Guardicore

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

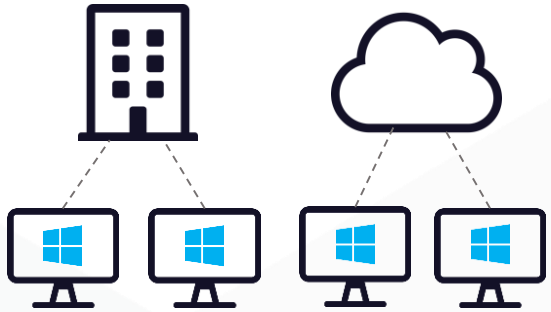
Effective Segmentation to Secure Remote Access

Avishag Daniely
Director of Product Management

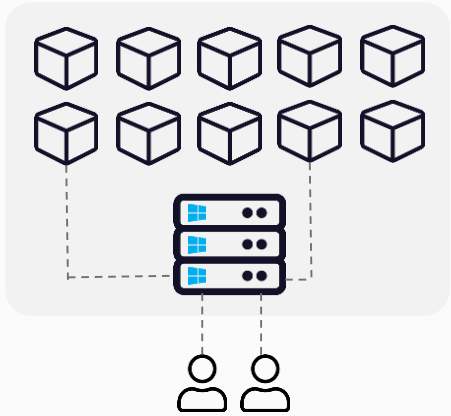
Guardicore

How Companies are Dealing with Today's Reality

Endpoints with VPN Connections



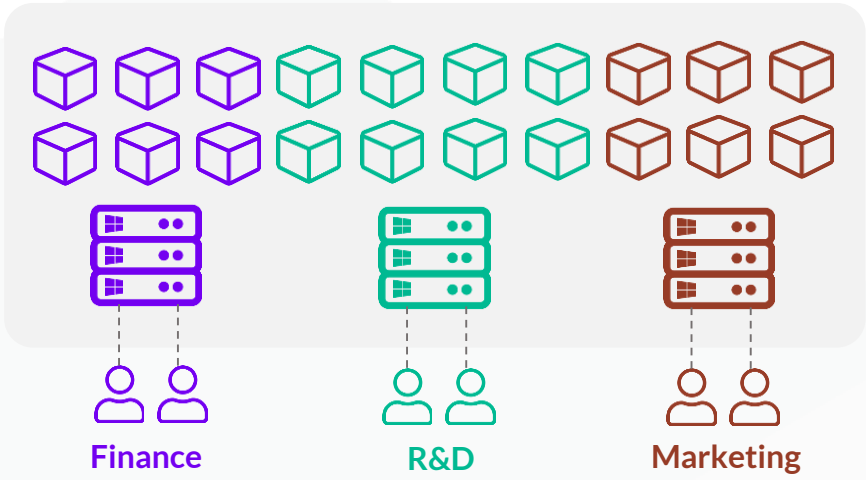
VDI or DaaS



Jumpboxes & Terminal Servers

Guardicore

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

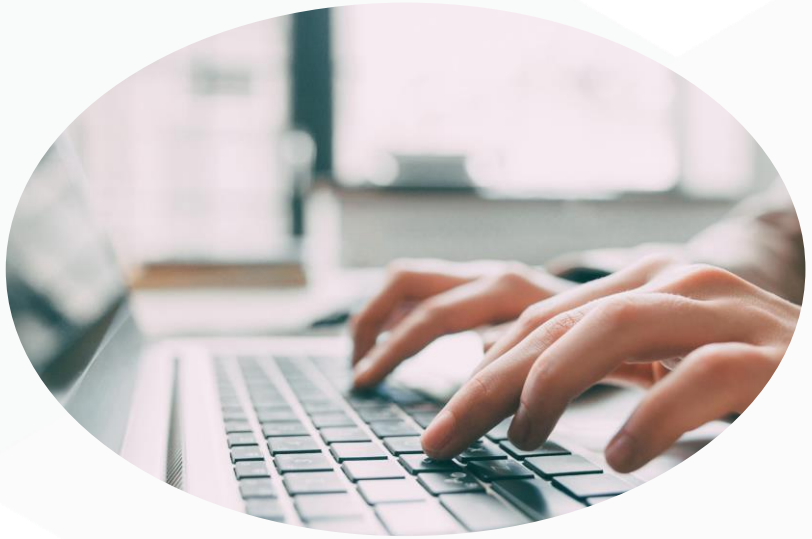
Guardicore

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

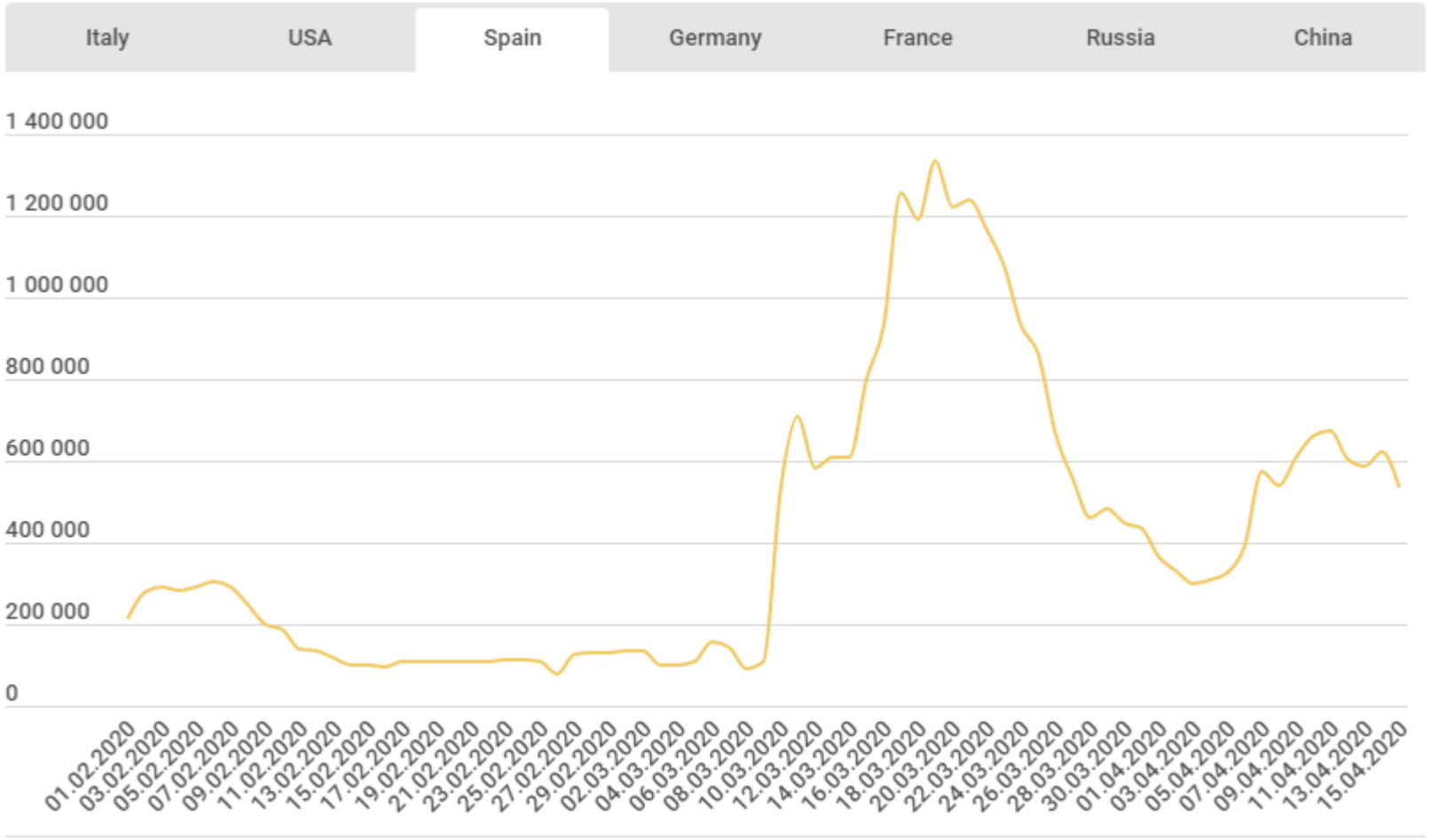
- “One size fits all” access privileges
- Blind spots: Limited visibility and control
- Bypassing security controls such as firewalls



Risk:

Humans are the weakest link

Rise of RDP Brute Force Attacks - Recent Days

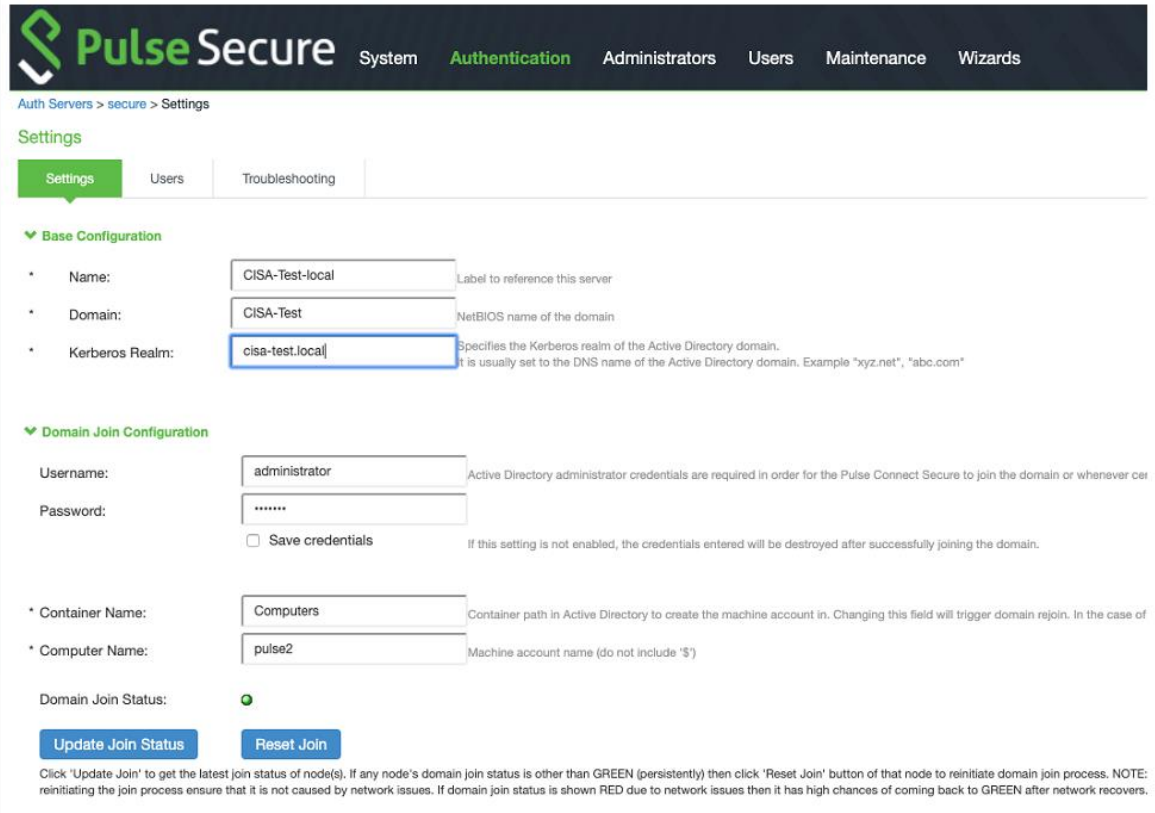


* Source: Kaspersky labs

Guardicore

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



Kaspersky labs

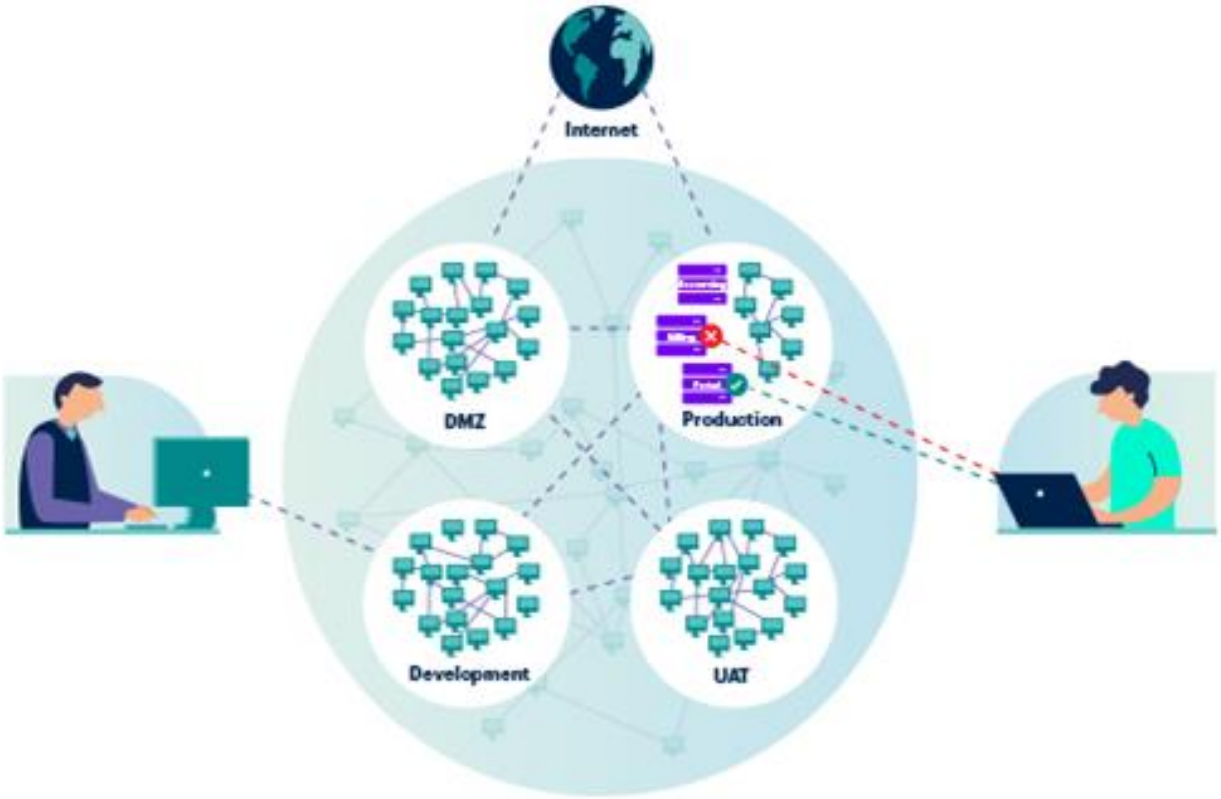
Guardicore

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

Use Case 1

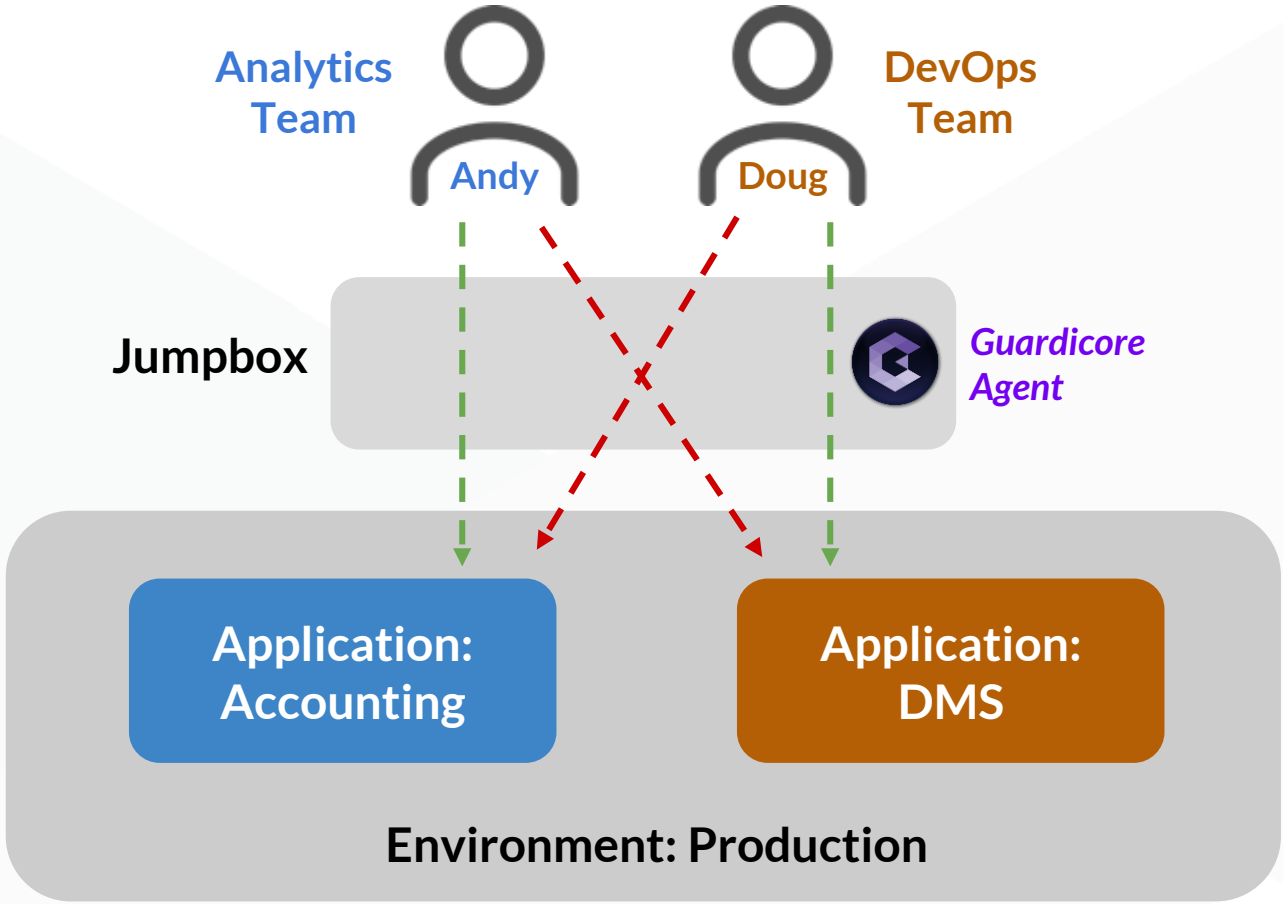
Visualize and Control User Access Anywhere



Guardicore

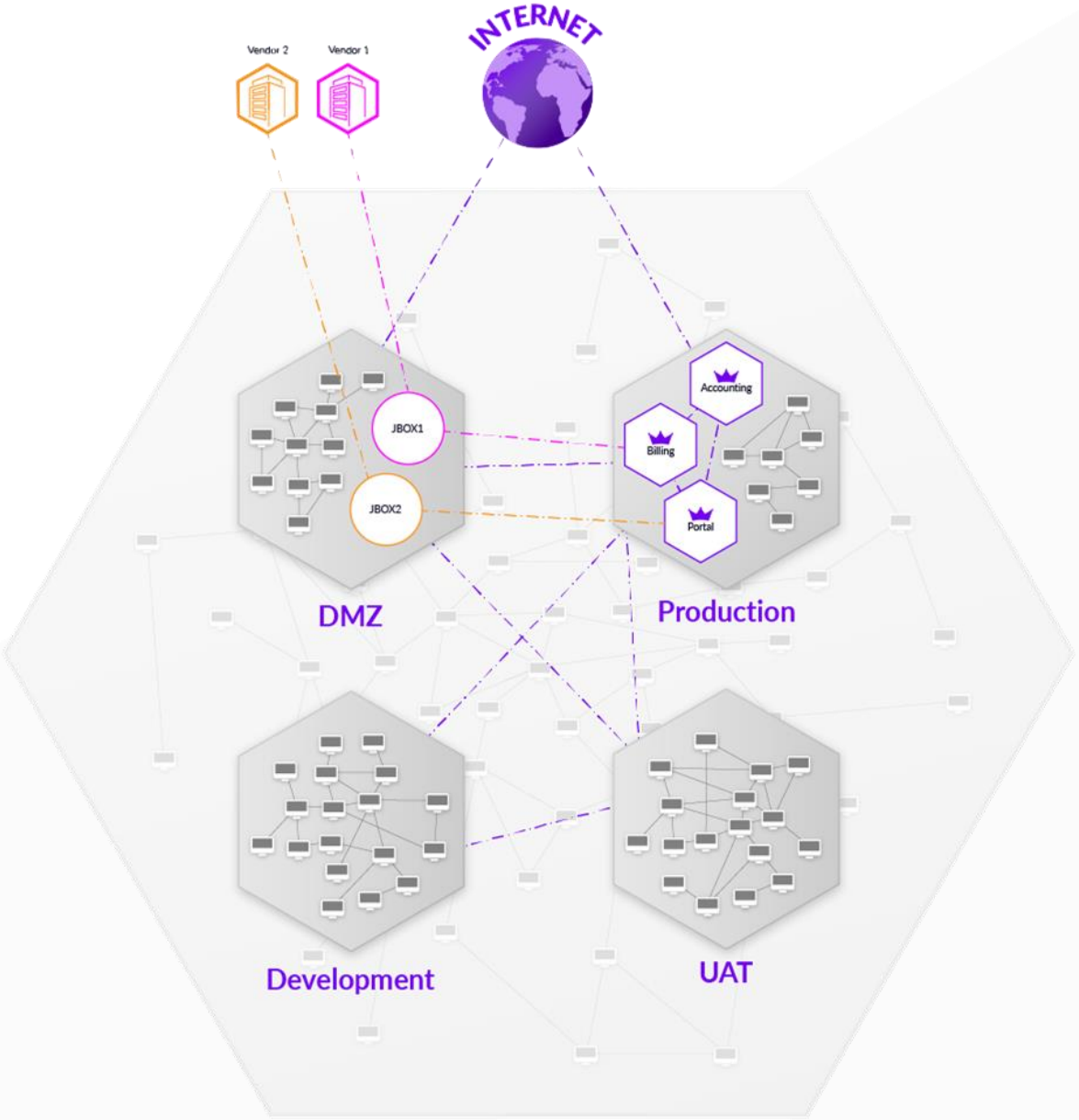
Use Case 2

Securing Access Based on User Identity



Guardicore

Third-Party Access Control

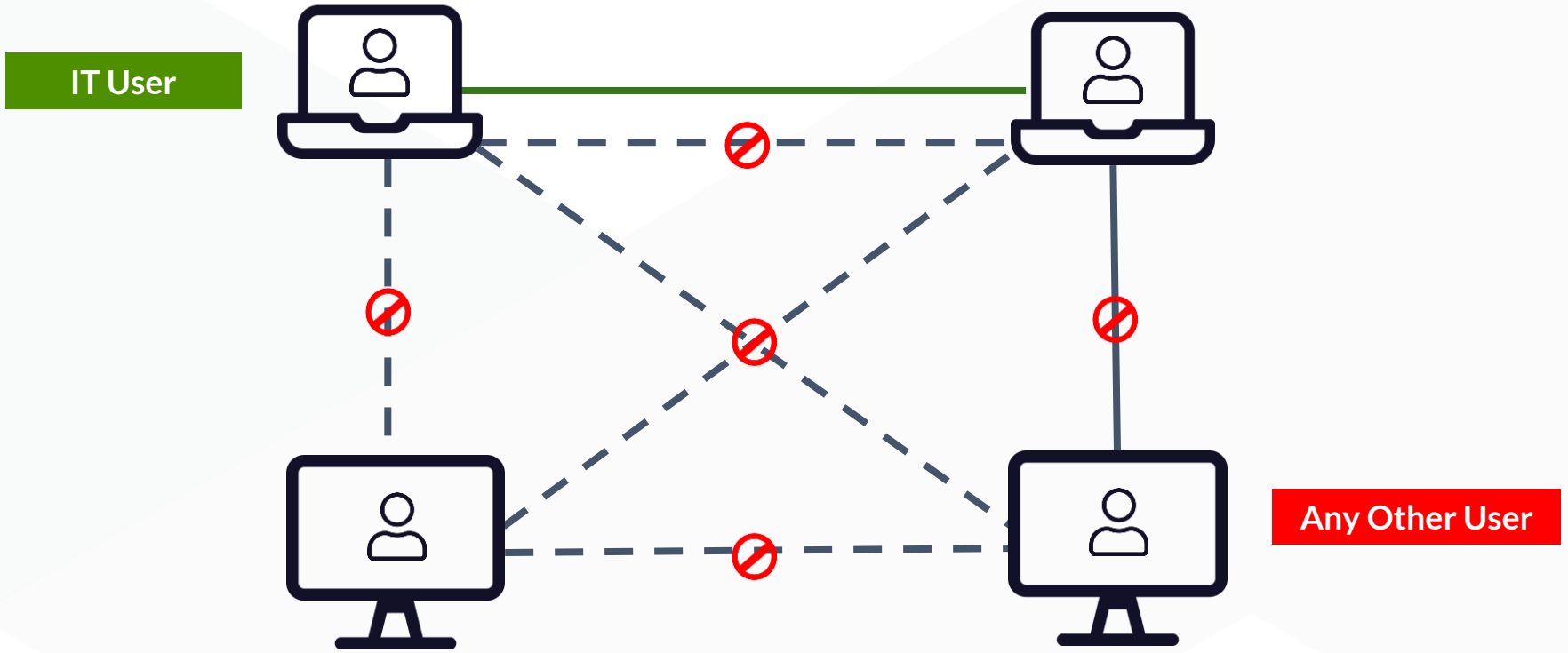


Guardicore

Use Case 4

Peer-to-Peer Isolation

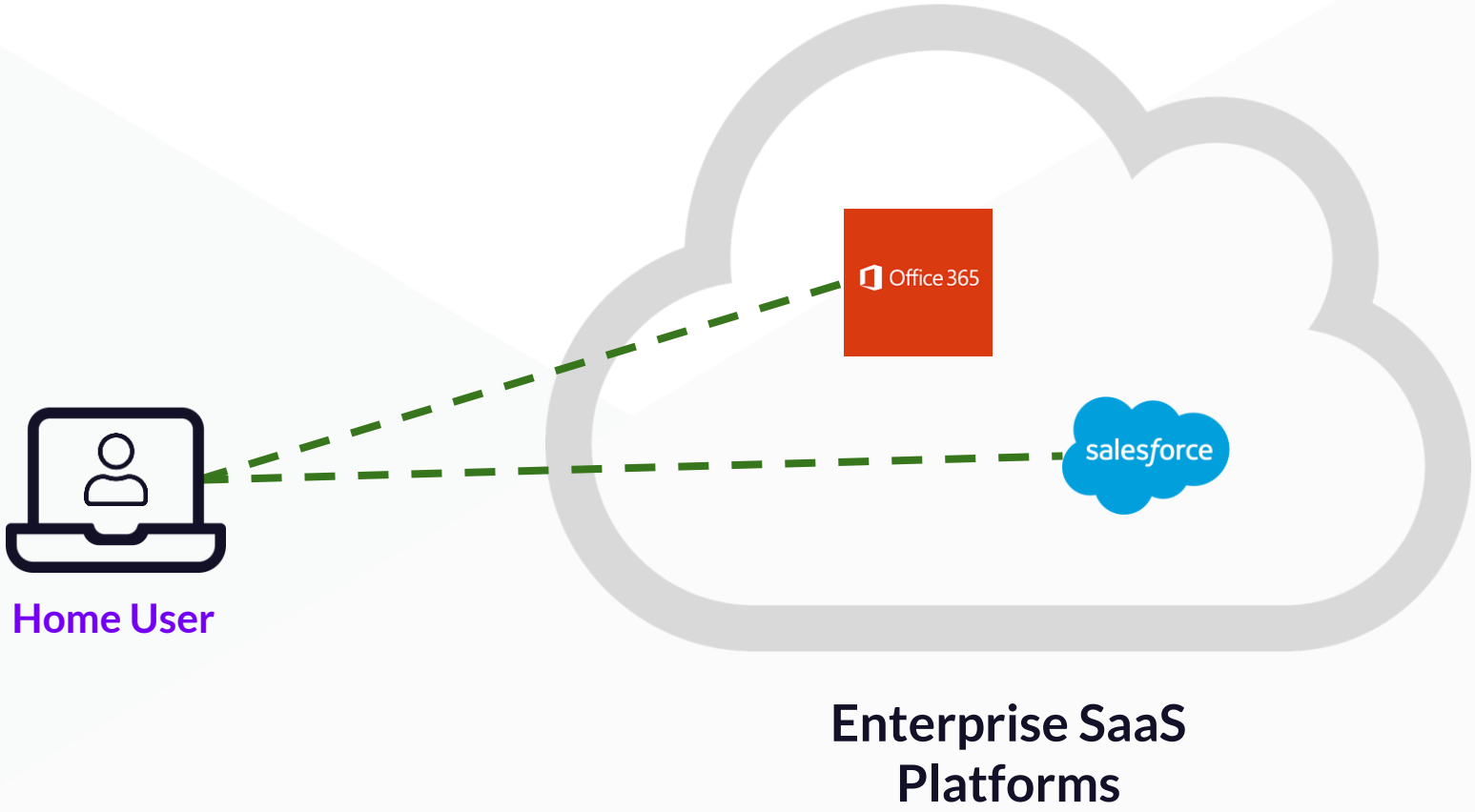
Example: Block all connections between peers except for privileged users



Guardicore

Use Case 5

Whitelist External Connections



Guardicore

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