



IGEL + Leostream Joint Solution Brief

Executive Summary

- IGEL Adaptive Secure Endpoint Platform™ and Leostream® Remote Desktop Access Platform create a trusted endpoint-to-workspace access model for hybrid, cloud, physical, and GPU-enabled environments.
- IGEL provides the immutable, trusted, and governed endpoint layer; Leostream provides centralized authentication, policy-driven brokering, workspace assignment, session orchestration, and secure gateway access.
- The combined design helps organizations improve security, strengthen resilience, and reduce operational costs while preserving choice across compute platforms, display protocols, and workspace architectures.
- A browser-first access pattern through the Leostream Gateway provides a practical path for secure remote access from IGEL OS™ endpoints, while protocol-specific clients can be used where they are available and validated for the target workflow.

The Market Challenge

Modern workspace strategies are becoming more distributed and more specialized. At the same time engineers, geoscientists, researchers, designers, analysts, and other high-performance users may need access to physical workstations, virtual desktops, GPU-backed cloud resources, or high-performance compute environments. IT teams must deliver that access without creating a new security gap at the endpoint or locking the organization into a single infrastructure, cloud, or display protocol.

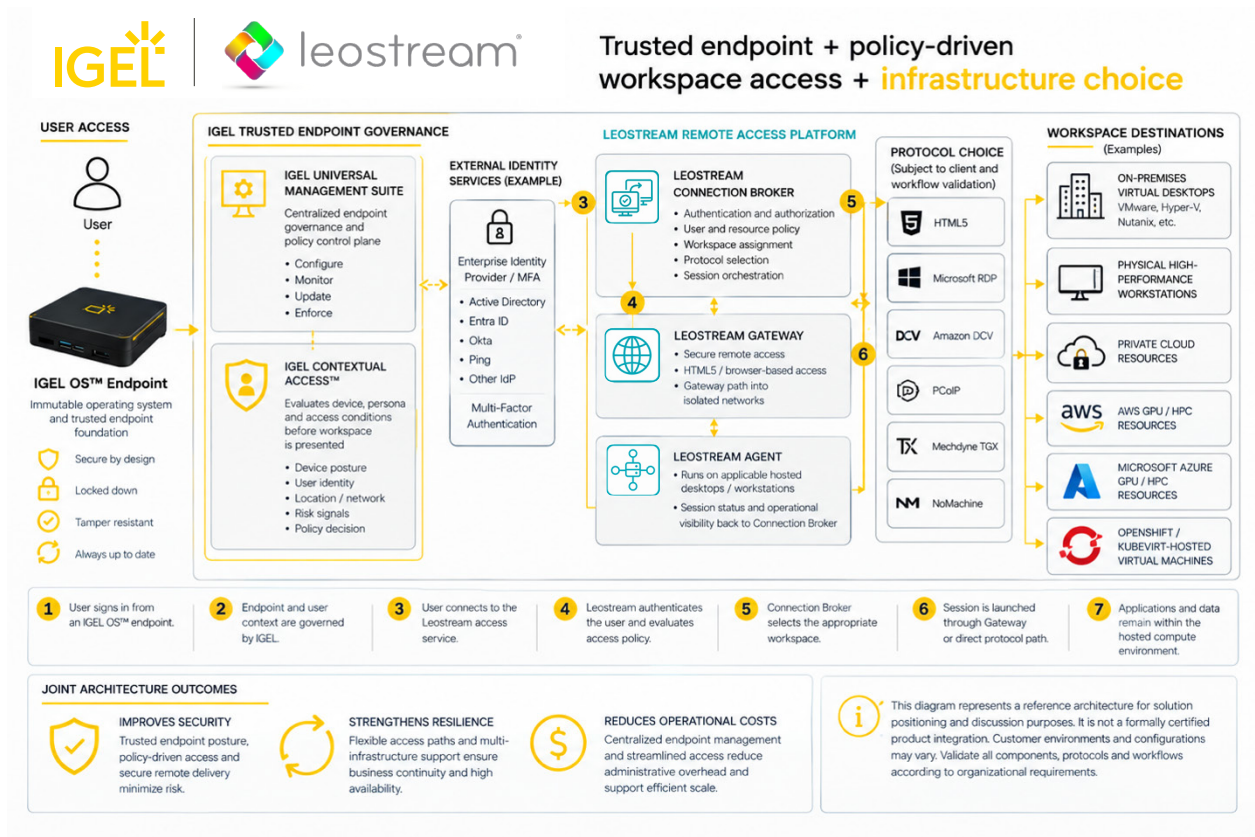
The problem is bigger than remote connectivity. Upstream identity and access controls still depend on a device layer that can be difficult to trust and govern, while high-value compute resources are expensive to leave idle or overprovisioned. The result is an endpoint trust problem on one side and a resource orchestration problem on the other.

IGEL and Leostream address these two layers with complementary capabilities. IGEL strengthens the device layer beneath secure access. Leostream brokers and governs access to the hosted workspaces and compute resources behind it.

Trusted Remote Access Architecture

Joint Solution Roles	
IGEL endpoint layer	Immutable endpoint foundation, centralized governance, contextual workspace control
Leostream access layer	Authentication, policy evaluation, resource brokering, session orchestration
Hosted workspace layer	Physical workstations, virtual desktops, cloud workstations, GPU and HPC resources
Display and access layer	Browser-based HTML5 access or validated protocol-specific client paths





IGEL Adaptive Secure Endpoint Platform provides an immutable, trusted, and governed endpoint layer for modern secure access architectures. IGEL OS is the immutable operating system at the core of the platform, while IGEL Universal Management Suite™ provides centralized policy orchestration, configuration control, and endpoint governance. IGEL Contextual Access™ can evaluate device, persona, and access conditions to shape the endpoint workspace and permitted local experience.

Leostream sits between users and hosted resources as the Remote Desktop Access Platform. Its Connection Broker authenticates users, applies assignment and connection policies, and directs users to the appropriate desktops, workstations, applications, or compute resources. The Leostream Gateway can provide secure remote access without requiring broad VPN exposure and supports browser-based connections as well as routed display-protocol traffic.

How The Session Comes Together

PHASE 1	PHASE 2	PHASE 3	PHASE 4
Establish trust User starts from a centrally governed IGEL OS endpoint	Evaluate access Leostream authenticates the user and applies resource and connection policy	Assign workspace Leostream selects the appropriate physical, virtual, cloud, GPU, or HPC resource	Launch session Browser-based or validated protocol access connects the user to the hosted workspace

This separation of responsibilities is useful because each platform can focus on the layer it is designed to govern. IGEL controls endpoint state and workspace behavior. Leostream controls resource assignment, access policy, protocol selection, session routing, and resource lifecycle. Applications and sensitive data can remain in the hosted environment while the endpoint stays tightly governed.

Key Benefits of IGEL and Leostream

1. Improve security from the device to the hosted workspace

IGEL supports Zero Trust-aligned architectures by strengthening the endpoint layer those models depend on. Its immutable operating foundation helps reduce drift, limit persistence, and preserve a known policy-aligned endpoint state. Leostream adds policy-driven authentication, least-privilege resource assignment, secure gateway access, and controls over how users reach hosted resources.

Together, the architecture creates a clearer trust boundary. The endpoint is governed before the remote session starts, and the remote access layer controls which resource the user can reach and how the connection is established.

2. Strengthen resilience across distributed workspaces

A remote workspace strategy is only useful if users can continue to reach the resources they need across changing infrastructure conditions. Leostream can broker across on-premises, private-cloud, public-cloud, and hybrid environments, helping organizations avoid tying user access to one hosting model. IGEL provides a consistent endpoint layer that can be centrally managed across distributed locations.

This combination supports a resilient operating model in which the access device, brokering layer, and hosted workspace can evolve independently without forcing a wholesale redesign of the user experience.

3. Reduce operational costs without reducing choice

Leostream can manage pools, power states, provisioning, and resource assignment so organizations can better align expensive compute capacity with actual demand. This is especially relevant for GPU-backed workstations and cloud HPC resources. IGEL can reduce endpoint operational burden through centralized governance, a controlled application model, and the ability to extend the useful life of compatible endpoint hardware.

The joint value is not simply lower cost. It is better allocation of cost: less operational effort at the endpoint, less idle capacity in the hosted environment, and more freedom to choose the compute and protocol model that fits each workload.

Access Patterns

Browser-first access through the Leostream Gateway

A practical joint deployment pattern is an IGEL OS endpoint running a centrally managed browser session to the Leostream Gateway. Leostream documents built-in HTML5 access for RDP, VNC, and SSH, with browser traffic from the client to the Gateway using HTTPS. The Gateway then connects to the hosted resource using the appropriate display-protocol port.

This pattern can simplify remote access because the endpoint does not need a dedicated Leostream client for the basic browser workflow. It is particularly useful for locked-down or task-focused endpoints and for environments that want to minimize broad network exposure.

Protocol-optimized access for demanding workloads

Leostream supports multiple display protocols so organizations can choose the connection method that best fits the workload. Current Leostream materials describe support for protocols including Amazon DCV, PCoIP, Mechdyne TGX, Microsoft RDP, NoMachine, and other options for specialized environments.

For graphics-intensive or high-performance workflows, the design can use a validated protocol-specific client path when the required client is available on the endpoint. Compatibility, GPU experience, peripherals, audio/video, USB, and smart-card requirements should be tested as part of the solution design.

Hybrid cloud and workstation access

Leostream can present a consistent access and policy layer across physical workstations, virtual desktops, and cloud-hosted resources. Public Leostream resources describe integrations with AWS services such as Amazon WorkSpaces Core and Amazon DCV, as well as Microsoft Azure deployments that include GPU-backed workstations and HPC nodes. IGEL keeps the endpoint experience centrally governed while the back-end compute platform changes according to workload, geography, or cost.

High-performance Use Case Spotlight

Geophysical workflow: Subsurface exploration requires large-scale compute, specialized applications, and a seamless end-user experience across hybrid infrastructure. Virtual workstations are dynamically provisioned, and power management is automated so compute resources can be allocated more efficiently.

For an IGEL and Leostream design, this creates a natural division of labor. Leostream manages access to specialized workstations and the lifecycle of expensive compute resources. IGEL provides the governed endpoint users rely on to reach those resources. The same pattern can extend to engineering, science, media, financial modeling, and other environments where the application and data belong close to high-performance compute rather than on the local device.

HIGH-PERFORMANCE WORKSPACES, SECURELY DELIVERED ANYWHERE

IGEL enables secure, policy-driven access to high-performance resources across industries and hosting environments.



	ENERGY AND GEOSCIENCE Secure access to GPU-backed workstations, seismic analysis, reservoir modeling, and hybrid HPC resources.	
	ENGINEERING AND DESIGN Policy-driven access to physical or virtual high-performance workstations without requiring workstation-class hardware at every user location.	
	MEDIA AND SPECIALIZED PRODUCTION Flexible access to high-performance resources while keeping project data and applications in the data center or cloud.	
	GOVERNMENT AND DEFENSE Centrally governed endpoints paired with isolated or tightly controlled remote workspace access patterns. Validate smart-card, protocol, and accreditation requirements for each environment.	
	CLOUD WORKSTATION MODERNIZATION A consistent endpoint and access experience while compute moves between on-premises infrastructure, AWS, Microsoft Azure, or other supported hosting platforms.	

SECURE | **POLICY-DRIVEN** | **CONSISTENT** | **HIGH-PERFORMANCE**

Delivering secure, high-performance access across industries, environments, and clouds.

Customer priority	Joint solution contribution
Improve endpoint trust	IGEL provides an immutable and centrally governed endpoint foundation for secure access.
Control remote access	Leostream applies authentication, resource policy, connection brokering, and session routing.
Protect high-value data	Applications and data can remain on hosted workstations or cloud resources rather than being processed locally.
Improve resilience	Users can access resources across physical, virtual, cloud, and hybrid infrastructure while retaining a consistent endpoint experience.
Optimize GPU and cloud capacity	Leostream can manage resource assignment and power states to reduce idle high-cost compute.
Simplify endpoint operations	IGEL centralizes endpoint policy and supports modular application delivery through IGEL App Portal.
Preserve architecture choice	The model supports multiple hosting platforms and display protocols rather than requiring a single closed stack.

About Leostream

Leostream digital workspace management solutions embody over 20 years of Leostream research and development in supporting customers with hosted desktop environments, including VDI, hybrid cloud, and high-performance display protocols. The Leostream high performance Remote Desktop Access Platform provides the world's most robust digital workspace connection management and remote access feature set, allowing today's enterprises to choose the best-of-breed components to satisfy their complex security, cost, and flexibility needs while working with them as they evolve into tomorrow. The Leostream Cloud service simplifies, secures, and monitors temporary access to corporate resources for employees, vendors, service providers, and external contractors.

About IGEL

IGEL provides a trusted and governed endpoint layer for secure access to enterprise applications and digital workspaces. Built on an immutable operating system, the IGEL Adaptive Secure Endpoint Platform helps organizations reduce endpoint attack surface, strengthen operational resilience, and simplify endpoint operations across a broad technology ecosystem.