AKAMAI SOLUTION BRIEF

User Identity Access Management with Segmentation

An additional critical layer of control for modern hybrid data centers

Reducing the attack surface for today's IT environments is about more than just creating tight controls around specific applications, ringfencing 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 a segmentation solution that supports user identity access management, your organization has a security blind spot that includes every single person that uses or enters your network.

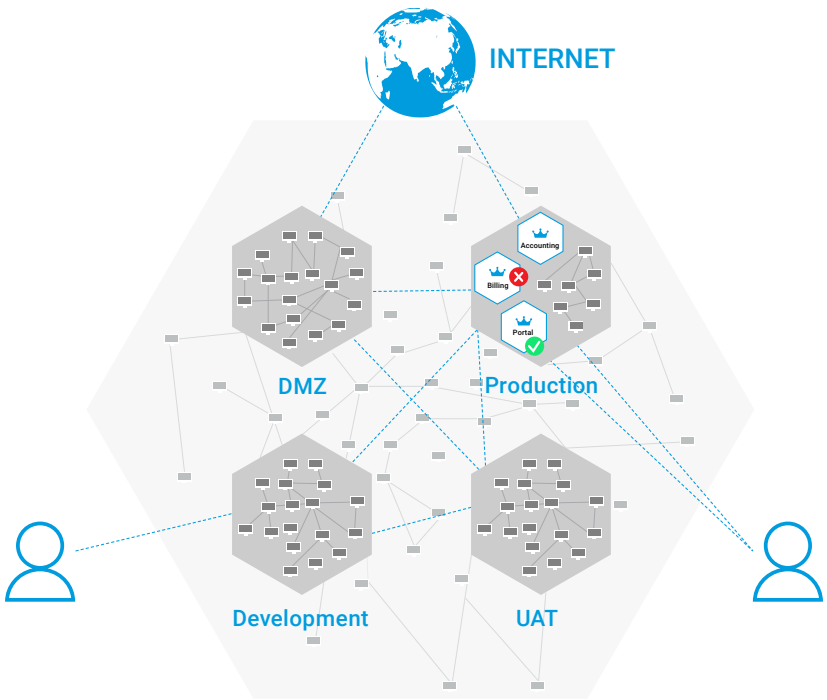
Once application segmentation is in place, the next essential step is to leverage your segmentation solution to create policy around who can access these applications, ensuring that these are just as secure on any and all architecture across your network.

Use cases: Segmentation for user identity access

Manage user access

Using an Active Directory user group, Akamai Guardicore Segmentation can control 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



Why segmentation for user access control?

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

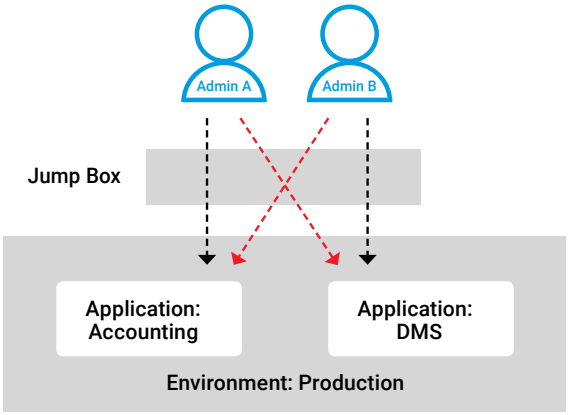
Quick and powerful
Policies are simple and intuitive to create, and take effect on both new and active sessions immediately

Cost-effective
Compared with similar use cases met with traditional jump box infrastructure, costs have been shown to be up to 60% less

Akamai

Handle simultaneous user access

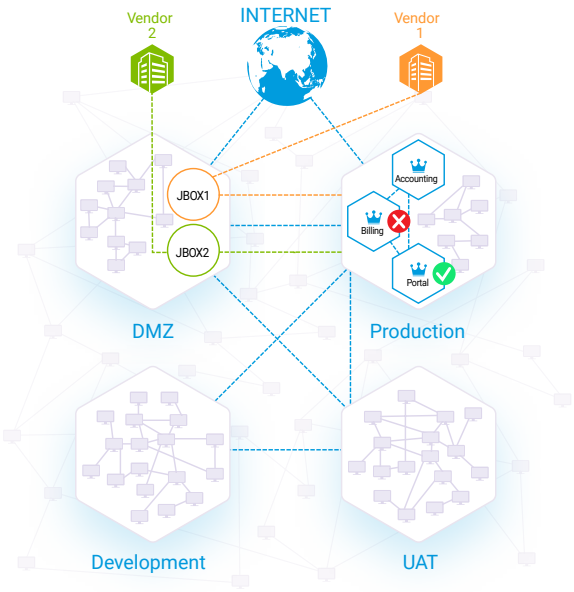
Admins can access different applications through the same jump box or terminal server, even when they are logged on at the same time. All the while, disparate policies will work seamlessly, allowing one user to access what they have rights to, while the other will remain blocked, with no disruption to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



Control third-party access

Based on user identity, Akamai Guardicore Segmentation 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.

Third-party access control



Together, application segmentation and user identity access management deliver the strongest one-two punch to protect the modern enterprise data center.

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

Published 06/23