

Fortify Your Cyber Defense

with a Unified Hybrid Multicloud Strategy



Data, apps, and security gaps.

Today, **data and apps are scattered** across diverse cloud environments. Traditional cyber security wasn't designed to handle this type of landscape—and IT leaders are finding it can't keep up.

▲ 750M

new applications will enter the market by 2026².

▲ 82%

of organizations leverage hybrid cloud⁴.

▲ 85%

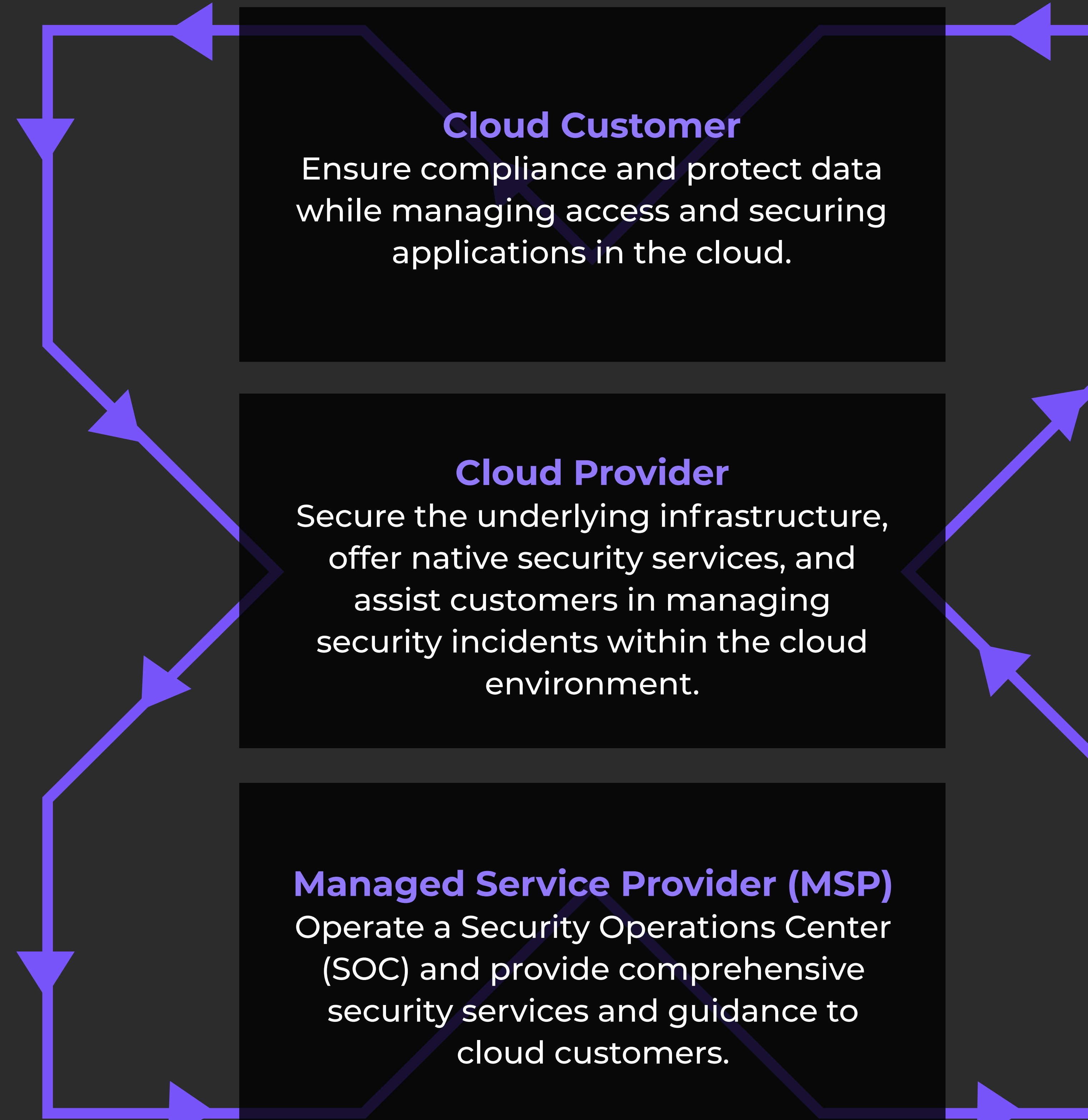
of organizations report that security is their top cloud challenge¹.

Nutanix ensures your platform, data, applications and networks are resilient and aligned to your security operations.

Unlock the full potential of shared security

In a shared service cloud operating model, securing the services that your managed or cloud service provides is increasingly complex.

For IT leaders, understanding each role, and having full visibility into access policies is vital to eliminating vulnerabilities.



Cloud Customer
Ensure compliance and protect data while managing access and securing applications in the cloud.

Cloud Provider
Secure the underlying infrastructure, offer native security services, and assist customers in managing security incidents within the cloud environment.

Managed Service Provider (MSP)
Operate a Security Operations Center (SOC) and provide comprehensive security services and guidance to cloud customers.

76%

of organizations lack complete visibility into access policies and applications across their multicloud platforms³.

Managing Security Through a "Single Pane of Glass"

Nutanix offers comprehensive security for hybrid multicloud, securing data, apps, and networks, regardless of location. Our approach provides IT leaders with a single pane of glass for managing security across all your cloud environments. This ensures consistent security policies and eliminates unseen gaps.

Hybrid multicloud is reality. Here's how you secure it.

Remote Work Environments

Combine policies, zero-trust security, multi-factor authentication (MFA), and a focus on timely software updates to create a strong security posture.

Data Encryption

Encrypt data at rest (stored), in transit (moving), and in use (accessed) to comply with regulations and safeguard sensitive information.

Firewalls

Create secure network zones and block sophisticated cyberattacks by utilizing firewalls with advanced features and micro-segmentation techniques.

"According to Gartner, by 2027,

75%

of employees will acquire, modify, or create technology outside IT's visibility—up from 41% in 2022."

Access Control

Ensure only authorized users have appropriate access to data and applications in hybrid multicloud environments, using third-party or cloud provider IAM tools.

AI Resources

Protect AI resources from traditional security threats like data breaches, insider attacks, and adversarial attacks targeting AI models and data.

It is critical for businesses to develop an enterprise-wide cyber resiliency approach that safeguards every organizational resource, regardless of location.

Because every organization is unique, so is their path to cyber resiliency. At Nutanix, we embed security into every layer of our product, ensuring hybrid multicloud operations remain secure throughout.

Visit [Nutanix Trust](#) and [Nutanix Security](#) to learn more about cyber resilience best practices for hybrid multicloud.



1 Source: Flexera 2024 State of the Cloud Report
2 Source: ICD FutureScape
3 Source: Strata Identity
4 Source: TK

Fortify Your Cyber Defense

with a Unified Hybrid Multicloud Strategy



Data, apps, and security gaps.

Today, **data and apps are scattered** across diverse cloud environments. IT leaders are finding that traditional cyber security can't keep up with today's landscape.

▲ **750M**

new applications will enter the market by 2026².

▲ **82%**

of organizations leverage hybrid cloud⁴.

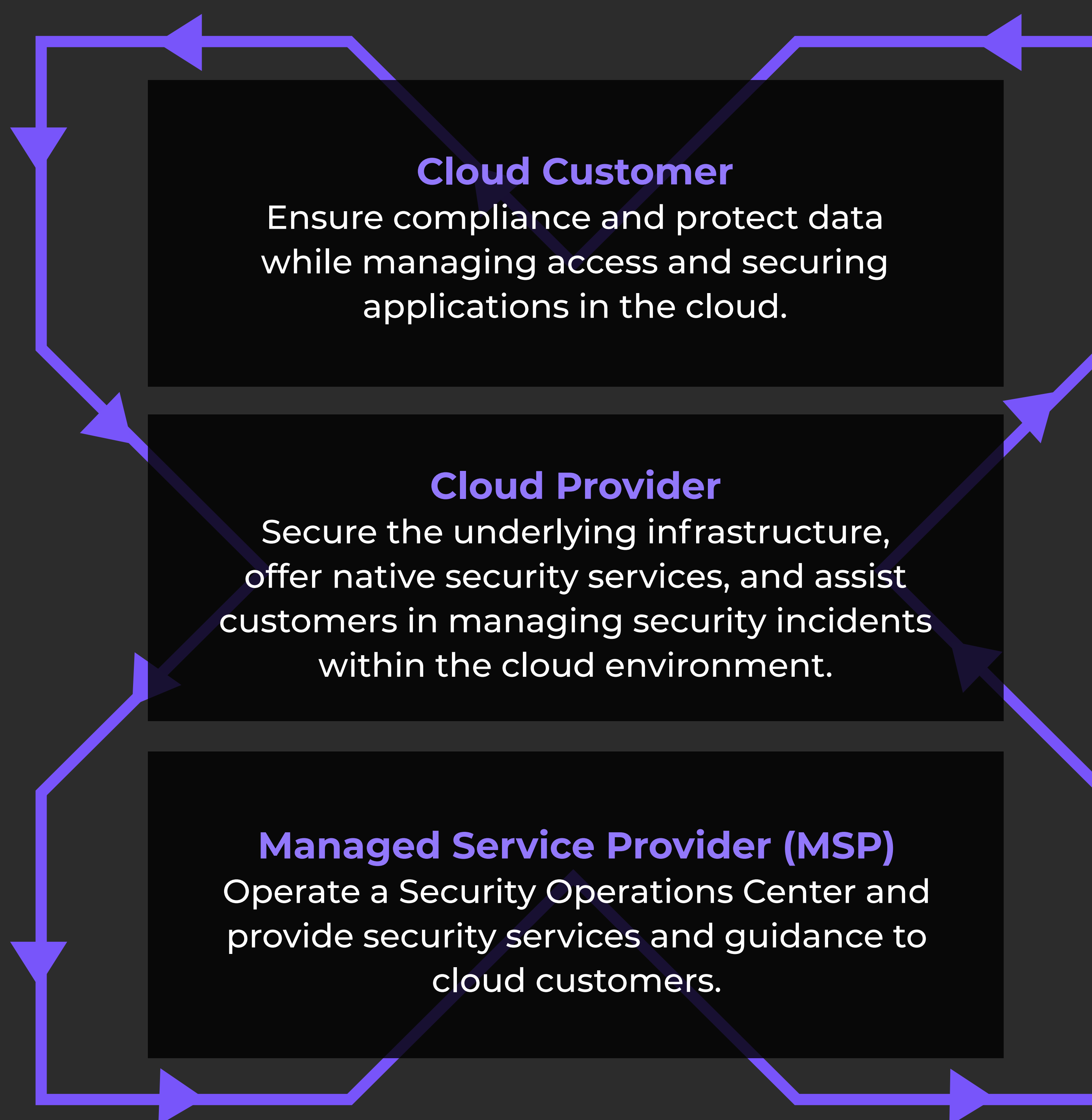
▲ **85%**

of organizations report that security is their top cloud challenge¹.

Nutanix ensures your platform, data, applications and networks are resilient and aligned to your security operations.

Unlock the full potential of shared security

In a shared service cloud operating model understanding each role and having full visibility into access policies is vital to eliminating vulnerabilities.



76%

of organizations lack complete visibility into access policies and applications across their multicloud platforms³.

Managing Security Through a "Single Pane of Glass"

Nutanix offers comprehensive security for hybrid multicloud. We secure data, apps, and networks, providing IT leaders with a single pane of glass for managing security across all cloud environments.

Hybrid multicloud is reality. Here's how you secure it.

Remote Work Environments

Combine policies, zero-trust security, multi-factor authentication (MFA).

Data Encryption

Encrypt data at rest (stored), in transit (moving), and in use (accessed).

Access Control

Ensure only authorized users have access to data and apps in hybrid multicloud environments.

Firewalls

Create secure network zones and block sophisticated cyberattacks.

AI Resources

Protect AI resources from traditional security threats targeting AI models and data.

"According to Gartner, by 2027,

75%

of employees will acquire, modify, or create technology outside IT's visibility—up from 41% in 2022."

Because every organization is unique, so is their path to cyber resiliency. At Nutanix, we embed security into every layer of our product, ensuring hybrid multicloud operations remain secure throughout.

Visit [Nutanix Trust](#) and [Nutanix Security](#) to learn more about cyber resiliency best practices for hybrid multicloud.



1 Source: Flexera 2024 State of the Cloud Report
2 Source: ICD FutureScape
3 Source: Strata Identity
4 Source: TK