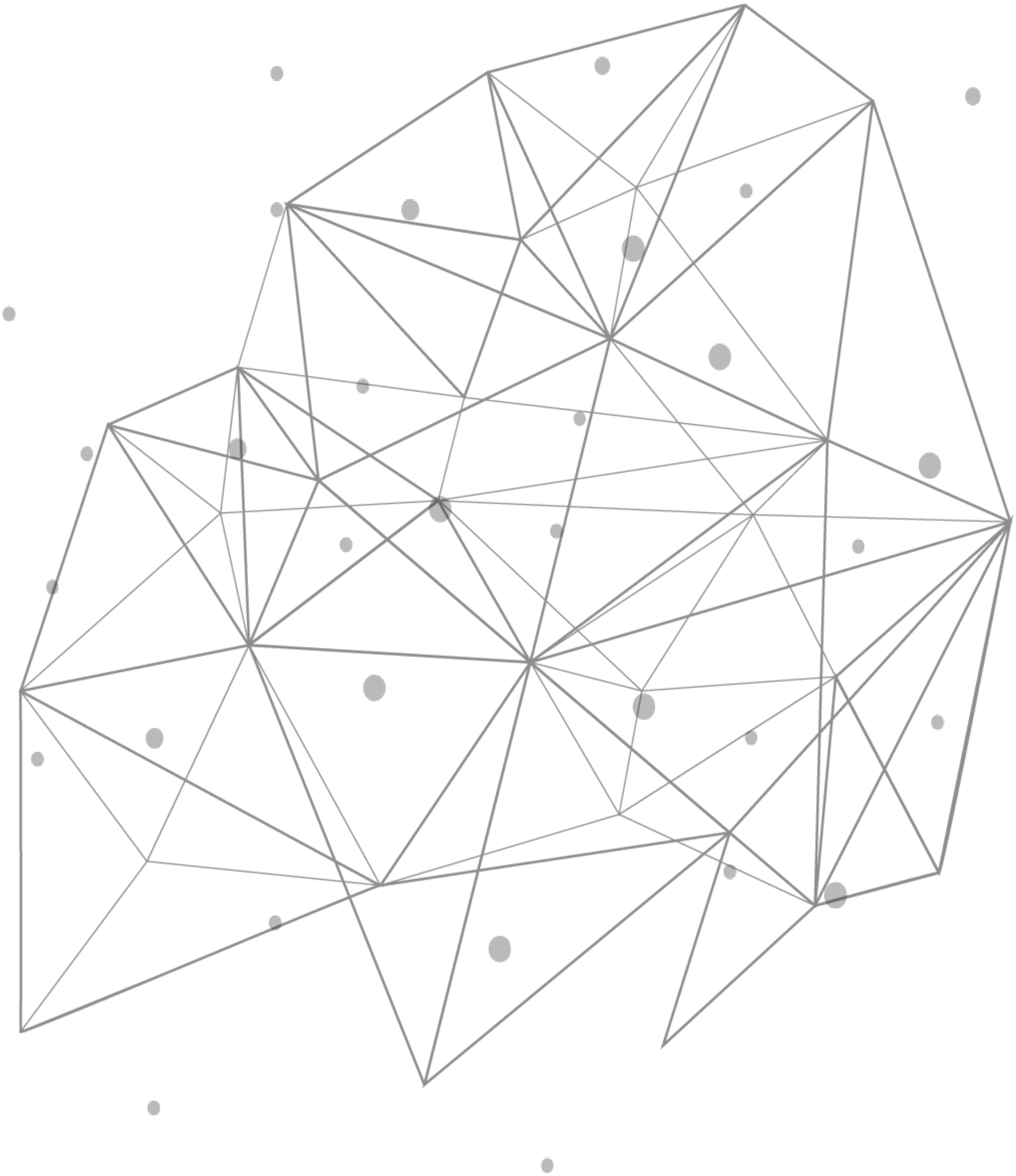
TCPWave DDI

Network Forensics with Microsoft Active Directory



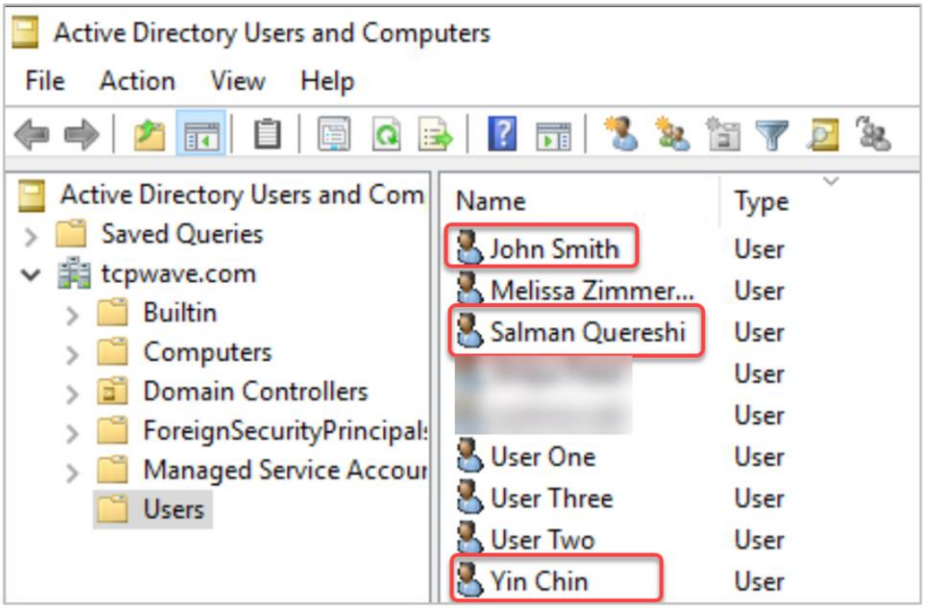
Introduction

Network and security teams are challenged to find the correlation between the users and the network devices. It is a cumbersome task, and organizations look forward to an optimized solution to bridge the gap. The TCPWave's Microsoft Active Users report bridges the gap and provides greater visibility into devices accessing Microsoft-based services. It helps the administrators and the security teams with how network resources are consumed and by whom, thereby providing comprehensive troubleshooting solutions. This white paper provides insights into the TCPWave IPAM – Microsoft Active Users Report.

TCPWave IPAM - Microsoft Active Users Report

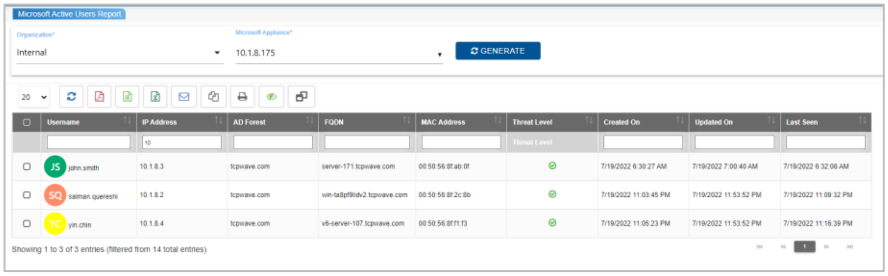
This report provides Active Directory (AD) domain user data whenever the TCPWave appliance is connected to a Microsoft server. Using the report statistics, the network teams can view all the active users currently logged in to AD domain services.

Example: The below screenshot depicts the active users on the Microsoft server:



Name	Type
John Smith	User
Melissa Zimmer...	User
Salman Quereshi	User
[redacted]	User
[redacted]	User
User One	User
User Three	User
User Two	User
Yin Chin	User

To view the active users and their related data in the TCPWave IPAM application, navigate to Reports >> DHCP Reports >> Microsoft Active Users Report.



Organization*: Internal

Microsoft Appliance*: 10.1.8.175

☐	Username	IP Address	AD Forest	FQDN	MAC Address	Threat Level	Created On	Updated On	Last Seen
		10				Threat Level			
☐	JS john.smith	10.1.8.3	tcpwave.com	server-171.tcpwave.com	00:50:56:8f:ab:0f	✓	7/19/2022 6:30:27 AM	7/19/2022 7:00:40 AM	7/19/2022 6:32:08 AM
☐	SQ salman.quereshi	10.1.8.2	tcpwave.com	win-ta8pf9lidv2.tcpwave.com	00:50:56:8f:2c:8b	✓	7/19/2022 11:03:45 PM	7/19/2022 11:53:52 PM	7/19/2022 11:09:32 PM
☐	YC yin.chin	10.1.8.4	tcpwave.com	v6-server-107.tcpwave.com	00:50:56:8f:f1:f3	✓	7/19/2022 11:05:23 PM	7/19/2022 11:53:52 PM	7/19/2022 11:16:39 PM

Showing 1 to 3 of 3 entries (filtered from 14 total entries)

Generating Report

- Select the organization and Microsoft appliance from the respective drop-downs.

  Note: The drop-down contains the Microsoft appliances defined in the TCPWave IPAM.

- Click Generate. The following data is displayed in the grid with the searchable and sortable columns:
  - **User Name**: Displays the name of the user logged into the Microsoft server as a user.
  - **IP Address**: Displays the IP address of the machine the user logged into.
  - **FQDN**: Displays the domain name of the Microsoft server that the user is logged into.
  - **MAC Address**: Displays the MAC address of the client.
  - **Threat Level**: Displays the green icon if the appliance is not malicious. Red indicates that the appliance is malicious.
  - **Created On**: Displays the time stamp of the Microsoft user.
  - **Updated On**: Displays the updated time stamp of the Microsoft user.
  - **Last Seen**: Displays the time the user was last seen active on the Microsoft server.
- To view detailed Identity Mapping data of a particular active user, right-click the icon next to the username. The system displays the IPAM details.

Business Advantages

- Provides the network and security teams greater visibility by relating username information to IP through which they can operate quickly on how to troubleshoot and mitigate the issues using the user-focused approach.
- Provides historical data through which the security teams can zero in on which devices within a network are involved in the security breach.
- With the correlation of user information and IP address, the security teams can identify the user responsible for the compromised account.

Conclusion

Network forensic analysis helps the users in gathering, monitoring, and analyzing the network activities to uncover the source of attacks, viruses, intrusions, or security breaches that occur on a network or in network traffic and respond within a minimal time interval, quickly troubleshoot the issues in the instance of any security breach and make effective decisions to improve the network efficiency. For a quick demo, contact the TCPWave Sales Team.