



## User Identity Access Management

### An Additional Critical Layer of Control for Modern Hybrid Data Centers

[Get in touch to schedule a demo](#)

Reducing the attack surface for today's IT environments is about more than just creating tight controls around specific applications, ring fencing them away from harm. This is a great first step, and can certainly help with some use cases such as breach containment or compliance. However, without User Identity Access Management, your organization has a blind spot that includes every single person that uses or enters your network.

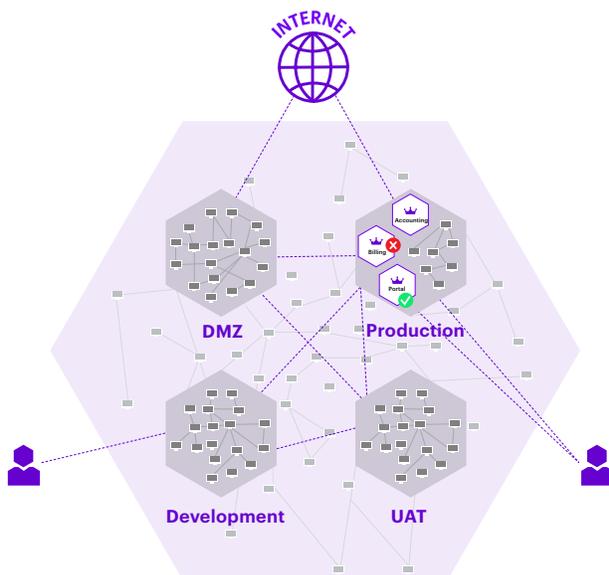
Once application segmentation is in place, the next essential step is to create policy around who can access these applications, ensuring that these are just as watertight on any and all architecture across your network.

### Meet any User Identity Access Use Case

#### Manage User Access

Using an Active Directory User Group, Centra controls user access to any application or workload, from any environment. Specific user groups have access to specific servers, over specific ports or processes, while others do not. User groups have their own permissions, while all other access can be blocked. With no need for a centralized firewall, you can use granular access control between workloads on specific segments of the network.

#### User Access Control

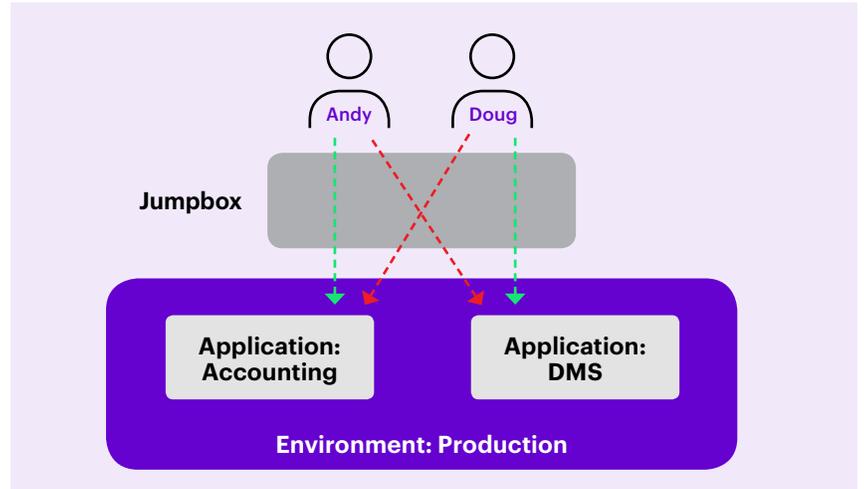


## Guardicore Centra User Identity Access Management

- ▶ **Control User Access Anywhere:**  
Policies work across laptops, desktops, VDI, virtual or bare-metal servers, and cloud infrastructure.
- ▶ **Software-defined Segmentation:**  
No network or architecture changes, no cables, no server downtime, and no reboot of systems.
- ▶ **Quick and Powerful:**  
Policies are simple and intuitive to create, and take effect on both new and active sessions immediately.
- ▶ **Cost-effective:**  
Compared to similar use cases met with traditional jumpbox infrastructure, costs have been shown to be up to 60% less.

### Handle Simultaneous User Access

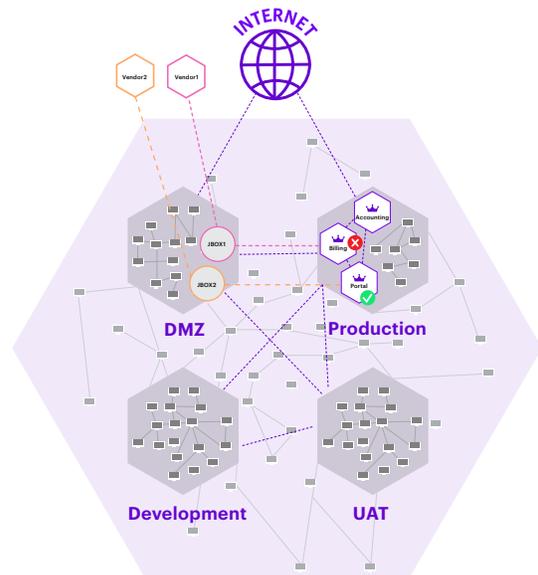
Admins can access different applications through the same Jumpbox or terminal server, even when they are logged on at the same time. All the while, disparate policies will work seamlessly, allowing one user to access what they have rights to, while the other will remain blocked, with no disruption to either's own service or access.



### Control Third-Party Access

Based on user identity, Guardicore Centra can control third-party access management, for example from external vendors or SaaS providers. With the help of user groups, each third-party connection can have its own access policies defined for both the data center and specific applications, allowing permissions to what the user needs for their own role, and nothing more.

### 3rd Party Access Control



## About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.

[www.guardicore.com](http://www.guardicore.com)

Together, Application Segmentation and User Identity Access Management is the strongest one-two punch to protect a modern enterprise data center.

*Want to learn more about how they work in tandem?  
Get in touch to speak to one of our experts.*