IGEL Business Continuity & Disaster Recovery

When endpoints stop, disruption starts. Reboot compromised Windows endpoints to IGEL for secure access to critical services on in-place devices in minutes.

The Endpoint Resilience Challenge

Cyberattacks and endpoint outages disrupt IT teams, halt business operations and shrink revenue. While most enterprises invest heavily in data center and cloud recovery, endpoint access recovery remains the weakest link—leaving employees offline for days, driving up costs, exposing the organization to noncompliance risks. Cyber threats and downtime are rising industry-wide with severe impact on business reputation, placing consumer trust on the line.

IGEL Business Continuity & Disaster Recovery delivers endpoint resilience

Close the endpoint gap. IGEL Business Continuity & Disaster Recovery delivers instant endpoint recovery without replacement devices or reimaging. By installing IGEL OS alongside the Windows partition, any compromised endpoint can be rebooted into a secure IGEL environment in minutes, bypassing the breached partition. Users immediately regain access to critical apps—Office 365, Teams, Zoom, VDI/DaaS and even connectivity to web-based isolated recovery environments (IREs) — ensuring communication and essential services continue uninterrupted for customers.

IGEL's approach is managed from a single console delivering instant operational continuity at scale by:

IGEL Dual Boot™ installs IGEL OS alongside the Windows partition, enabling a clean boot to IGEL for secure user access to critical services.

IGEL USB Boot™ enables the user clean boot to IGEL OS on compromised endpoints and securely access critical business apps via a secure external USB device.

IGEL Universal Management Suite (UMS) manages endpoint configuration, updates, and policy—available as UMS as a Service (cloud-managed) or as software.

Specialist Services provide support during the setup, testing and recovery validation phases as well as for ongoing support during tabletop and simulation exercises and during a business recovery incident.

72%

of organizations report a ransomware attack within the past 12 months[1].

24.6 days

is the average downtime following an attack in 2025.[2]

$1.4M-$4.5M

is the average cost of an outage per incident.[3]

- Minimize downtime
- Reduce endpoint recovery costs
- Protect brand reputation
- Preserve forensic evidence
- Prevent reinfection

IGEL Business Continuity & Disaster Recovery accelerates operational continuity

IGEL's BC&DR solution enables instant endpoint business continuity for every user to securely reconnect to critical apps and services.

The secure, immutable endpoint operating system installed by IGEL Dual Boot™ bypasses the Windows partition, significantly reducing the chances of reinfection while maintaining enterprise manageability and control.

Reduce recovery costs
Eliminate hidden costs of procuring backup devices, IT resources for reimaging devices, and end-user downtime by securely rebooting existing, in-place devices.

Compliance simplified
Reduce endpoint complexity to align with mandates for global cybersecurity regulations such as NIST CSF, NIS2, CER, GDPR, HIPAA 2, and DORA. IGEL enables built-in rapid recovery that easily meets the 48-72 hour regulatory mandates.

Preserve incident forensics
The Windows partition is untouched and preserved to enable analysts to pinpoint vulnerabilities or misconfigurations that were exploited.

Match endpoint recovery time objective with **infrastructure RTO's**

Conclusion
IGEL Business Continuity & Disaster Recovery enables you to match your endpoint recovery time objective with your infrastructure RTO for all users across the enterprise.

Contact us to learn how IGEL can accelerate your incident response plan

Sources

[1] ITPro   [2] SQ Magazine   [3] Sophos

igel.com