TransientX

Protecting On-Premises Microsoft Exchange Servers

How TransientAccess Zero Trust Application Access Can Secure Critical Assets in the Data Center

Mar 10, 2021 / #1.0.1_EN

Fully Protect your Microsoft Exchange server with TransientX

An Urgent Problem To Address

On March 3, 2021 the US Government issued a rare directive to mitigate vulnerabilities with on-premises Microsoft Exchange servers because of a widespread hack by a state-sponsored group Microsoft calls Hafnium. With 43% of all Exchange mail accounts managed on-premises, and more than 30,000 servers in the United States alone, the risk of Chinese hackers obtaining invaluable data from these at-risk servers is the new info-pandemic.

The underlying reason why this hack is so widespread is simple: Businesses have cracks in IT infrastructure that permit hackers to violate two key tenets of IT security:

1. **Protect the servers:** Block bad-actors from access to the enterprise data center or private cloud where the apps and data reside.
2. **Protect the data:** Prevent end-users or malware on devices from exfiltrating data.

Hackers have accessed Microsoft Exchange through publicly exposed paths, and back-door breaches have allowed them to access the server directly. To stop both risks, all access to the servers must be controlled. Specifically, unprotected access to these services must be stopped:

- Outlook Web Access (OWA).
- Microsoft Active Sync for mobile access.
- Microsoft MAPI over HTTP access for Outlook to access Exchange.

VPN: You are still at risk

The first answer that may come to mind is to use a VPN. That unfortunately just kicks the can down the road. The VPN limits access to the data center only. However, any infected end-user device then just needs to connect via the VPN to OWA or the Exchange server. At that point, malware will have unfettered access.

ZTNA: You could still be exposed

Many zero trust access services have arisen to limit user devices to only access designated servers. Said differently, if a user device uses Zero-Trust Network Access (ZTNA) and their infected device is accessing an application other than Exchange, they will not be able to reach Exchange and infect the server. This is fine if the user is not using Outlook or OWA. If they are, once Outlook attempts to access Exchange, most ZTNA solutions will treat this as a legitimate access request and open the path to Exchange. Then, malware on the device will likewise have a clear path to Exchange!

TransientX: The only zero-trust solution to prevent Microsoft Exchange Server infections

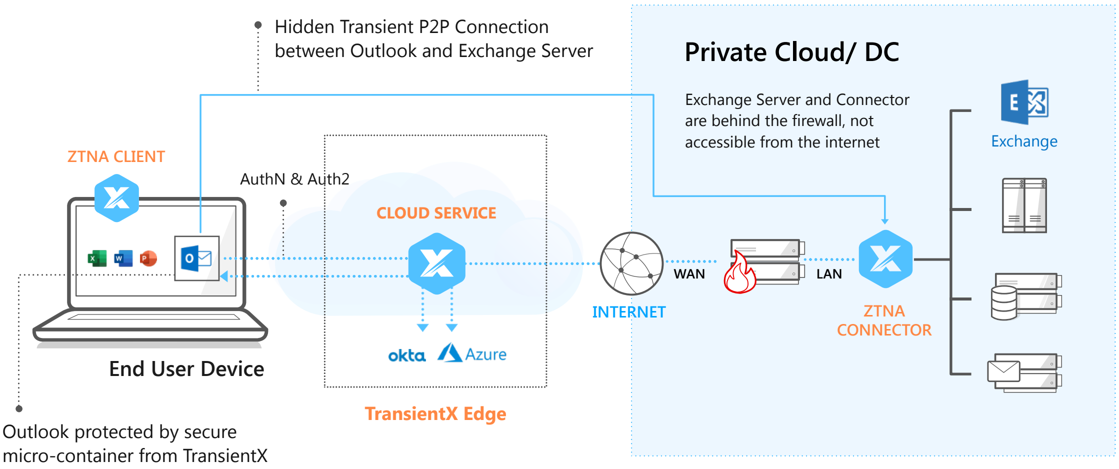
The only fool-proof way to protect enterprise-managed on-premises Microsoft Exchange servers is via TransientAccess, the next-generation Zero Trust Application Access solution from TransientX.

TransientAccess delivers three distinct capabilities to prevent malware from ever reaching the Exchange server, for all access methods:

- **Hide the Exchange Server:** The server IP addresses, and DNS names are never published or visible. The TransientAccess virtual network dynamically maps virtual addresses to the real address, with different mappings per user and per server. Malware looking for these servers cannot find them because they are camouflaged. By preventing this potential east-west traversal, malware is blocked from attacking the servers.

- **Connect the app to the Exchange server:** TransientAccess is unique in the market in its ability to securely wrap any application, including browsers and Outlook, in an isolated workspace to limit its available network destinations. Therefore, malware cannot reach the enterprise data center without infecting Outlook itself, or the browser directly.

- **Secure the browser and Outlook from malware:** The TransientAccess secure micro-container protects applications from malware. When the user activates their browser to reach OWA, or uses Outlook, the secure micro-container prevents malware from affecting the application. This means that as long as the browser or Outlook are protected by TransientAccess, malware cannot reach or infect Exchange servers.


Hidden Transient P2P Connection between Outlook and Exchange Server
Private Cloud/ DC
Exchange Server and Connector are behind the firewall, not accessible from the internet
Exchange
ZTNA CLIENT
AuthN & Auth2
CLOUD SERVICE
INTERNET
WAN
LAN
ZTNA CONNECTOR
okta
Azure
End User Device
TransientX Edge
Outlook protected by secure micro-container from TransientX

Below is a comparison between VPN, basic ZTNA, and TransientAccess:

	VPN	Zero Trust Network Access	Transient- Zero Trust Application Access
Protect Data Center and cloud	Yes	Yes	Yes
Controlled Access		Yes	Yes
Prevent Malware from accessing Exchange			Yes
Prevent users from copying, downloading data			Yes

Visit www.transientx.com for more on zero-trust network access
or get TransientAccess for free at https://transientx.com/pricing.html .