assigning specific roles to technicians is the most overlooked aspect of Exchange administration, and where major problems tend to originate. The native tool offers generic roles that include several Exchange permissions that do not necessarily suit the access levels or hierarchy of each technician. More rights are granted than what is required for certain technicians. Given the varied nature and dynamic structure of organizations, the needs are also becoming unique. Technicians cannot be assigned standard sets of permissions, these need to be flexible and contain checks and balances.

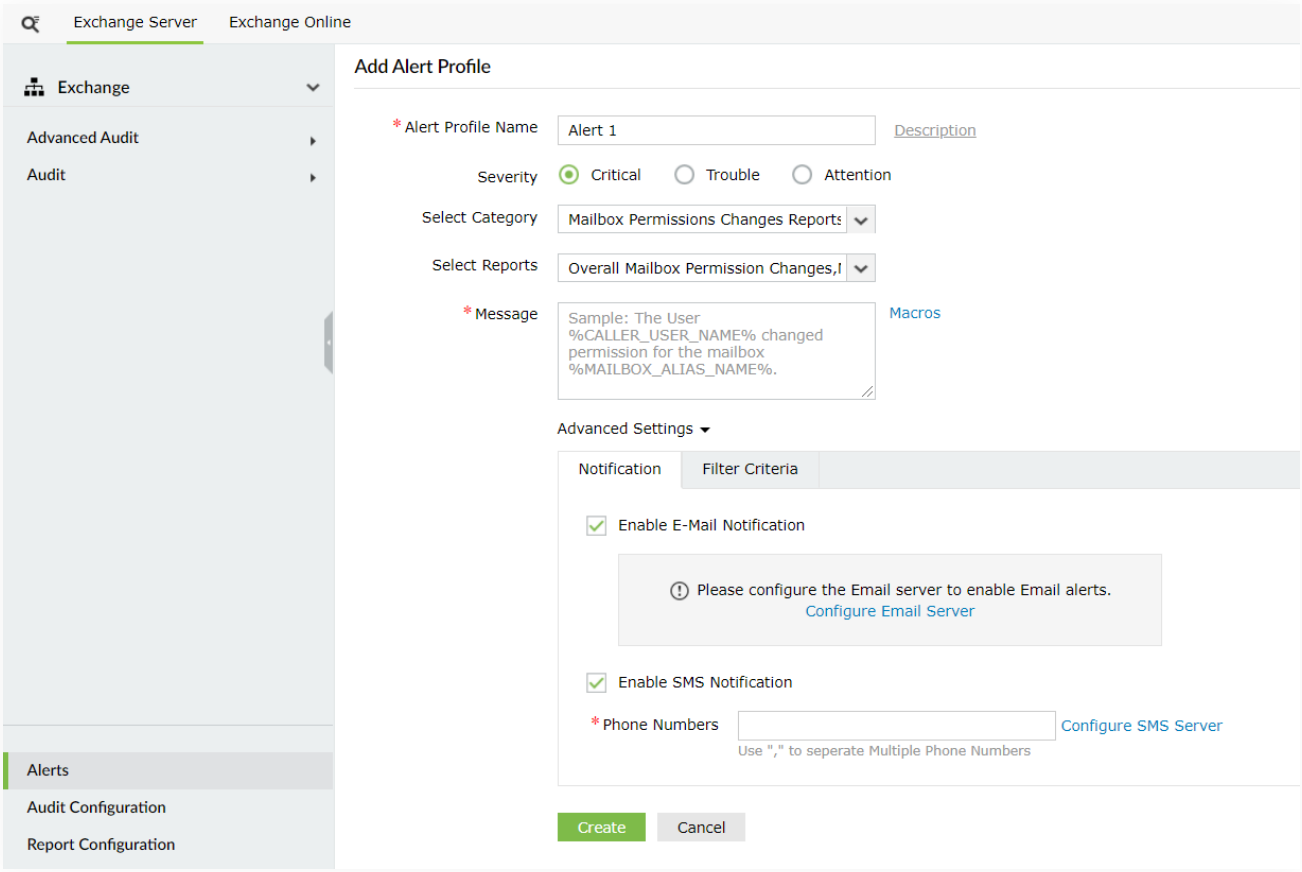
If you are using Exchange Reporter Plus to manage your Exchange environment, then you can create custom roles granting only selected permissions that you can assign to individual technicians. As shown in the image below, you can create a new Exchange Reporter Plus technician role for accessing only select Exchange server reports.



7. Creating alert profiles for immediate notifications

The purpose of setting strategies is to fortify your Exchange environment by taking the right actions at the right time. An important feature in that respect is alert profiling. Unfortunately, the monitoring and alert settings in the native tool are not extensive. Before you can manually investigate these errors, the damage is already done. You need a tool that can monitor services vigilantly, and audit every important change and notify you about the anomalies that you deem serious. Exchange Reporter Plus can help.

By creating alert profiles in Exchange Reporter Plus, you can receive immediate notifications about all anomalies via email and SMS. With the severity of the alert established, when an alert is triggered, you can implement an immediate action plan to tackle unforeseen issues. You can deploy macros to distribute different customized alert messages based on the severity of the action. You can also use filters to scrutinize the conditions to raise an alert.



Conclusion

The FBI's internet crime report states that in 2019, the Internet Crime Complaint Center (IC3) received around half a million complaints including Business Email Compromise (BEC), ransomware, elder fraud, and tech support fraud, that produced estimated losses of over $3.5 billion. Apart from monetary losses, many organizations have also been subjected to a number of lawsuits for not adhering to compliance and security standards like GDPR, FISMA, and GLBA.

Though Microsoft Exchange and Microsoft 365 offer methods to protect your Exchange Server and Exchange Online environments, like patches and other security options, they are not fool proof. It is prudent to use a specialized tool, intuitively designed to protect and safeguard your hybrid Exchange environment. Exchange Reporter Plus can help you with this. You can monitor multiple mailboxes, servers, and tenants using this tool. The reporting, monitoring, and auditing features promptly detect anomalies. With real-time alerts, you can stay informed about all small activities and issues, and take immediate action to remedy them at the grassroots level.