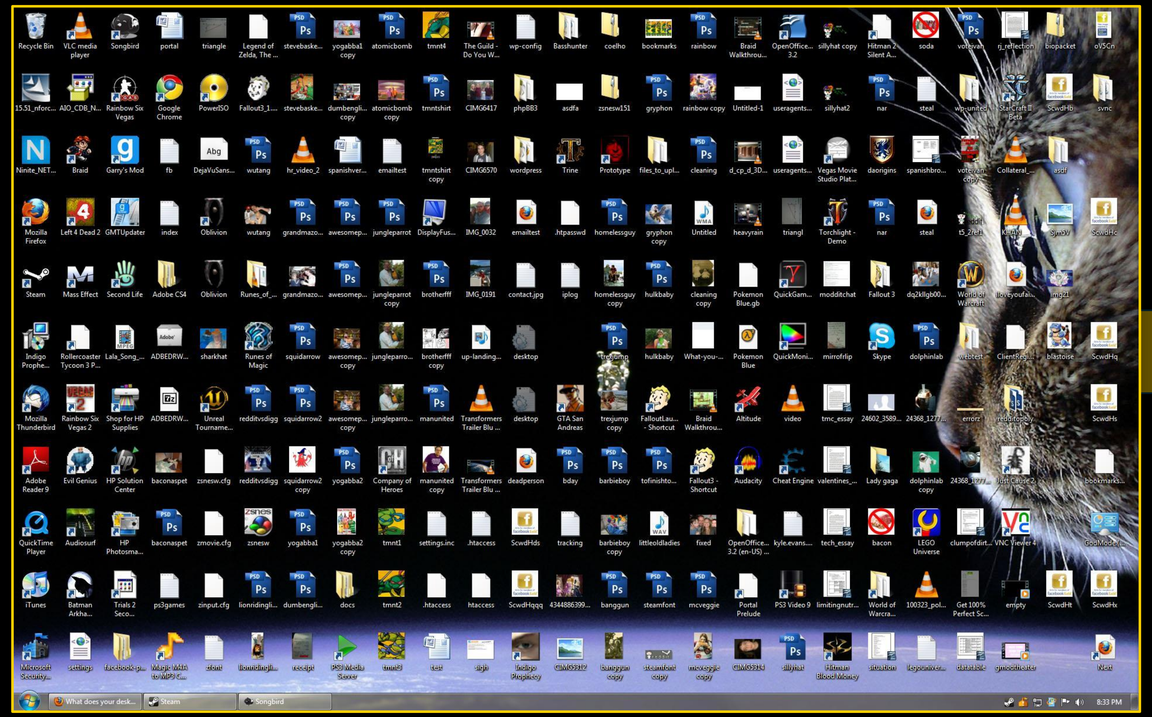
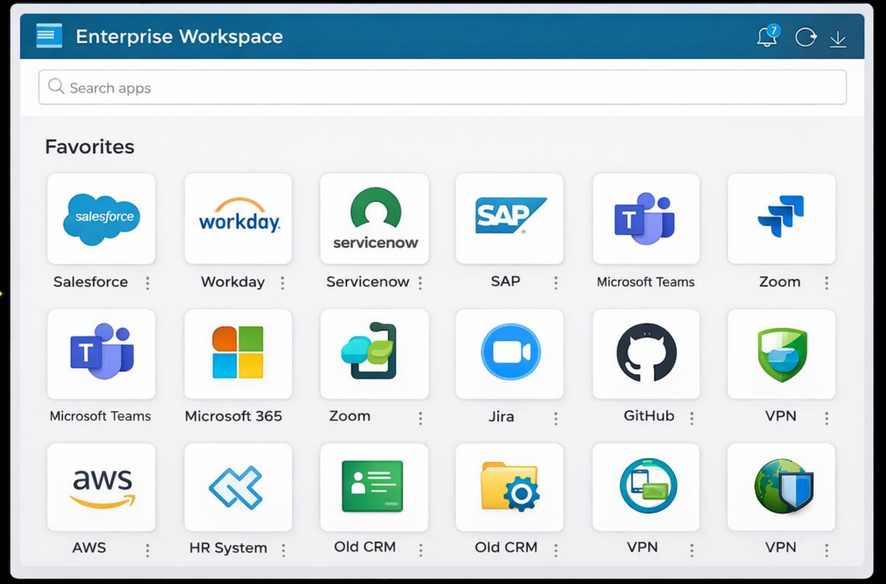

IGEL now
&next

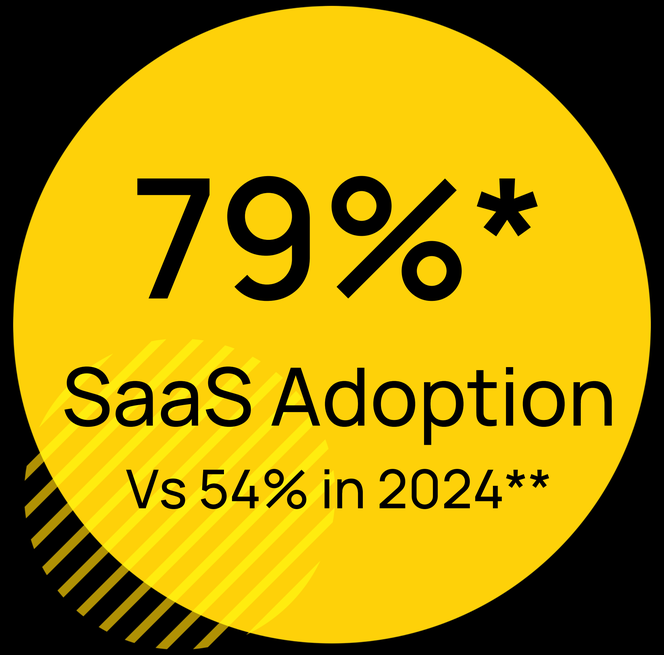
James Millington

VP Product Marketing




Enterprise Workspace
Search apps
Favorites
Salesforce
Workday
Servicenow
SAP
Microsoft Teams
Zoom
Microsoft Teams
Microsoft 365
Zoom
Jira
GitHub
VPN
AWS
HR System
Old CRM
Old CRM
VPN
VPN

Forrester:
SaaS Adoption is at 79% among enterprise organizations

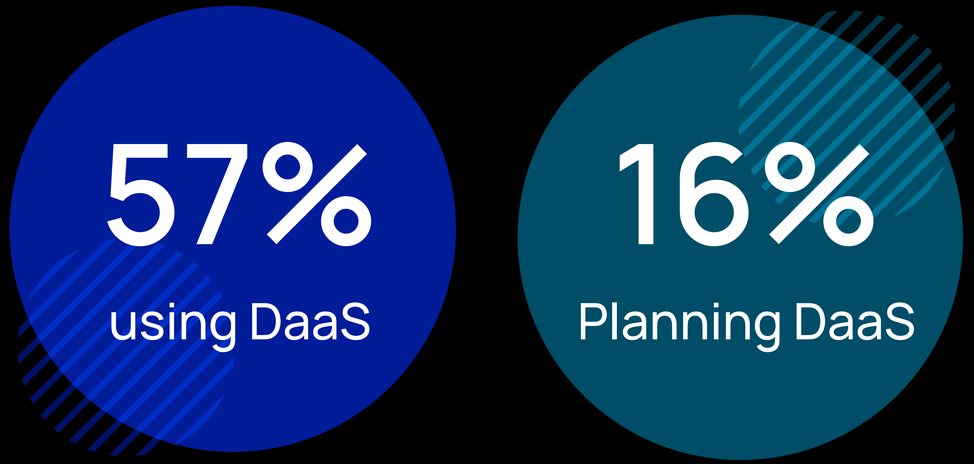


*Forrester – Enterprise Applications Software Survey (2025)

*Data Overview: Technology Landscapes Continue To Grow With SaaS

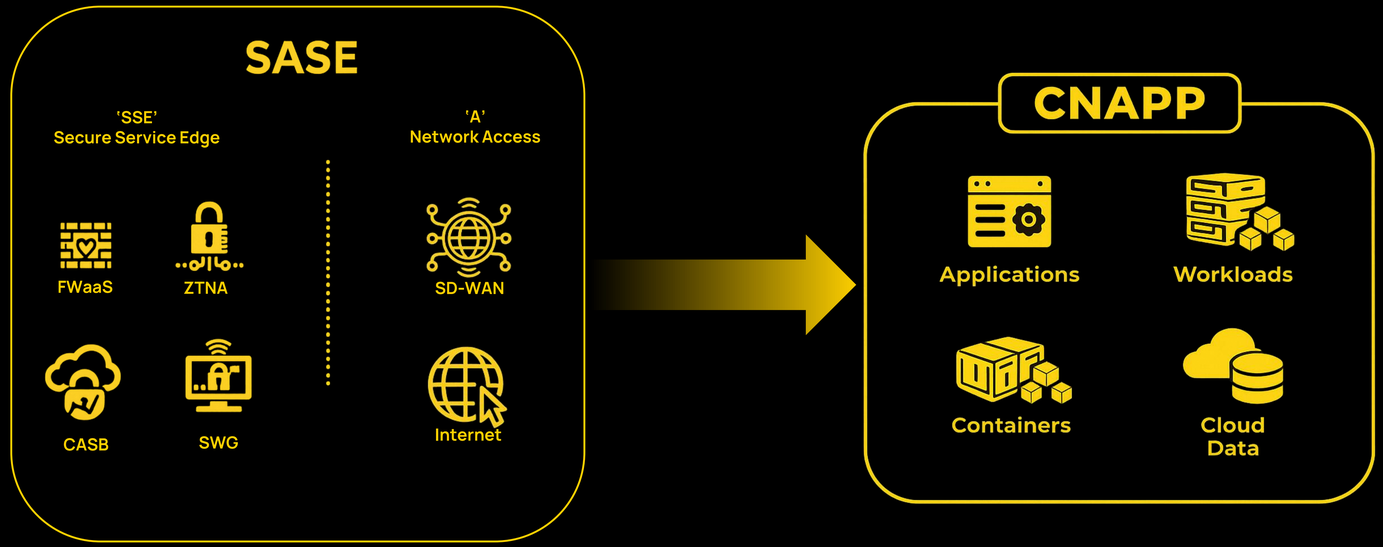
Forrester:

57% of organizations are already using Desktop-as-a-Service or provider-managed VDI, with another 16% planning to adopt it

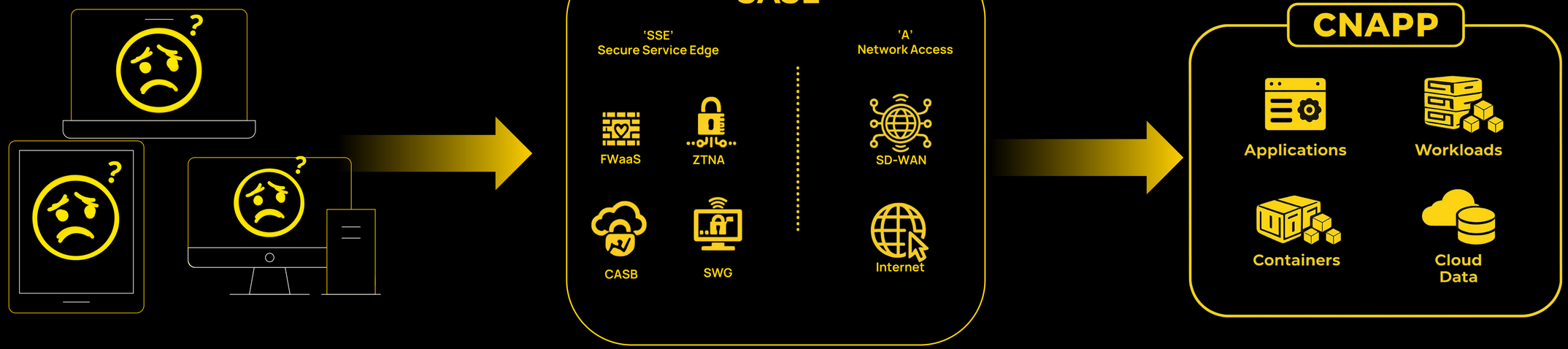


Forrester End-User Computing / Digital Workspace research (2024–2025)

The security infrastructure has shifted




SSE
24.8%
CAGR
SASE
65%
Enterprise
Adoption
CNAPP
28.1%
CAGR
Markets and Markets
Ponemon Institute
Frost & Sullivan


SASE
'SSE'
Secure Service Edge
'A'
Network Access
FWaaS
ZTNA
SD-WAN
CASB
SWG
Internet
CNAPP
Applications
Workloads
Containers
Cloud
Data

Gartner.

Use Immutable Endpoints to Defeat Ransomware, Stop Configuration Drift, and Guarantee Rapid Recovery

27 February 2026 - ID G00845723 - 9 min read

By: Franz Hinner, Eric Grenier, Evgeny Mirolyubov, Nikul Patel

Initiatives: Build and Evolve a Resilient and Agile Cybersecurity Program; Delivery of Functional Responsibilities

> Endpoints are an organization's most fragmented, porous surface. CISOs should use this research to transition to the Workspace Immutable Secure Endpoint (WISE) model — a strategy that centralizes security to reduce attack vectors by aiming to eliminate persistent mutable endpoints.

Insights at a Glance

Mutable, agent-heavy endpoints create technical debt and remain a primary beachhead for attack. CISOs seeking to test immutable endpoints, or if ready to fully move to an immutable endpoint setup should use the WISE model transition plan. The phases are designed for controlled deployment; resulting in a more secure environment by reducing mutable endpoints, reducing configuration drift, and recovery times without relying on hardware logistics.

Key Insights:

- Break ransomware kill chains by using immutable endpoints that revert to pristine on reboot, removing persistence for low-and-slow attacks. [13]
- Slash hybrid worker downtime by 98% by replacing slow physical device swaps with automated firmware-level rehydration. [1-3]
- Protect DEX rigorously to avoid friction that drives users into unmanaged shadow IT.

Take Action:

Segment users by mission-criticality, risk, and SaaS-only needs to target Cloud DaaS, stateless OS, or secure BYOD.

Use Immutable Endpoints to Defeat Ransomware, Stop Configuration Drift, and Guarantee Rapid Recovery

27 February 2026 - ID G00845723 - 9 min read

By: Franz Hinner, Eric Grenier, Evgeny Mirolyubov, Nikul Patel

Initiatives: Build and Evolve a Resilient and Agile Cybersecurity Program; Delivery of Functional Responsibilities

Gartner

Use Immutable Endpoints to Defeat Ransomware, Stop Configuration Drift, and Guarantee Rapid Recovery

> Endpoints are an organization's most fragmented, porous surface. CISOs should use this research to transition to the Workspace Immutable Secure Endpoint (WISE) model — a strategy that centralizes security to reduce attack vectors by aiming to eliminate persistent mutable endpoints.

Impact Brief

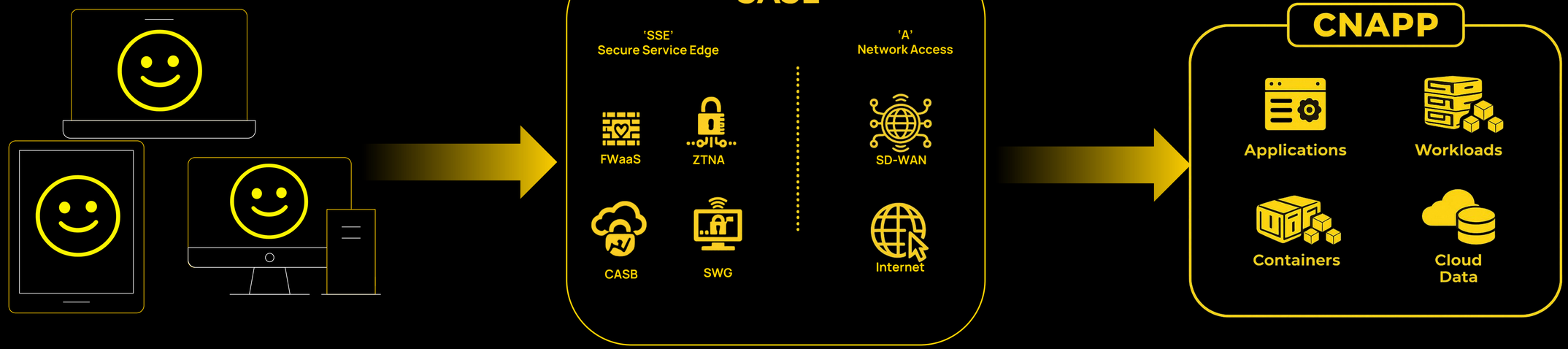
- Reduce attack surface by eliminating the configuration drift that causes 22% of enterprise endpoint controls to silently fail or drop out of compliance by transitioning to immutable, stateless workspaces. This architectural shift mechanically denies ransomware the local persistence it needs to dwell and spread across the network. [11]
- Ensure business continuity by protecting revenue and reputation by shifting disaster recovery timelines from an industry average of over seven months down to minutes. Mandating automated, stateless workspace refreshes completely bypasses the catastrophic downtime associated with manual reimaging after a malware event. [13]
- Unlock security budget by retiring complex on-device agents and patch tools, reclaiming up to 30% of endpoint OpEx for threat hunting.
- Satisfy insurability by using verifiable immutability to meet carriers' hardened posture expectations.

Strategic Planning Assumption

By 2030, immutable workspaces will become the primary interface for 30% of the workforce, necessitated by the need to neutralize AI-driven ransomware and cut support costs by 30%. [4-12]

Gartner

- Mandate Ephemeral OS disks for cloud workloads and stateless OSs, like IGEL,

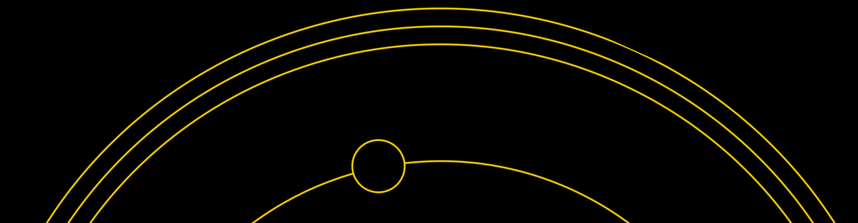

SASE
'SSE'
Secure Service Edge
'A'
Network Access
FWaaS
ZTNA
SD-WAN
CASB
SWG
Internet
CNAPP
Applications
Workloads
Containers
Cloud
Data

Simply IGEL it™

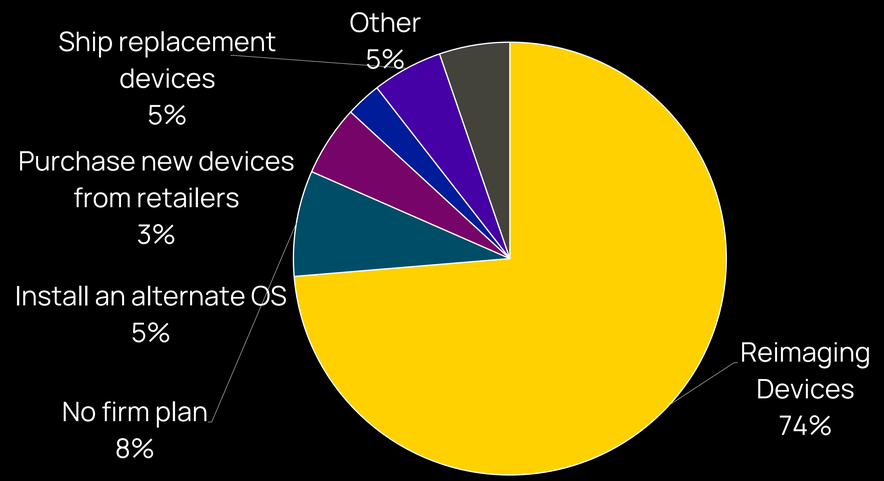
Business Continuity & Disaster Recovery

The Math of Recovery

Are organizations in denial?

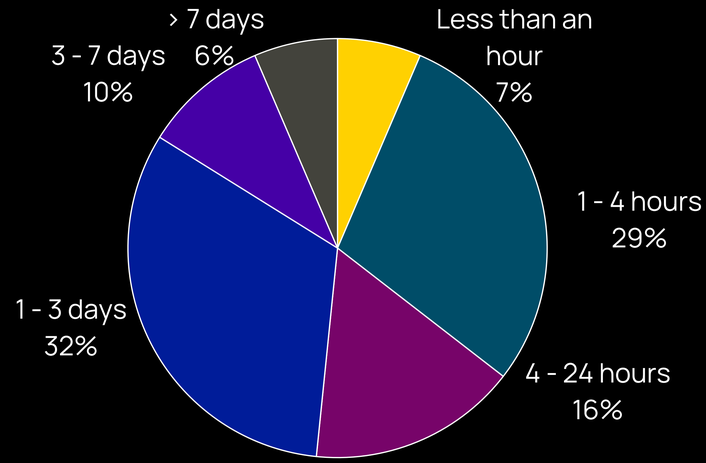


What best describes your organization's current approach to endpoint recovery following a cyber incident



74% - Reimaging Devices

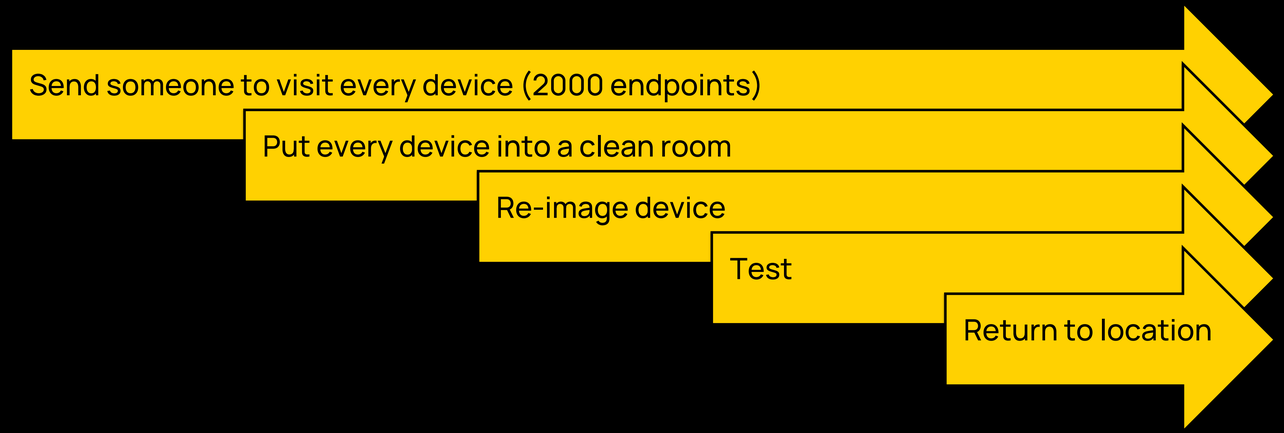
How long does it take to restore the majority of user's endpoints after a significant cyber event?



29% < 4 hours
68% < 3 days

IGEL CHIME Survey November 2025

Customer BC&DR Plan Discussion 1



= 2.5 hours per device

= 5000 person hours

= 125 person weeks

Customer BC&DR Plan Discussion 2

“We can recover 1000 endpoints in a week”

“We have 40,000 endpoints”

Maybe the answer isn’t…

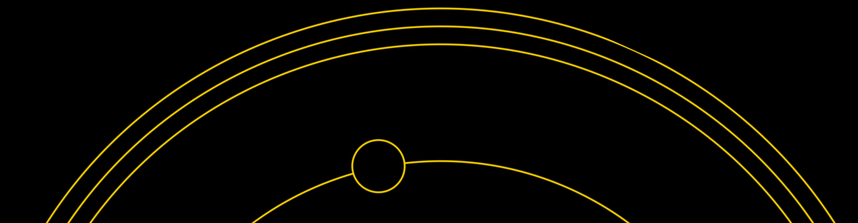
A better recovery plan

Maybe the answer is…

A better endpoint strategy

~~Recovery~~

Resilience



Simply IGEL it™

EUREKA!

EUC's EUREKA! Moment

Simply IGEL it™


IGEL now
& next