

Security Audit Report

**THE CUSTOMER
EXPERIENCE**

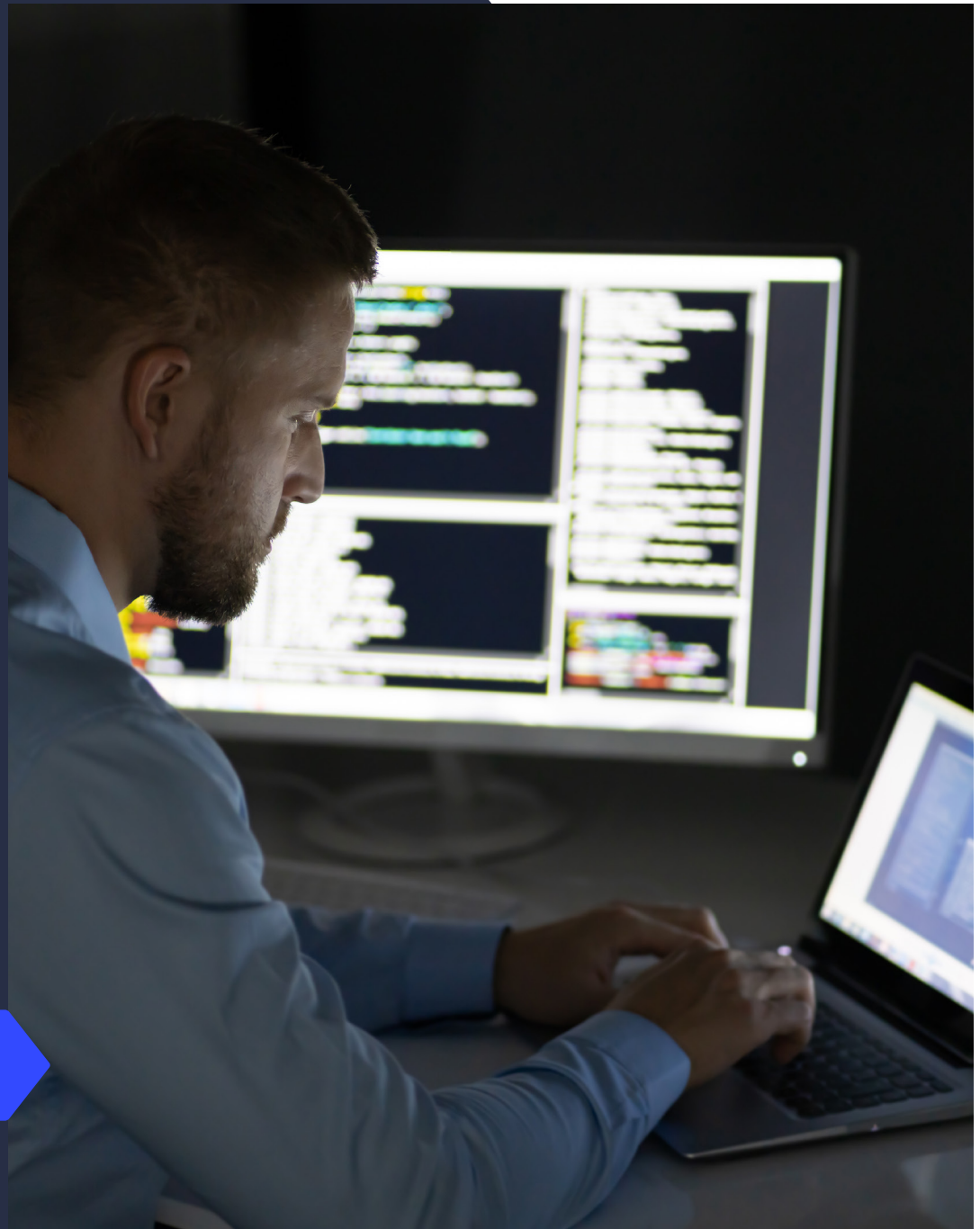


TABLE OF CONTENTS

Audit Report Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules Report

Inbox Rules Report

Security Strategy

Operational Model

Audit Report Summary

At a glance gain insight into major potential issues and gaps within a Microsoft 365 instance. Using each of the subsequent report you are able to dive into deeper detail but here is where you get the overview to help you understand your potential risk.



Email Security

Your inbox is currently at risk for phishing and malware.



Encryption

You are currently at risk for non-compliance.

Category	Results
Admin Report Summary	Total Admins: 2 Total Global Admins: 0
User Report Summary	Total Users: 5 Total Users with MFA Enabled: 0 Total Users with MFA Disabled: 5 Total Users with Passwords over 90 Days Old: 4 Total Users with Passwords Set to Never Expire: 0
Mailbox Report Summary	Total Mailboxes: 3 Total Mailboxes with Advanced Auditing Enabled: 2 Total Mailboxes with Advanced Auditing Disabled: 1 Total Mailboxes Inactive for 30 Days: 3 Total Mailboxes Never Activated: 1
Forwarding Rules Summary	Total Mailboxes with Forwarding: 1 Total Mailboxes with OWA Forwarding: 1 Total Mailboxes with Exchange Admin (EAC) Forwarding: 0 Total Mailboxes with Inbox Forwarding Rules: 1
Inbox Rules Summary	Total Number of Mailboxes with Rules: 1 Total Number of Rules: 2 Total Inbox Rules Set to Move Messages: 1 Total Inbox Rules Set to Delete Messages: 0

TABLE OF CONTENTS

Audit Report Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules Report

Inbox Rules Report

Security Strategy

Operational Model

Admin Report

The Admin Report identifies potential comprises and gaps within a company's security stance for users with elevated roles. This report also helps to guide customers to respect the rule of least privilege. Microsoft Admins can then leverage this insight to remove/reduce permissions where it makes sense. The Office 365 Security Audit Tool has analyzed your customer's administrators and identified potential security vulnerabilities.



Display Name	Email	Roles	Severity
VA Admin	adminva@mbsecurityaudit-resoldtwo.onmicrosoft.com	Dynamics 365 Administrator, Exchange Administrator, Power BI Administrator, Service Administrator, SharePoint Administrator, Skype for Business Administrator, User Management Administrator	High 
test test	testsuspend2@mbsecurityauditresoldtwo.onmicrosoft.com	Exchange Administrator, Helpdesk Administrator	High 

TABLE OF CONTENTS

Audit Report Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules Report

Inbox Rules Report

Security Strategy

Operational Model

User Report

With the User report customers are able to gain insight into unauthorized access, gain insight into password policy adherence, and use of multi factor authentication. Working with their Microsoft 365 admin team customers are able to quickly remediate compromised accounts and block future sign ins if needed. The Office 365 Security Audit Tool has analyzed your customer's users and identified potential security vulnerabilities.






Display Name	Email	Recipient type	Password	Multi-Factor Authentication	Severity
test test	testsuspend2@mbsecurityauditresoldtwo.onmicrosoft.com	None	Last Changed On: 11/11/20, 2:05 PM Expires On: 2/9/21, 2:05 PM	State: Disabled	High 
VA Admin	adminva@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Last Changed On: 8/4/20, 10:35 AM Expires On: 11/2/20, 9:35 AM	State: Disabled	High 
test test	test@mbsecurityauditresoldtwo.onmicrosoft.com	None	Last Changed On: 11/11/20, 2:06 PM Expires On: 2/9/21, 2:06 PM	State: Disabled	Medium 
test suspend	testsuspend@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Last Changed On: 11/11/20, 2:05 PM Expires On: 2/9/21, 2:05 PM	State: Disabled	Medium 
Double User	doubleuser@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Last Changed On: 4/27/21, 9:10 AM Expires On: 7/26/21, 9:10 AM	State: Disabled	Medium 

TABLE OF CONTENTS

Audit Report Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules Report

Inbox Rules Report

Security Strategy

Operational Model

Mailbox Report

The Mailbox report enables the logging of IP addresses, country of origin for logins, and deeper understanding of the use of advanced mailbox auditing (used for forensic investigation) within the customer's organization. The Office 365 Security Audit Tool has analyzed your customer's mailboxes and identified potential security vulnerabilities.




Display Name	Email	Recipient type	Advanced Auditing	Last Accessed	Ip Address	Country	Created On	Severity
test suspend	testsuspend@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Enabled	2/21/21, 12:32 PM	N/A	N/A	11/11/20, 2:06 PM	Medium 
VA Admin	adminva@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Enabled	11/22/20, 3:45 AM	N/A	N/A	8/4/20, 10:36 AM	Medium 
Double User	doubleuser@mbsecurityauditresoldtwo.onmicrosoft.com	User Mailbox	Disabled	Never	N/A	N/A	4/27/21, 9:11 AM	Medium 

TABLE OF CONTENTS

Audit Report
Summary

Admin Report

User Report

Mailbox Report

**Forwarding Rules
Report**

Inbox Rules Report

Security Strategy

Operational Model

Forwarding Rules Report

The Forwarding Rules report helps highlight users who are forwarding to private mailboxes and more importantly helps admins prevent sensitive data leakage. The report lists all forwarding rules (internal and external) and provides options for admins to prevent forwarding rules from being set up in the future and allows for quick deletion for problematic forwarding rules. The Office 365 Security Audit Tool has analyzed your customer's forwarding rules and identified potential security vulnerabilities.


Display Name	Email	External Forwarding Rules	Total Forwarding Rules	Severity
VA Admin	adminva@mbsecurityauditresoldtwo.onmicrosoft.com	2	2	High 
Type: OWA Rule Name: OWA Rule Addresses: smtp:admin@vacoffee297.onmicrosoft.com				
Type: Forward To Name: Rule QA Addresses: "vesna.arezina@appriver.com" [SMTP:vesna.arezina@appriver.com]				

TABLE OF CONTENTS

Audit Report
Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules
Report

Inbox Rules Report

Security Strategy

Operational Model

Inbox Rules Report

The Inbox Rule report lists all inbox rules with the intention to highlight potentially compromised accounts. Using this tool an admin is able to gain a better understanding of how bad actors are moving within an environment and with the Security Audit Tool to disable suspicious rules if needed. The Office 365 Security Audit Tool has analyzed your customer's inbox rules and identified potential security vulnerabilities.


Display Name	Email	Rules	Severity
VA Admin	adminva@mbsecurityauditresoldtwo.onmicrosoft.com	Forward, Move	High 
Rule QA: Forward			
Rule1: Move			

TABLE OF CONTENTS

Audit Report
Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules
Report

Inbox Rules Report

Security Strategy

Operational Model

A straightforward Security Strategy

Cyberattacks making headlines like SolarWinds and Hafnium call into question the scale and sophistication of attacks infiltrating the mailbox. While the headlines may come and go, long term effects of these attacks will be felt across organizations. SolarWinds sites they anticipate 18 months of impact from the attack that all began in an M365 mailbox while the Hafnium attack across on-premise exchange servers enabled access to victim email accounts allowing the installation of added malware that paves the way for long-term access. While some may think patching is enough in today's cyber age, addressing the threat lifecycle of bad actors with a simple and proactive security strategy will close 95% of your attack prevention gap.

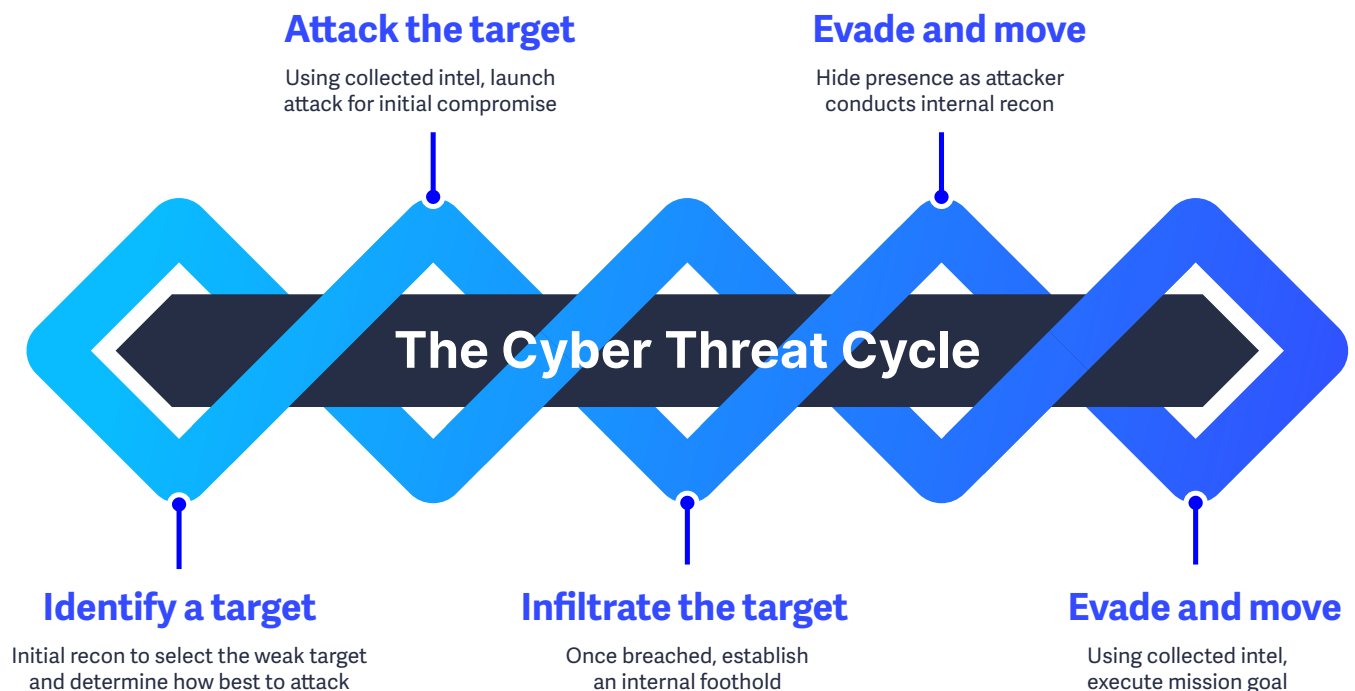


TABLE OF CONTENTS

Audit Report Summary

Admin Report

User Report

Mailbox Report

Forwarding Rules Report

Inbox Rules Report

Security Strategy

Operational Model

Turn a Complex Plan into a Simple Operational Model

Protect

Advanced Email Threat Protection & Incident remediation for targeted phishing attacks enables a multi-layered email defense strategy.

Detect

Our Security Audit, powered by Zix | AppRiver, helps detect suspicious user behavior and vulnerable user management practices.

Respond & Recover

Email backup and recovery keeps your employees productive by providing a clean copy of their data, while responding to a potential breach.

