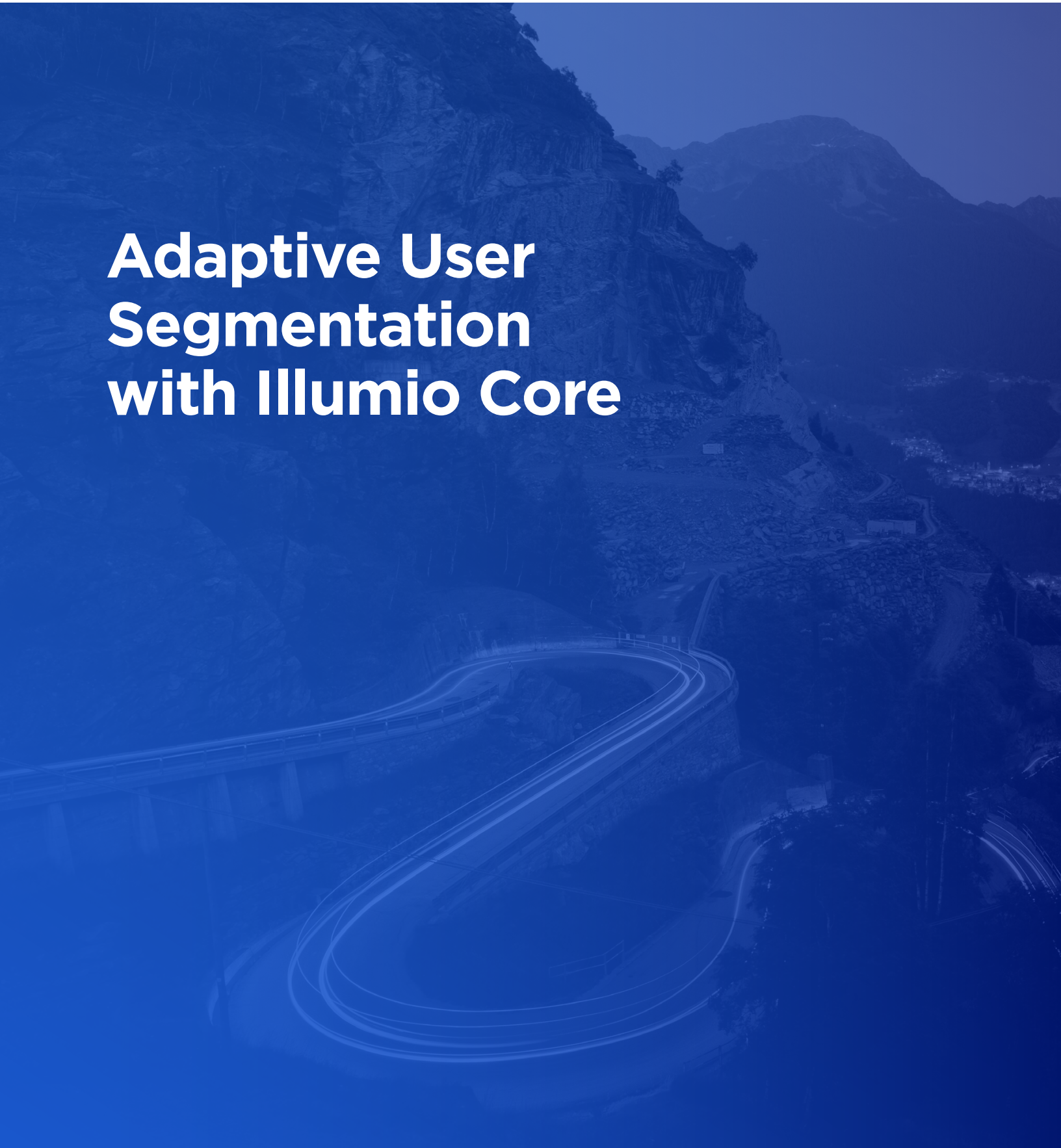
illumio

SOLUTION BRIEF

Adaptive User Segmentation with Illumio Core



Illumio Core™ integrates with Microsoft Active Directory group memberships to control which applications a VDI user can communicate with, thereby massively reducing the surface area of attack available to bad actors and internal threats. Organizations have deployed desktop virtualization for a variety of reasons including security, IT costs, and application control. Many of these organizations have deployed their VDI plants within their data center. User access of applications from VDI is typically unrestricted, which exposes data center applications to 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.
If a user relies on a weak password, or a malicious actor gets access to a user's credentials, then the application is compromised.	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, but rather than solely being used for authentication, Active Directory is also used to determine connectivity entitlements.

Adaptive User Segmentation

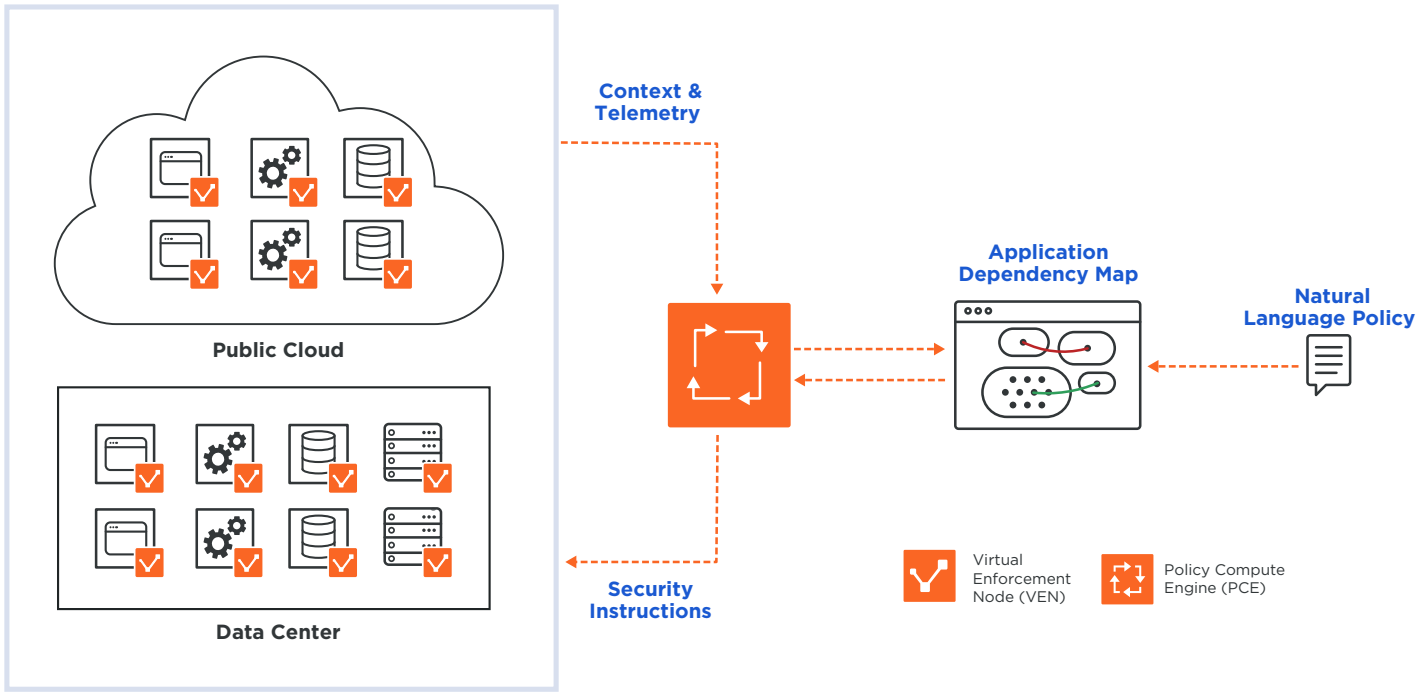
- **Uses the user's identity,** not IP address. By examining who the user is at the time that he or she logs in, policies can be dynamically created and enforced without any reliance on the underlying network while still allowing administrators to use dynamic IP address assignment.
- **Integrates with Microsoft Active Directory.** As users are added to existing groups, or new groups are added into Active Directory, policies are dynamically updated. This ensures that 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.

illumio

Feature	Benefit
Enforcement at the host	• Does not rely on changing the underlying network • Provides real-time feedback if a user changes IP addresses or moves
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

The Illumio Core 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 Core automatically adapts by recomputing and updating the policies.

ILLUMIO CORE ARCHITECTURE



illumio

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.)

Assets like domain controllers, DNS servers, and DHCP servers can have VENs installed on them, or they can be added into the PCE as unmanaged workloads.

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.

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 Core 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.

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.