



Secure Workspaces Anywhere with Citrix and Guardicore

Add Visibility and Control to Virtual Desktop Infrastructure

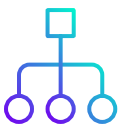
Remote workers are increasingly relying on Virtual Apps and Desktops (also known as VDI) environments to ensure business continuity and enable WFH, but security outside of the traditional perimeter is complex. In such an environment, end user machines cannot be physically separated from other servers, either inside the data center or the cloud, giving users a dangerous amount of access to sensitive data and applications.

Use Cases for Citrix with Guardicore Centra:



Remote working

Allow employees to work from home without adding to the enterprise risk, even considering unknown factors such as BYOD.



Peer-to-peer isolation

Create silos from the same machine or account, enabling security over advanced use cases such as remote support or control.



Enforce rules for supply chain

Control third-party access for vendors, providers or administrators, limiting access to what's necessary.



Endpoint protection for roaming users

Allow remote workers to access enterprise resources in the cloud or on premises from changed locations enforcing different security policies based on location profile.



Key Benefits

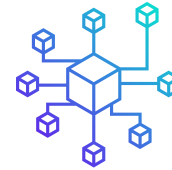
- ◆ **Holistic Security and Control**
Protect across all Citrix environments, as well as on-premises deployments, hybrid and multi-cloud, containers, and serverless.
- ◆ **Limit Risk to Critical Applications**
Ring-fence digital crown jewels with precise policy that tightly controls exposure and adds security where it matters most.
- ◆ **Control Lateral Movement**
Restrict an attacker's ability to move from the VDI environment to elsewhere in the data center, reducing the attack surface.
- ◆ **Accelerate Compliance**
Ensure that sensitive data is protected at rest and in transit, and that only those who need to have access, do.
- ◆ **Work Towards a Zero Trust Model**
Each user accesses only what they need for their role, even when sharing a machine, dramatically reducing risk and exposure.
- ◆ **Reduce Infrastructure Costs**
Eliminate the need for multiple jump boxes or servers for various use cases, replacing heavy CAPEX with software-defined segmentation.

Guardicore Centra with Citrix, anywhere: Limiting access to only what an individual user needs, and no further



Complete Visibility

- ◆ Accurately visualize Virtual Apps and Desktops communication and flows in real-time, as part of the entire dynamic hybrid IT ecosystem.
- ◆ Discover and map communication over all Citrix environments, Citrix Virtual Apps and Desktops service, Citrix Virtual Desktops (XenDesktop), Citrix Virtual Apps (XenApp), Citrix Virtual Apps and Desktops service on Azure
- ◆ Access a map of all communications and flows, down to the individual user and even at the process level, (Layer 7), seeing exactly how to create effective policies.



Granular Security

- ◆ Create tight segmentation policies that follow the workload, isolating applications, users, data and critical systems.
- ◆ Enforce access down to the specific user level, segmenting activity that originates from the same jump box or machine.
- ◆ Create secure zones that have no impact on business continuity, working towards a zero trust access model that doesn't impede remote working.
- ◆ Support all on-premises and cloud scenarios, including multi-user workloads.

Reduce risk with holistic security:
www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.