

Enabling Business Continuity without Compromising on Security

Avishag Daniely
Director of Product Management

May 2020

Today's Reality



- Sudden need for support remote work at scale
- Entirely new setup for some organizations
- Others have existing capabilities facing unprecedented demands

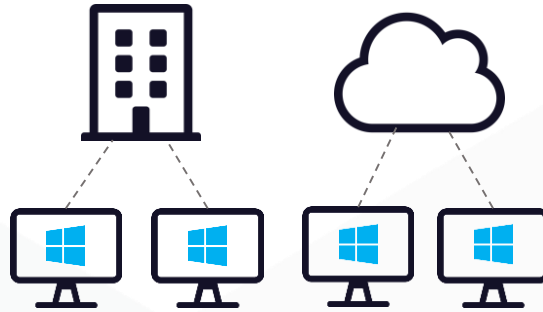
Effective Segmentation to Secure Remote Access

Avishag Daniely
Director of Product Management

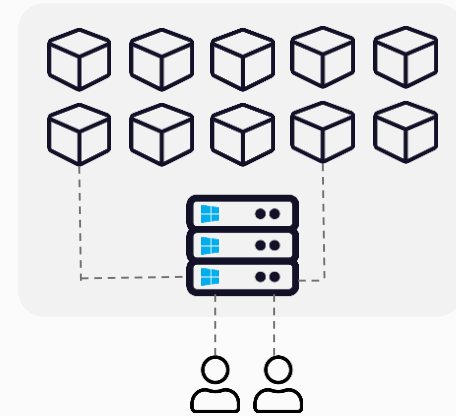
How Companies are Dealing with Today's Reality



**Endpoints with
VPN Connections**

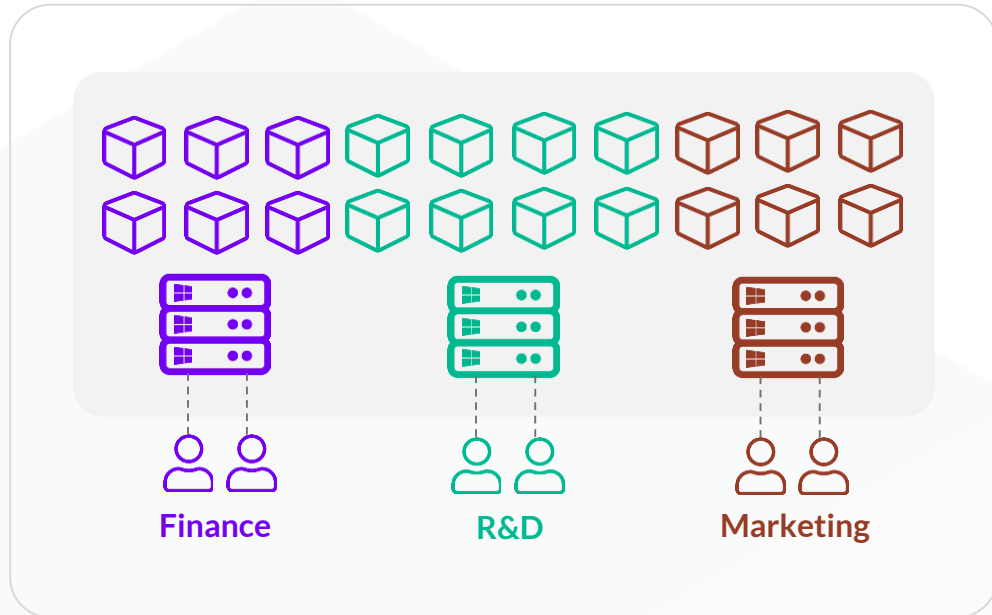
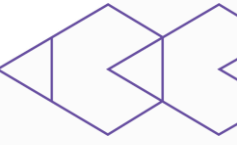


VDI or DaaS



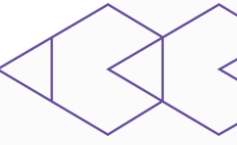
**Jumpboxes &
Terminal Servers**

Traditional Security Methods



1. Separate remote access servers / networks for each group
2. Complex remote access firewall rules
3. Multiple applications / servers per user group
4. Complex internal firewall rules

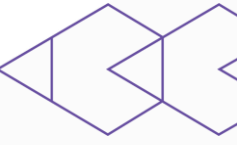
High Costs for Proper Security



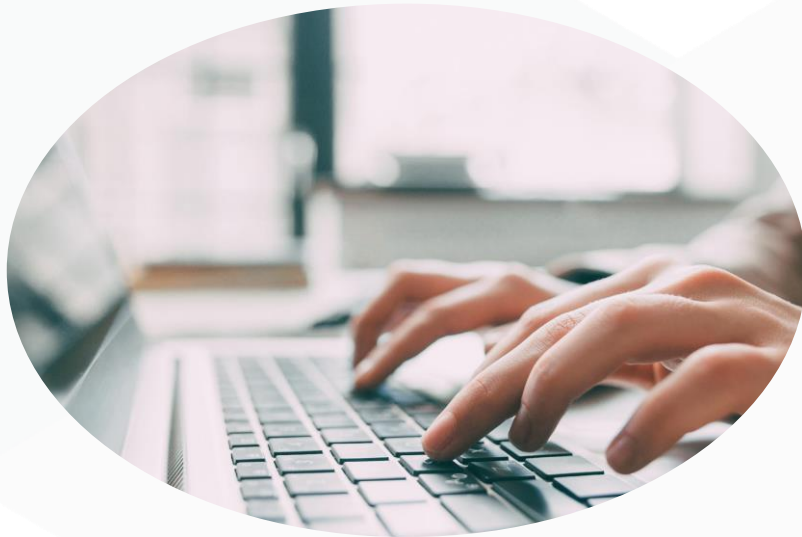
- Over-provisioning of server hardware
- High level of operational burden on IT and security teams



Inevitable Compromises That Increase Risk



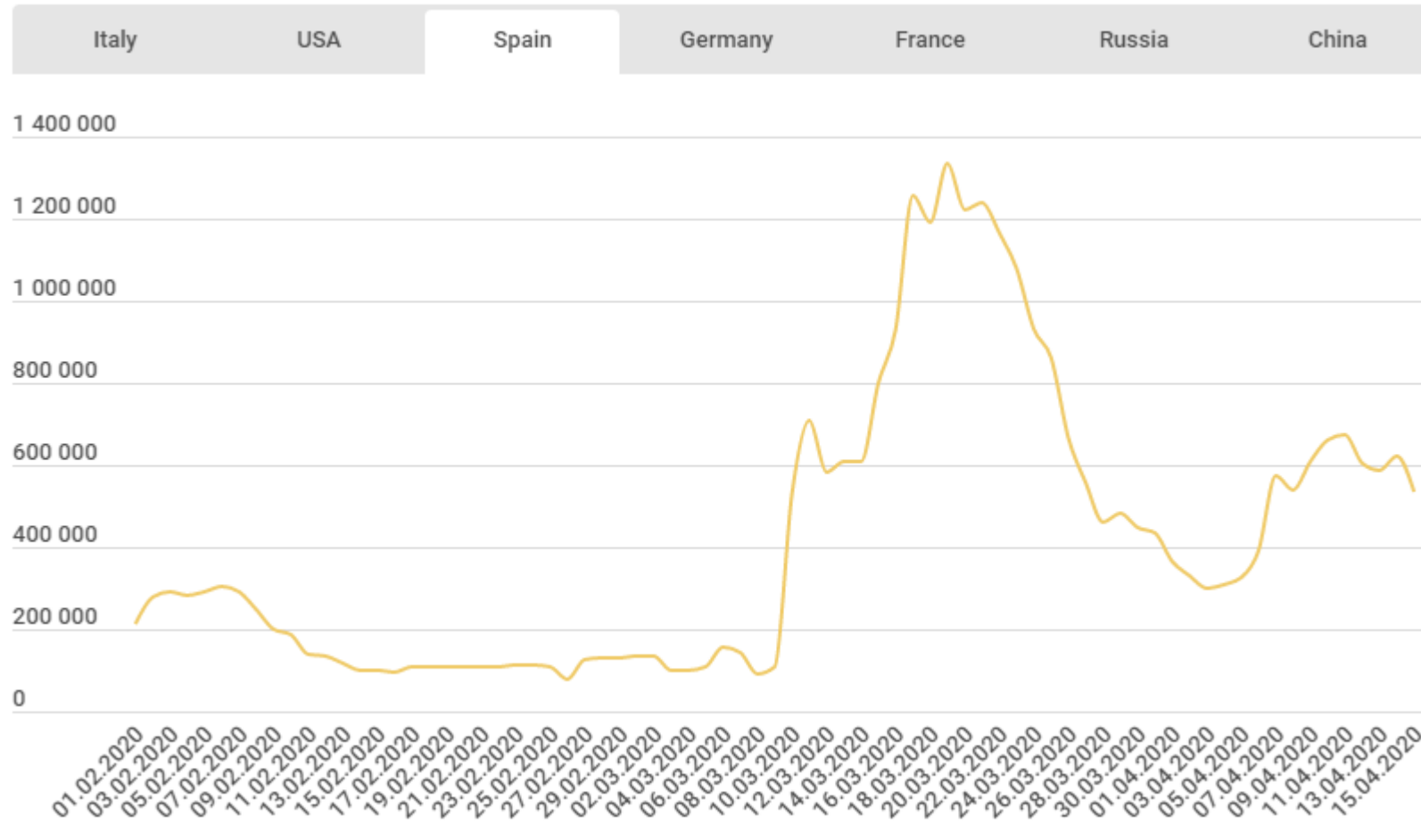
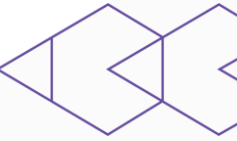
- “One size fits all” access privileges
- Blind spots: Limited visibility and control
- Bypassing security controls such as firewalls



Risk:

Humans are the weakest link

Rise of RDP Brute Force Attacks - Recent Days



* Source: [Kaspersky labs](#)

VPN Compromises

- CVE-2019-11510
- Arbitrary file reading vulnerability affecting Pulse Secure VPN appliances— enables attackers to gain access to victim networks
- Published April 16 2020

Pulse Secure System **Authentication** Administrators Users Maintenance Wizards

Auth Servers > secure > Settings

Settings

Base Configuration

- Name: CISA-Test-local Label to reference this server
- Domain: CISA-Test NetBIOS name of the domain
- Kerberos Realm: cisa-test.local Specifies the Kerberos realm of the Active Directory domain. It is usually set to the DNS name of the Active Directory domain. Example "xyz.net", "abc.com"

Domain Join Configuration

- Username: administrator Active Directory administrator credentials are required in order for the Pulse Connect Secure to join the domain or whenever cer
- Password:
 Save credentials If this setting is not enabled, the credentials entered will be destroyed after successfully joining the domain.
- Container Name: Computers Container path in Active Directory to create the machine account in. Changing this field will trigger domain rejoin. In the case of
- Computer Name: pulse2 Machine account name (do not include '\$')

Domain Join Status: ●

[Update Join Status](#) [Reset Join](#)

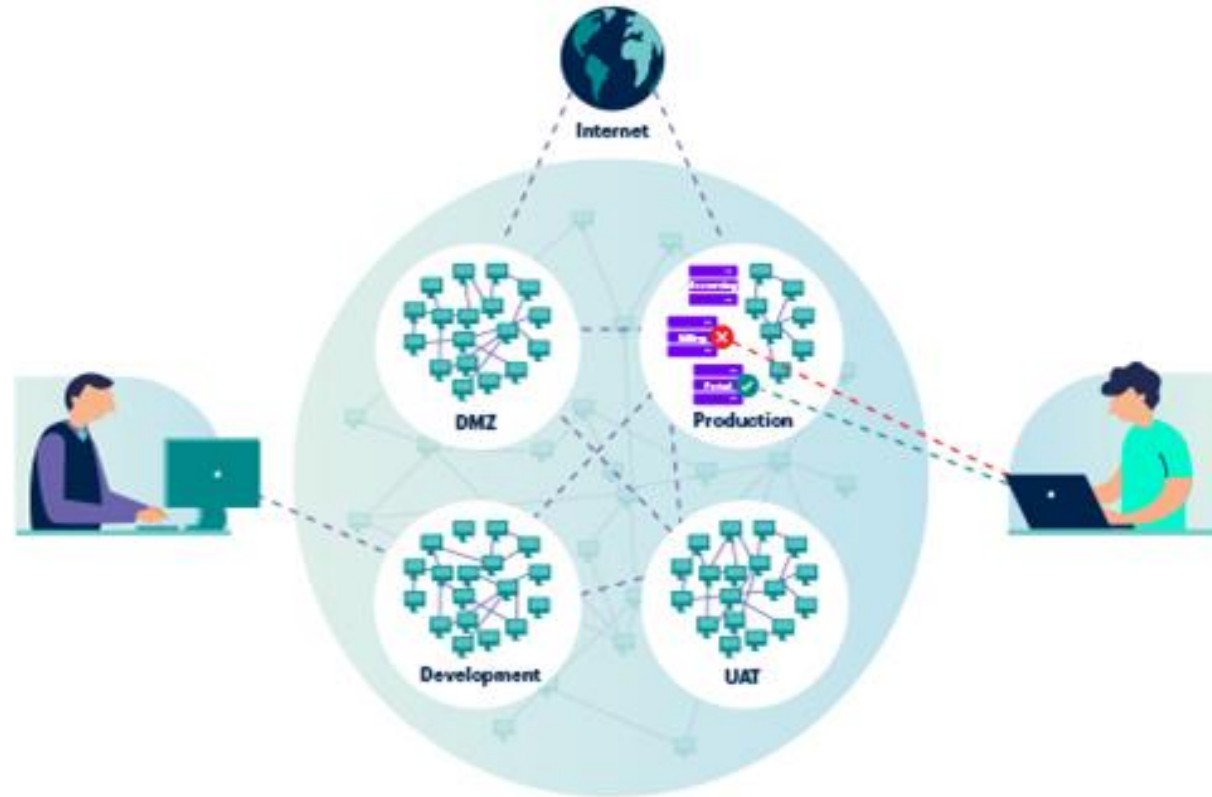
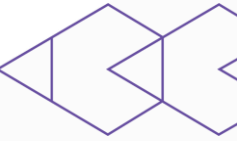
Click "Update Join" to get the latest join status of node(s). If any node's domain join status is other than GREEN (persistently) then click "Reset Join" button of that node to reinitiate domain join process. NOTE: reinitiating the join process ensure that it is not caused by network issues. If domain join status is shown RED due to network issues then it has high chances of coming back to GREEN after network recovers.

[Caspersky labs](#)

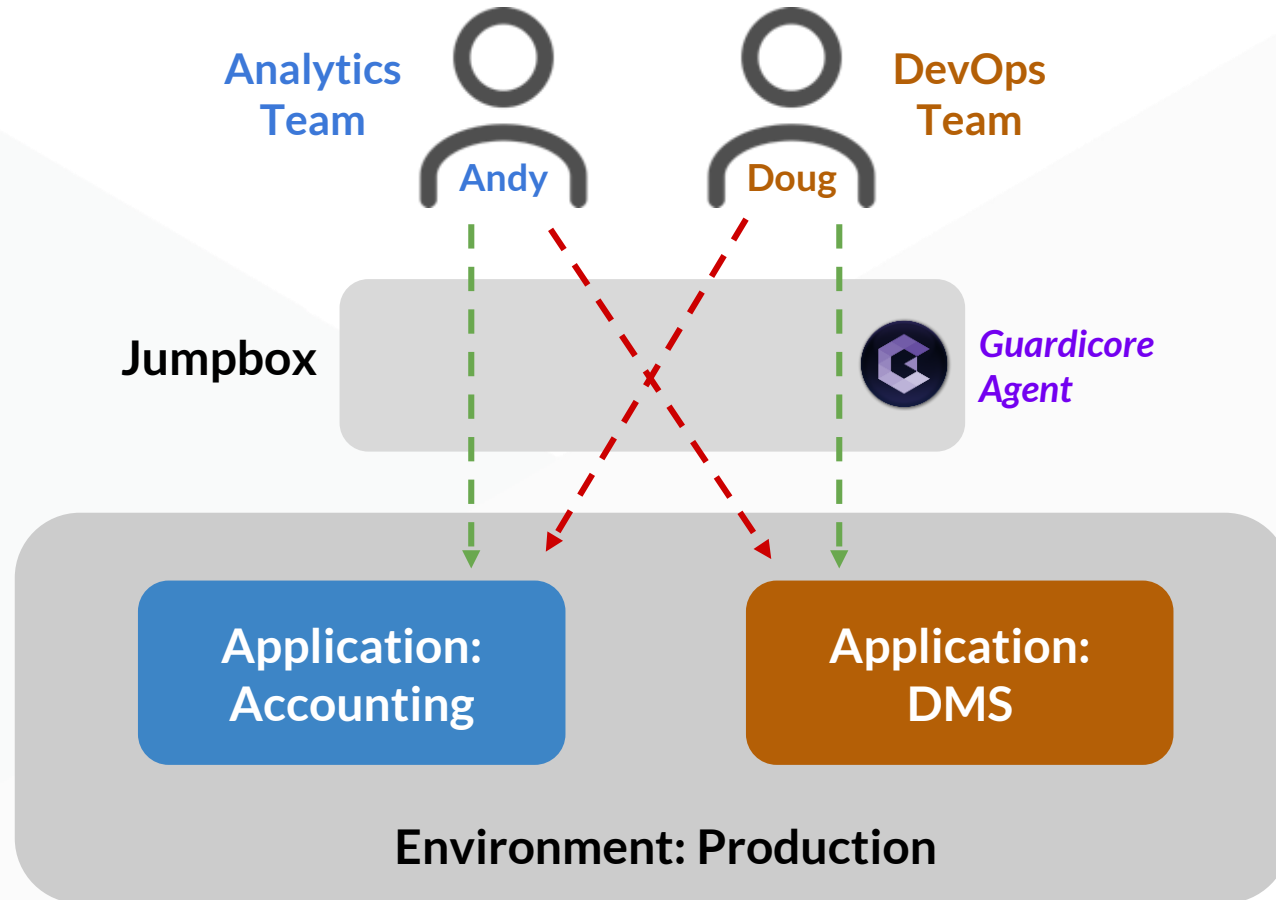
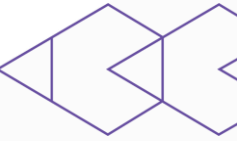
What's Needed

- Apply least privilege to remote access
- Workload-centric segmentation
- Enable business continuity
- Avoid downtime
- Avoid network changes
- Gain visibility into user access activity
- Ensure speed / timeliness
- Scale reliably and cost-effectively

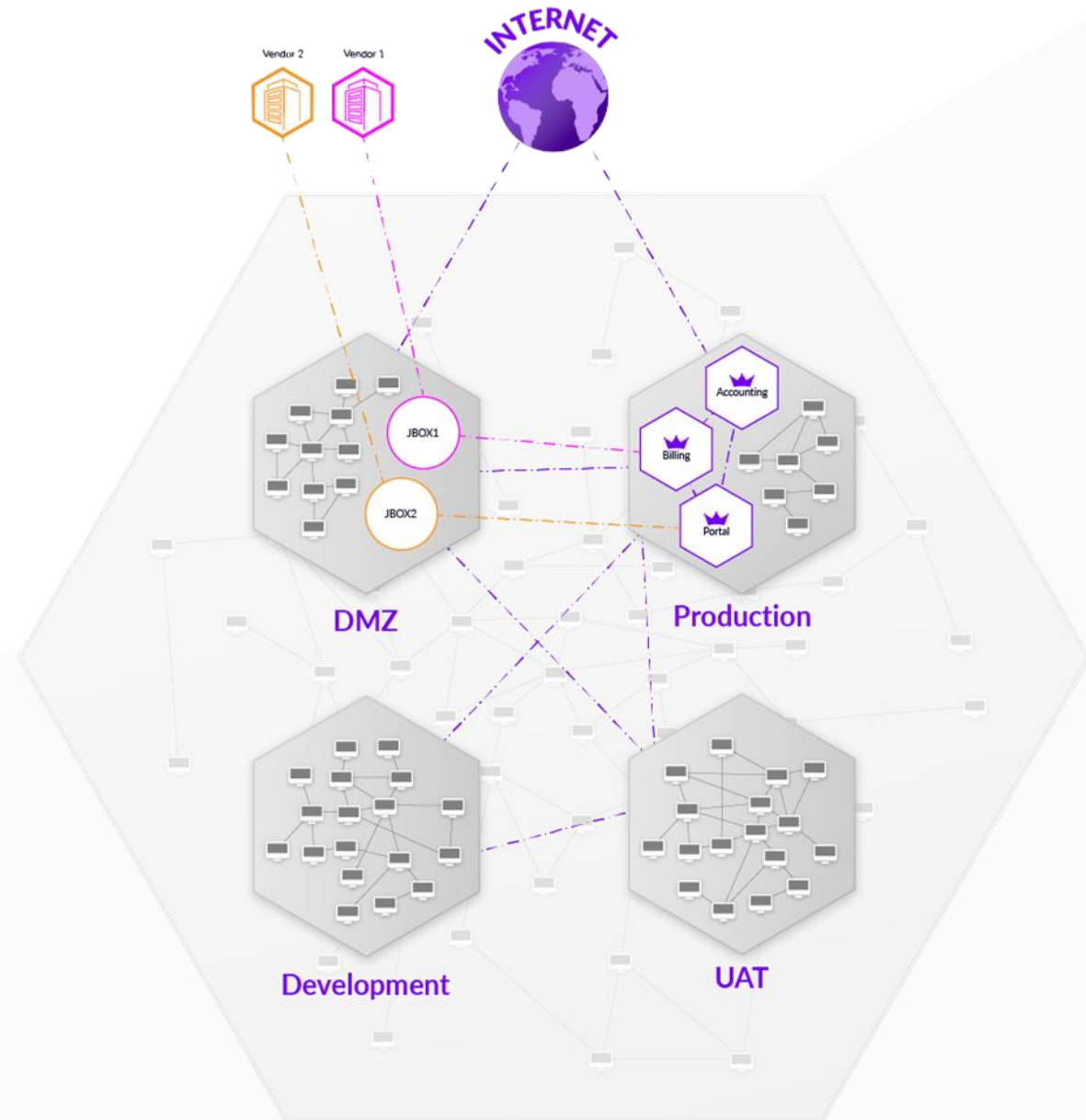
Visualize and Control User Access Anywhere



Securing Access Based on User Identity



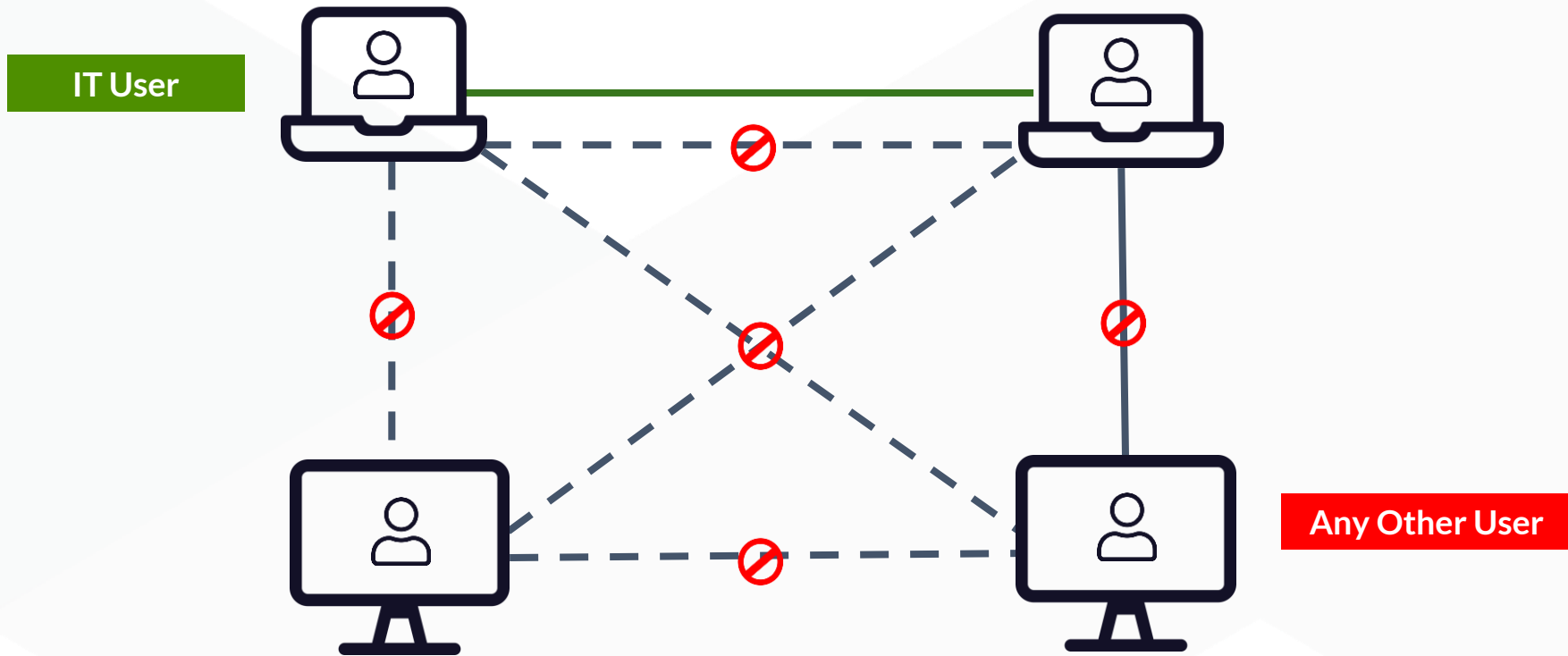
Third-Party Access Control



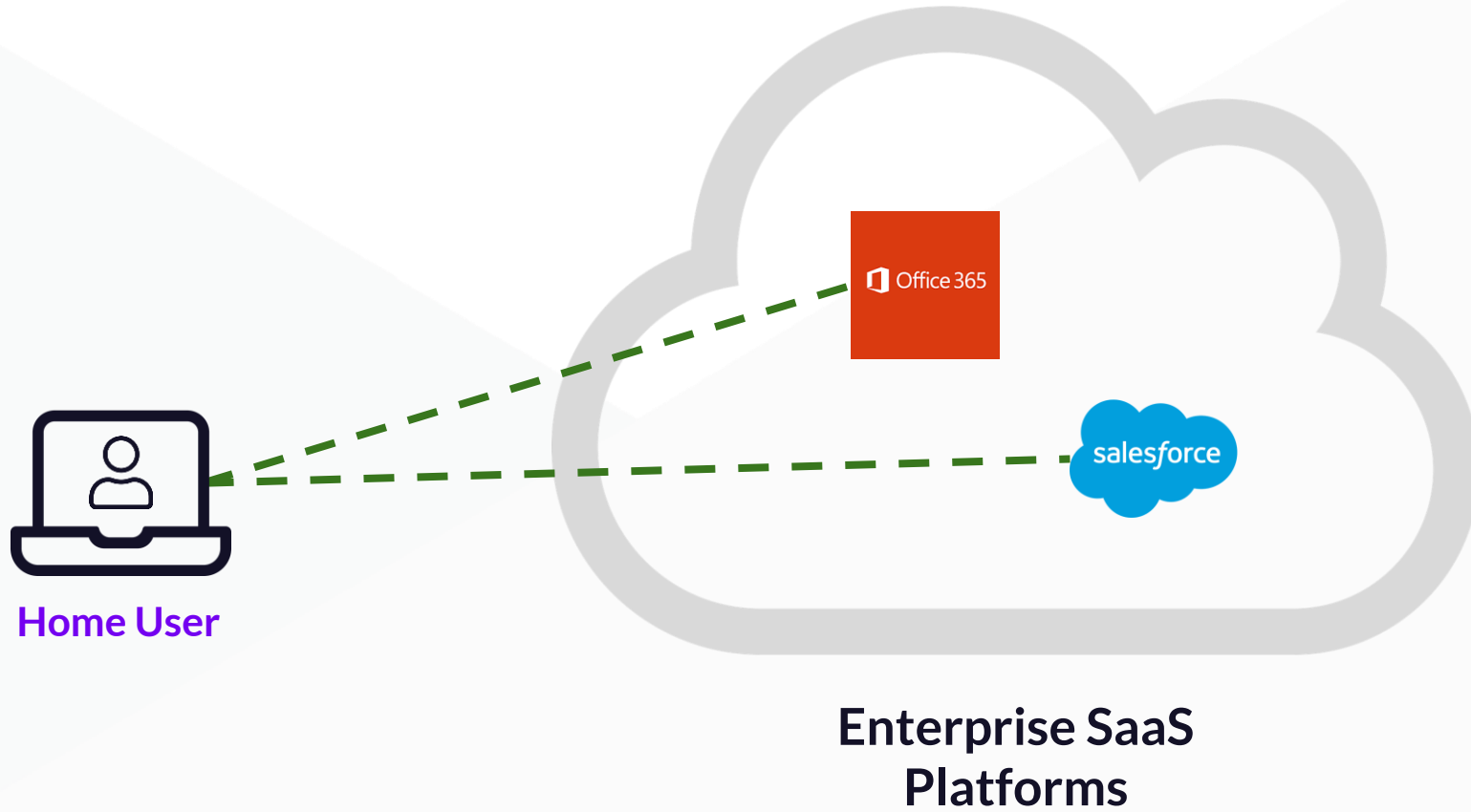
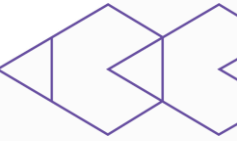
Peer-to-Peer Isolation



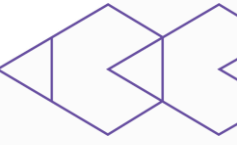
Example: Block all connections between peers except for privileged users



Whitelist External Connections



Segmentation that accounts for the user's identity



Benefits

1. Risk Reduction
2. Controls user access from a single pane of glass
3. Simpler to implement
4. Flexible policy engine
5. Visibility
6. Lower costs

Contact us

Twitter: @Guardicore

Web: guardicore.com

[Request a Demo](#)