Close The Endpoint Access Recovery Gap

A faster path to secure access to applications when a cyber attack threatens operations, revenue, and trust.

86%

of organizations studied experienced operational disruption following a data breach[1]

$1.5M

average ransomware recovery cost, excluding ransom payments[2]

53%

of ransomware-affected organizations recovered within one week[2]

The Overlooked Continuity Risk

Your applications, data, and recovery environments may be available, but can your workforce securely reach them?

Downtime becomes a business crisis at the endpoint

When ransomware, a failed update or a Windows disruption takes endpoints offline, the impact reaches far beyond IT. Employees cannot serve customers, clinicians may lose access to patient care workflows, transactions stall, and production slows down.. Every delay increases operational loss, recovery expense, regulatory exposure, and the risk of lasting reputational damage.

Traditional business continuity plans often prioritize restoring data centers, networks, and applications. Yet recovered infrastructure delivers little value if employees lack a secure endpoint from which to use it. This disconnect is the endpoint access recovery gap, and it can leave the business offline even when core infrastructure and services are technically available.

Traditional recovery compounds the disruption

Reimaging compromised devices, maintaining standby laptops, shipping replacements and dispatching technicians are difficult and expensive to execute at enterprise scale. These processes consume scarce resources, create inconsistent recovery experiences, and can keep large parts of the workforce disconnected while Windows investigation and remediation continue.

How IGEL BC&DR Compares

RECOVERY CONSIDERATION	TRADITIONAL APPROACH	IGEL BC&DR
Primary Objective	Repair, reimage, or replace the endpoint	Recover secure access to applications
Recovery Hardware	Replacement or rebuilt device may be required	Existing device is reused
Execution	Manual and device-by-device	Centrally controlled with Emergency Mode
Endpoint Access Recovery TimeFrame	Can take days, weeks	Can be restored within minutes
Windows Environment	Modified, wiped, or remediated	Preserved for remediation
User Involvement	Depends on user instructions and actions	Administrator-led through UMS
Application Access	Delayed until endpoint recovery completes	Browser, VDI/DaaS, native apps, or PWAs
Operational Model	Recovery and remediation are coupled	Access continuity and remediation proceed separately

Recover secure access without waiting for traditional remediation sequences.

IGEL Business Continuity & Disaster Recovery™ (BC&DR) gives organizations a prepared, administrator-controlled path to reconnect users from compromised Windows endpoints. Instead of repairing or reimaging the affected Windows environment before work can resume, IT can reboot authorized devices into secure IGEL OS™ on the same hardware with IGEL Dual Boot™, all components of the IGEL BC&DR solution. Users can then access approved SaaS and web applications, unified communications, VDI or DaaS desktops, critical business applications, and isolated recovery environments.

This separates endpoint access recovery from Windows remediation. Employees regain a secure way to work while security teams investigate and remediate the Windows environment in line with the remediation sequence on their Business Continuity Plan.

Reboot	Reconnect	Resume	Retain
Admins use IGEL Emergency Mode to initiate and manage IGEL Dual Boot, a controlled reboot of one device, selected groups, or broader populations into secure IGEL OS.	Users securelyconnect from existing hardware to the applications and recovery services authorized for the incident.	Teams restore communications, customer service and critical workflows through a consistent recovery experience managed at scale.	Devices remain in IGEL OS until administrators release them. The Windows partition is untouched and preserved for forensic and compliance review.

Reduce the risk and cost of prolonged recovery time

- Reduce endpoint-related downtime by enabling users a faster path to access authorized services.
- Avoid the cost, logistics, and time lapses of storing, preparing, and shipping replacement devices as the primary recovery plan.
- Reduce dependence on individual users making the correct recovery decision during a high-pressure incident.
- Preserve the Windows partition so forensic investigation can proceed without delaying workforce access and productivity.
- Extend continuity beyond selected executives or locations with a repeatable approach designed for enterprise scale.

Turn controlled endpoint access recovery into business continuity

Business continuity and risk leaders need evidence that recovery can be activated consistently, tested against business requirements, and measured across the workforce. IGEL® helps organizations establish a prepared endpoint continuity model supported by centralized administration, recovery validation, and tabletop exercises.

RTO VS RTA

Is your actual time to recover secure user access shorter than the downtime your business can tolerate?

Value across the resilience team

Business Continuity leaders:
Align endpoint access recovery with infrastructure and service recovery objectives.

Risk and Compliance leaders:
Support repeatable, auditable workflows and evidence for applicable regulatory, contractual and insurance requirements.

CISOs and Incident Response teams:
Maintain administrator control, reduce the risk of users returning to an at-risk environment and preserve the Windows partition for review.

CIOs and IT Operations:
Reduce manual reimaging, hardware logistics, and resource pressure while improving workforce coverage.

Prepare before disruption becomes downtime

- Identify critical users, workflows, locations, and endpoint dependencies.
- Compare endpoint Recovery Time Actual with infrastructure and business Recovery Time Objectives.
- Quantify standby-device, shipping, reimaging, labor, and downtime exposure.
- Define approved recovery services and validate the experience through exercises.

Sources and messaging references

1. IBM, Cost of a Data Breach Report 2025, pp. 41–42: https://www.ibm.com/reports/data-breach
2. Sophos, The State of Ransomware 2025: https://www.sophos.com/en-us/content/state-of-ransomware-2025

Schedule an IGEL Endpoint Resilience Assessment

Identify gaps in your current endpoint recovery strategy, estimate operational and cost exposure, and define a faster path to secure application access. Request an IGEL BC&DR demonstration and put endpoint access recovery to the test.

IGEL is a registered trademark of IGEL Technology GmbH. Preventative Security Model is a trademark of IGEL.
All other hardware and software names are registered trademarks of their respective manufacturers. Errors and omissions excepted. Subject to change without notice. September 2026.