Controlling User-to-Application Connectivity

SECURING VDI ENVIRONMENTS WITH THE ILLUMIO ADAPTIVE SECURITY PLATFORM (ASP)™

Deploying VDI in the core of the data center—as well as its role in enabling remote access for users—makes it a prime target for bad agents. Hackers can leverage remote connectivity to find and exploit vulnerabilities in the VDI environment or launch account hacking attempts to gain unauthorized access to virtual desktops.

Access to applications within the VDI plant is typically unrestricted, so once a hacker gains access to the VDI environment, he or she can connect to and attack any end point inside the data center. Further, all users permitted to connect to the virtual desktop environment also have the ability to connect to any end point inside the data center, which exposes data center applications to internal threats.

Illumio ASP leverages adaptive segmentation to massively reduce the surface area of attack available to bad actors and internal threats.

Before Illumio	After Illumio
VDI users are allowed to connect to any application within the data center—relying on authentication as the only means of protecting against unauthorized access.	Adaptive User Segmentation adds a layer of protection before a user can even log in to an application. It does this by blocking connectivity to unauthorized applications based on a user's identity—and without the network.
Applications are compromised if a user relies on a weak password, or a malicious actor gets access to a user's credentials.	Enterprises gain an added layer of control before authentication, thereby reducing exposure of key business assets and applications to bad actors.
Controlling user access to applications requires significant network reconfigurations.	Adaptive User Segmentation relies on Microsoft Active Directory as the source of truth around what applications a user is allowed to access, as well as to determine connectivity entitlements.

Secure Virtual Desktops with Illumio ASP

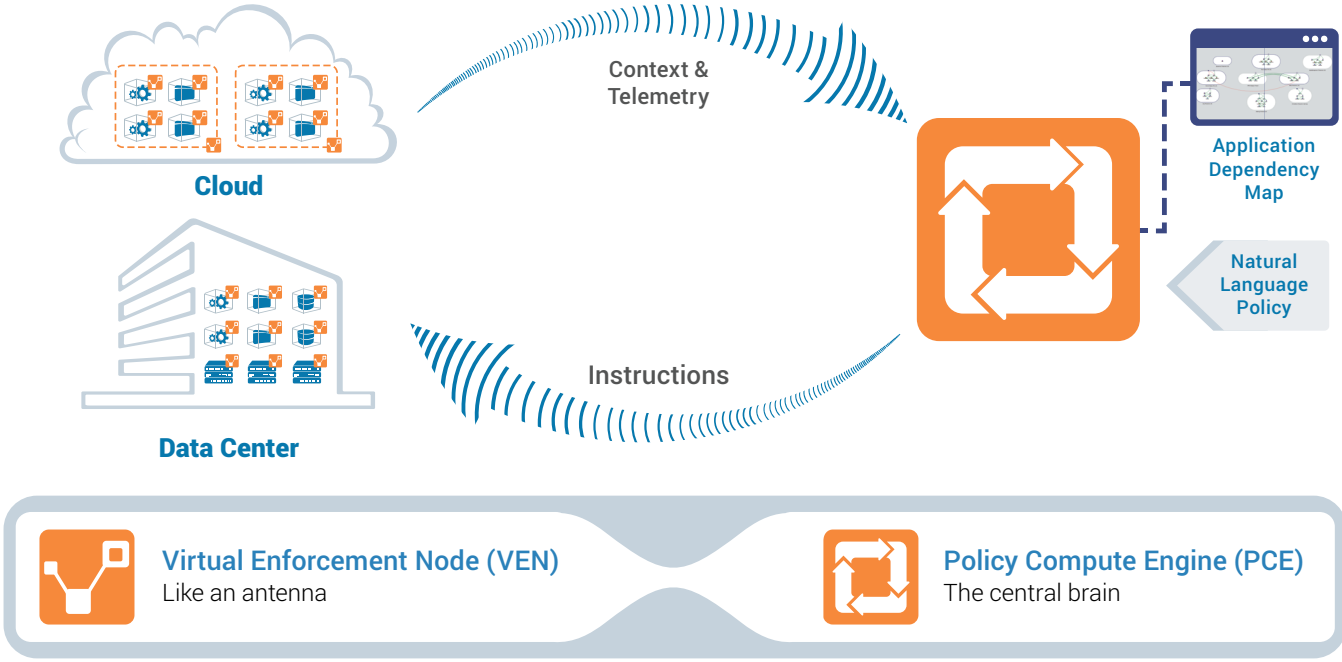
Control which applications a VDI user can communicate with.

- **Uses the user's identity, not IP address.** By examining who the user is at the time that he or she logs in, policies can be dynamically created and enforced without any reliance on the underlying network—while still allowing administrators to use dynamic IP address assignment.
- **Integrates with Microsoft Active Directory.** As users are added to existing groups, or new groups are added into Active Directory, policies are dynamically updated. This ensures there is a single source of truth around user entitlements.
- **Integrates with VDI.** Ensures that connectivity restrictions can be enforced in the VDI plant, a level of control that was previously unavailable.

Feature	Benefits
Enforcement at the host	■ Does not rely on changing the underlying network ■ Provides real-time feedback if a user changes IP addresses or moves
Microsoft Active Directory integration	■ Does not rely on changing the underlying network ■ Provides real-time feedback if a user changes IP addresses or moves
Reduced attack surface	■ Massively reduces the opportunities for bad actors to access sensitive applications

TECHNICAL DETAILS

The Illumio ASP architecture consists of lightweight Virtual Enforcement Nodes (VENs) installed on workloads residing in any data center or cloud. The VENs act as antennas and send telemetry information about the workloads to a Policy Compute Engine (PCE) that acts as the central brain of the platform. The PCE builds a graph of all dependencies between workloads and their applications and computes precise security policies that are instrumented into the native security capabilities (iptables or Windows Filtering Platform) in every workload. Anytime applications or environments change, Illumio ASP automatically adapts by recomputing and updating the policies.



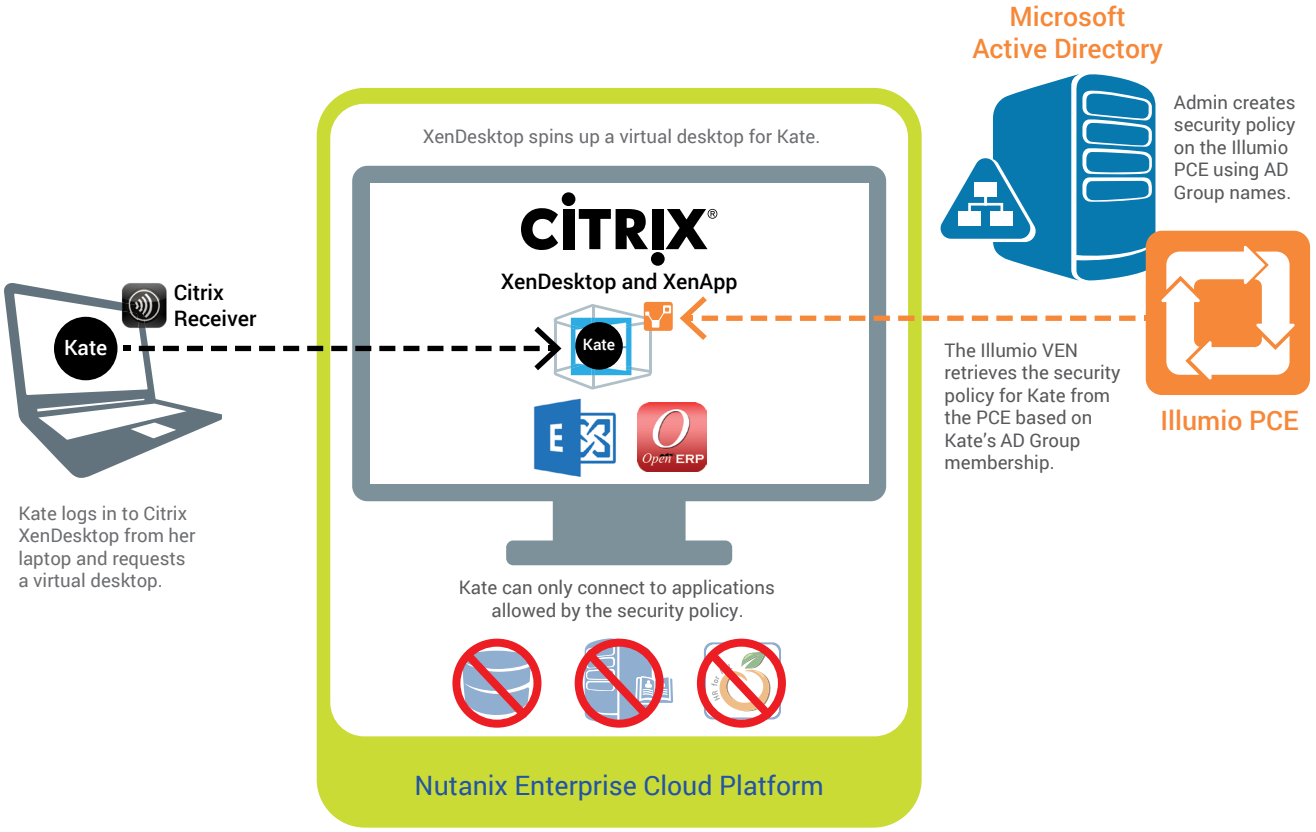
For Adaptive User Segmentation, a script is run against one of the Active Directory servers within the customer's infrastructure, which imports the organization's Active Directory groups into the PCE via its REST API. (Note: nothing needs to be installed on the Active Directory server.

Administrators define a set of default policies such as: "VDI hosts can use domain controllers, DNS, DHCP, and Internet proxies." The PCE turns that natural-language policy into a set of instructions that are used on every VDI host.

The VEN is installed into the guest Operating System and enforces the default policy. If a user were to look at the policy on any given VDI host, it would show that the host was allowed to talk to the IP address(es) of domain controllers, DNS servers, DHCP servers, and proxies.

When a user logs in to the host, the VEN checks his or her group membership, then requests the specific policy for that user from the PCE. The PCE then sends the additional, user-specific policies back down to the host where they are received by the VEN and added into the workload.

Whenever a user locks or logs out of the workstation, the default policy is restored.



Validated Solution

Illumio ASP has been verified as Citrix Ready® for XenDesktop and XenApp. The Citrix Ready program helps customers identify third-party solutions that are recommended to enhance virtualization, networking, and cloud computing solutions from Citrix Systems, Inc. Illumio completed a rigorous verification process to ensure Adaptive User Segmentation works with XenDesktop and XenApp, providing confidence in joint solution compatibility.

The combined virtual desktop and security solution is also fully validated to work on the Nutanix Xtreme Computing Platform (XCP), with full support for Nutanix Acropolis Hypervisor (AHV), VMware vSphere, and Microsoft Hyper-V environments. With Illumio's successful validation for Citrix XenDesktop and XenApp in place, customers and solution partners can deploy a fully secured, massively scalable, and radically simple virtual desktop environment.

illumio + CITRIX® + NUTANIX™

CITRIX Ready

NUTANIX READY • AHV •

GET STARTED TODAY

Technical resources on Illumio's architecture and quick-start guides for deployment in a range of environments are available at www.illumio.com/resources. Illumio offers a wide range of services around design, deployment, and optimization, as well as custom services tailored to customer requirements. For more information about Illumio ASP and how it can be used to control user-to-application connectivity, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve environmental separation, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com