LOGICALIS
Architects of Change

Microsoft
Solutions Partner

Solution Brief

Turnkey Disaster Recovery with Logicalis PRC + Azure

Reduce downtime, recovery costs, and risk with Azure and Logicalis.

The modern threat landscape is evolving at an unprecedented rate. According to Microsoft's recent Digital Defense Report, Microsoft customers face more than 600 million cyberattacks daily from cybercriminals and nation-state actors.

Microsoft recorded a
2.75x year-over-year increase
in human-operated ransomware attacks between July 2023 and June 2024

At least
52% of cyberattacks
in 2024 were fueled by financial gain

At least
In 80% of incidents,
the primary objective was data theft

In on-premises ransomware, the threat actor typically deploys malware that encrypts crucial files on as many endpoints as possible, then negotiates with the victim for the decryption key. In cloud-based ransomware attacks, cloud features and capabilities give the threat actor the capability to quickly exfiltrate and transmit large amounts of data from the victim environment to their own infrastructure, destroy the data and backup cloud resources in the victim cloud environment, and then demand the ransom.

Isolated, immutable cyber vaults are increasingly used by security teams to protect both on-premises and cloud infrastructure. Logical and physical "air gaps" keep data separate from production environments, unalterable, and inaccessible to attackers.

Onsite cyber vaults require commitments to infrastructure, expertise, and resources, which is why many teams turn to cloud-based solutions, such as those offered through Logicalis and Azure. Cloud-based cyber vaults offer a secure recovery environment that use a combination of logical air-gapping, immutability, and zero-trust principles to protect data in the event of a security breach.

Paired with Logicalis Production Ready Cloud (PRC), a Microsoft-approved, Azure Expert MSP framework, on-premises clients can quickly access a turnkey, enterprise-grade disaster recovery solution.

The Cost of an Unprepared Recovery Environment

The consequences of a ransomware event extend far beyond the initial breach. Without a structured recovery environment in place, organizations face recovery timelines measured in weeks. During this time, business operations are often partially or fully suspended, revenue losses compound, and regulatory exposure escalates with every hour of downtime.

A well-architected recovery environment changes that scenario entirely. With pre-built clean-room infrastructure, immutable backups, and tested failover orchestration, organizations can restore critical workloads in as little as 24 to 72 hours.

Fortunately, the difference between weeks and days can be closed with the proper preparation, as described below.

Azure as Disaster Recovery for On-Premises Clients

Disaster recovery and cyber vault protection for on-premises workloads is built on a layered architecture, anchored by enterprise-grade data protection platforms from Veeam and Rubrik, and extended through Azure's native infrastructure services. This partner-led approach delivers the technology depth, flexibility, and operational maturity that modern ransomware threats demand.

Veeam provides comprehensive backup, replication, and recovery for on-premises and hybrid workloads, with deep integration across VMware, Hyper-V, and physical server environments. Its cloud-tier capabilities enable seamless offload to Azure-managed storage, creating a durable, immutable protection layer without dependency on native Azure Backup agents.

Rubrik delivers a zero-trust data security architecture with air-gapped, immutable backups and automated threat detection. Its ransomware recovery capabilities include clean-room recovery workflows, data threat analytics, and near-instant recovery orchestration across hybrid and multi-cloud environments.

Azure Site Recovery complements these partner platforms by enabling continuous replication of on-premises workloads to Azure. When an outage or cyberattack strikes the primary site, organizations can fail over and resume operations from a secondary location. Near-synchronous replication and application-consistent snapshots continuously protect disk data, in-memory data, and in-flight transactions.

Together, these capabilities give on-premises organizations a cyber vault solution that combines the technology depth of best-in-class data protection platforms with the scale and logical isolation of Azure infrastructure — without the cost of a secondary physical data center.

VMware and Nutanix: Accelerated Recovery Without Conversion for organizations running VMware or Nutanix hypervisor environments on-premises, native workload protection and recovery to Azure is available without requiring conversion to Azure-native VM formats.

Azure VMware Solution (AVS) provides a dedicated, VMware-native environment running insie Azure data centers, enabling organizations to fail over VMware workloads directly. Recovery teams operate within consistent tooling, runbooks, and operational processes, which reduces friction and risk. When the primary site is restored, workloads migrate back without re-platforming.

Nutanix Cloud Clusters (NC2) on Azure delivers the same capability for Nutanix AHV environments. On-premises Nutanix workloads can be protected and recovered within Azure using native Nutanix infrastructure, preserving operational familiarity and accelerating return-to-production timelines. AVS is compatible with both Veeam and Rubrik protection layers.NC2 on Azure is supported through the Veeam Plug-in for Nutanix AHV, maintaining a consistent data protection policy across hypervisor platforms.

Protecting Cloud-Native Workloads Through DevSecOps

As organizations migrate and build workloads natively in Azure, backup and recovery strategies must extend beyond on-premises infrastructure to include cloud-native resources.

Yet applications deployed through CI/CD pipelines introduce distinct protection requirements: infrastructure-as-code definitions, container configurations, pipeline secrets, and application state must all be treated as recoverable assets.

A mature DevOps or DevSecOps practice addresses this by embedding backup and recovery controls directly into the deployment pipeline. Infrastructure definitions stored in version-controlled repositories can be rapidly redeployed to a clean environment. Security scanning, policy enforcement, and secrets management integrated at the pipeline level ensure that recovered environments are rebuilt from a known-good, compliant baseline.

Logicalis PRC extends its governance and security controls into CI/CD environments, ensuring cloud-native workloads are protected by the same defense-in-depth posture applied to traditional on-premises replications.

Building an Azure Cyber Vault Solution

with Logicalis Production Ready Cloud (PRC)

Logicalis Production Ready Cloud (PRC) is a Microsoft-approved, Azure Expert MSP framework designed to help organizations rapidly adopt, deploy, and manage Azure environments. Built on the Azure Cloud Adoption Framework and the Azure Well-Architected Framework, PRC provides a pre-configured, secured landing zone with enterprise-grade governance, security, and operational maturity.

A foundational component of the PRC landing zone is the deployment of Break Glass accounts within the Azure environment. Break Glass accounts are highly privileged, emergency-access credentials maintained outside of standard Identity Access Management (IAM) systems. In the event that an organization's IAM platform is compromised during an attack, Break Glass accounts provide a guaranteed pathway to regain administrative control of the Azure environment. Combined with the logical air gap inherent to the PRC architecture, the landing zone functions as a clean room entirely outside the blast radius of a production network compromise.

With this proven, blueprinted methodology, PRC can accelerate time-to-value for disaster recovery and cyber vault deployments, from initial assessment through continuous managed services.

Benefits of Logicalis PRC

- **Identity-resilient architecture:** Break Glass accounts and zero-trust IAM controls maintain administrative access even when production identity systems are compromised
- **Accelerated deployment:** Compress the timeline from assessment to a fully operational Azure cyber vault
- **Reduced risk:** Automated Azure toolsets and standardized building blocks minimize human error and ensure consistent, repeatable deployments
- **Cost transparency and optimization:** A Cloud Management Portal provides real-time visibility into current usage and predicted spend
- **Enterprise-grade security and compliance:** The PRC landing zone is built to the Azure Well-Architected Framework and continuously scanned to maintain compliance posture
- **Continuous managed services:** Ongoing managed services cover availability monitoring, security operations, cost optimization, and monthly health checks

Protect Against Ransomware and Data Loss

with Disaster Recovery Solutions from Logicalis + Azure

Transitioning to Microsoft Azure for disaster recovery and cyber vault protection represents a key step in organizational resilience. A successful transition requires structured deployment and proven expertise.

Logicalis brings deep Microsoft Azure experience and the proprietary Production Ready Cloud (PRC) methodology to ensure disaster recovery environments are properly architected, secured, and managed.

From assessment to continuous managed services, our teams work closely with IT and security teams to accelerate time-to-value across every phase of disaster recovery modernization.

If your organization is ready to explore cloud-based cyber vaults with Azure, schedule a free disaster recovery consultation today.

Schedule Free Consultation

Why Logicalis?

- 25+ year Microsoft partner, spanning the full history of Azure, with deep joint IP and co-innovation across cloud, security, and managed services
- 12 Microsoft Advanced Specializations and 5 Solution Area Designations, including Cloud Security, Threat Protection, IAM, and Infrastructure
- One of fewer than 70 partners worldwide to achieve Global Azure Expert MSP (AEMSP) status
- 7,000+ employees across 30 territories serving 10,000+ clients globally
- Microsoft Intelligent Security Association (MISA) member and verified Managed XDR partner

LOGICALIS
Architects of Change

Microsoft
Solutions Partner