It's All in the Cloud

It's All in the Cloud: From Cloud First to Security First

Cloud adoption was on the rise well before 2020. But as the pandemic tightened its grip, companies of all sizes rushed to adopt cloud-based tools to stay competitive. And because there was – and continues to be – a dearth of cloud expertise, many MSPs and MSSPs saw their businesses grow.

In fact, more than half said COVID-19 enabled them to expand services to clients, while 62% saw an increase in their overall monthly recurring revenue (MRR). Nearly half of MSPs reported MRR above 10%.[1]

The cloud has proven itself with its resiliency, scalability, flexibility and speed and now underpins new technological disruptions. By 2025, "over 95% of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021."[2] At the same time, hybrid, multi-cloud and edge environments are growing, creating new distributed cloud models.

But while the cloud offers great promise, it brings new risks.

In this playbook, we'll talk about legacy versus cloud security, the types of cloud models and some cloud security best practices. Then we'll discuss everyone's favorite topic: the value of recurring revenue for MSPs and MSSPs. We'll also review some cloud security approaches, including cloud-controlled Wi-Fi, cloud security brokers, fragmented environments and network virtualization. Finally, we'll delve into emerging trends, such as industry cloud platforms and AI/machine learning.

Over 3%
of all data breaches in 2022 were caused by unsecured databases, accounting for leaks of over
800
million records.[3]

25,112
CVEs were reported in 2022
—a 4.4% increase over 2021 and a
287%
increase over 2016.[3]

> *"Unpatched vulnerabilities provide attackers with the most cost-effective and straightforward way to gain initial access into or elevate privileges within organizations."*[3]

> ***"Misconfigurations and human error continue to pose significant in the cloud."***

98.6%
of organizations have misconfigurations in their cloud environments that cause critical risks to data and infrastructure.[4]

55.1%
of organizations leverage more than a single cloud provider, and
66.7%
of organizations have public cloud storage buckets.[4]

97.1%
of organizations use privileged user access controls without MFA enforcement.[4]

68%
of organizations have external users with admin permissions to the cloud environment.[4]

74%
of MSPs
strongly or somewhat agree that their customers struggle to meet regulatory compliance requirements.[1]

44%
of MSPs
say that one-quarter of their clients have an active incident response plan, while 30% of say that half of their clients have an incident management plan in place.[1]

Cybersecurity
is the top
investment priority
for global organizations in 2023.[5]

40% say
"strong capabilities for protecting and controlling my data in the cloud"
is the top security criteria that would make them trust their cloud provider.[5]

By 2026,
60%
of organizations
will see preventing cloud misconfiguration as a cloud security priority, compared with 25% in 2021.[6]

Traditional IT Security vs. Cloud Security: A New Generation

Today's organizations now face a new problem: the perimeter-based security practices built for their on-premises environments are no match for a software-based, tightly integrated cloud environment. Why?

- **Evolve...or die –** Legacy security systems typically no longer provide updates with the latest security features. Organizations may also fear losing data and functionality by upgrading or moving to the cloud.
- **Growing technical debt –** Even if they do move to the cloud, organizations may keep legacy systems "just in case" —but forgotten security protocols may add to their technical debt over time.
- **Disappearing security talent –** Legacy systems often require in-house teams to manage security updates and respond to threats, but up-to-date security skills may be lacking due to inadequate training, complacency and resignations. Your customer may have the latest security in the cloud but fall behind with their on-premises systems.
- **The security "donut" hole –** The challenge for organizations is to evolve their people, processes and technology stacks and take a best practices-based, security-first approach as they shift to cloud-first strategies.

"Digital business assets are distributed across cloud and datacenters. Traditional, fragmented security approaches focused on enterprise perimeters leave organizations open to breaches."

Cloud Security Best Practices: Making Cloud Security Sustainable

Today's organizations now face a new problem: the perimeter-based security practices built for their on-premises environments are no match for a software-based, tightly integrated cloud environment. Why?

- **Evolve...or die –** Legacy security systems typically no longer provide updates with the latest security features. Organizations may also fear losing data and functionality by upgrading or moving to the cloud.
- **Take responsibility for configuring and maintaining your own environment.** The responsibility for securing cloud environments typically lies with both providers and customers, so it's important to have a clear understanding of roles and responsibilities. A cloud security posture management (CSPM) service can help identify misconfigurations and, with cloud infrastructure entitlement management (CIEM), identify permission issues and act as a logical progression from long-established identity and access management (IAM) and privilege access management (PAM) solutions built on least-privilege approaches.
- **Encrypt what you can and inspect all encrypted traffic.** Encryption protects sensitive traffic, but it's also a common way for threats to sneak into systems. Strong encryption and inspection capabilities will protect in both directions.
- **Log and monitor access and traffic.** Besides maintaining visibility as part of zero trust, incident response activities require comprehensive logging across all assets and services.
- **Monitor and audit configurations for all clouds and data centers.** Most misconfigurations stem from user error; automation can help keep configurations in check.
- **Run regular vulnerability scans to identify weak points.** Use an automated solution built to triage vulnerabilities by risk profile so teams can focus on the most relevant—and dangerous—issues.
- **Apply security patches as promptly as possible.** The time between a patch release and update can be a window of opportunity for attackers. To eliminate this threat vector, use cloud services that are responsible for patching.
- **Enforce zero trust security.** The tenets of zero trust—where users, applications and devices are everywhere—are built on least-privileged access and strong authentication. To secure the cloud for the future, organizations should hide applications behind a proxy, limit privileged access and broker one-to-one connections between users and applications with zero trust network access (ZTNA).
- **Have a tested response plan in place in case of a breach.** Separating backup storage from the original data source helps avoid a single point of failure and speeds remediation.
- **Secure endpoints, including mobile and IoT devices.** Endpoints remain the weakest link in the chain, making it critical to protect cloud data traveling through and between these endpoints.

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints and data—including how they access that data. But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

Cloud Services: On-Premises, Private Cloud and Public Cloud

Securing the Hybrid Model: Having the Best of Both Worlds

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints, and data—including how they access that data. But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

While as-a-service models proliferate these days—everything as a service—there are three predominant cloud service models: software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS).

Depending on the type of service model, security responsibilities will vary. For example:

- **SaaS –** Your customer purchases the use of a cloud-based application from a software provider. In this case, your customer is typically responsible only for security components associated with accessing the software—such as identity management, their organization's network security, etc.—and the software provider manages the security architecture. These components often include application security, IAM, cloud access security broker (CASB, for visibility), access controls and data protection using APIs, proxies or gateways. Examples include Microsoft 365 and Salesforce.

- **IaaS –** Your customer purchases the infrastructure from a cloud provider and then installs their own operating systems, applications and middleware, making them accountable for securing anything they own or install on the infrastructure. The provider, on the other hand, is typically responsible for securing architecture components, such as endpoint protection, CASB, vulnerability management, access management and data and network encryption. An example is Microsoft Azure.

- **PaaS –** Your customer purchases a platform from a cloud provider that they can use to develop, run and manage applications without developing or managing the underlying platform infrastructure. In this instance, your customer is typically responsible for the security associated with application implementation, configurations and permissions, while the provider is responsible for the platform security (e.g., standard cloud security architecture, as well as less common solutions). An example is Amazon Web Services (AWS).

Cloud Services: On-Premises, Private Cloud and Public Cloud

Securing the Hybrid Model: Having the Best of Both Worlds

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints, and data—including how they access that data. But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

Cloud Services: On-Premises, Private Cloud and Public Cloud

Your customer must choose the right cloud deployment model for their needs. But which one is best—on-premises, private cloud or public cloud? To make the best decision, it's important to understand that each has their advantages and disadvantages and distinguish between them:

- **On-premises data centers –** These data centers are built and maintained by your customer's IT team on the premises of their organization. They typically have full control over the infrastructure and data and are wholly responsible for securing the environment.
- **Private cloud –** Whereas on-premises data centers are physically on your customer's premises, a private cloud is hosted on remote infrastructure and is typically managed by your customer's IT team, or a managed services provider. Security measures should include encrypting data in motion and at rest, implementing access controls and multi-factor authentication and performing regular data backups. Regular security audits and vulnerability assessments should also be conducted to identify potential security risks and threats.
- **Public cloud –** In a public cloud, your customer shares the same hardware, storage and network devices with other organizations or "tenants," and they access services and manage their account via a web browser. These resources—such as compute, virtual machines, applications, database resources, enterprise infrastructure, etc.—may be free or consumption-based, depending on the service provider. Like a private cloud, public cloud offers massive scalability and cost efficiency. But it may be difficult to customize the solution to your customer's needs. In addition, misconfigurations are a significant risk to public cloud security, making it important to ensure that cloud services are properly configured and regularly audited for compliance with security best practices.

Securing the Hybrid Model: Having the Best of Both Worlds

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints, and data—including how they access that data. But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

Cloud Services: On-Premises, Private Cloud and Public Cloud

Securing the Hybrid Model: Having the Best of Both Worlds

A hybrid cloud combines both public and private cloud environments, allowing your customer to take advantage of the benefits of both models: use the public cloud for high-volume, lower-security needs and the private cloud for sensitive, business-critical operations. It's great for organizations with diverse workloads—some may require high security and others require high scalability. It also provides the cost-effectiveness of public cloud with the security and control of a private cloud. Finally, hybrid cloud enables your customer to have the flexibility needed to gradually transition to the cloud. Hybrid environments can improve your customer's security posture by better:[8]

- **Managing their security risk –** Secure their most sensitive and/or highly regulated data in a private cloud while cost-effectively storing less sensitive data with a third party.
- **Avoiding a single point of failure –** Store your customer's data across multiple clouds to reduce the risk of them losing it all to a ransomware or other malware attack.
- **Complying with data governance –** Enable your customer to better comply with regulations like CCPA and GDPR with a hybrid or multi-cloud environment.
- **Reducing the attack surface –** Use micro-segmentation to help you close gaps without having to reconfigure your customer's network.
- **Providing secure access to data and apps –** Provide your customer with direct access to specific resources, while still being governed by policy, without ever touching your customer's network.

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Consider these solutions

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints, and data—including how they access that data. But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

Cloud Services: On-Premises, Private Cloud and Public Cloud

Securing the Hybrid Model: Having the Best of Both Worlds

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Is cloud the best environment for your customer's applications? That depends on several factors. Security is key due to a cloud's large threat surface and complex configurations. The challenge is how to adopt cloud initiatives while balancing the need for security and compliance with standards and regulations. But what does it mean to ensure a secure environment? With no clear consensus on what a secure environment is, it's more important than ever to help your customer adopt a framework, like zero trust, that helps them address cloud security in a comprehensive way.

There are also regulations and standards that may impact your customer's cloud security, depending on their industry, location, manner of business, etc. Here are some of the more common ones:

- **ISO Standards –** ISO 27001 pertains to safeguarding data, but ISO/IEC 17789 (2014), 19944-1 (2020), 27018 (2019) and ISO/IEC Technical Specification 23167 (2020) all relate to cloud computing and cloud services.
- **Payment Card Industry Data Security Standard (PCI DSS) –** Pertains to organizations that store and process cardholder data.
- **Health Insurance Portability and Accountability Act (HIPAA) –** Relates to the security of individuals' health-related information.
- **General Data Protection Regulation (GDPR) –** Aims to safeguard the personal information of businesses and individuals in the European Union. Article 25 (Data protection by design and by default), Article 30 (Records of processing activities), and Article 32 (Security of process) relate specifically to public cloud environments.
- **System and Organization Controls (SOC) Reporting –** While SOC reporting is voluntary, certification does show your commitment to data security. These five trust principles relate to public cloud environments: CC2.0: Communication and information, CC5.0: Control activities, CC6.0: Logical and physical access control, CC7.0: System operations and CC8.0: Change management.

35%
of organizations
have more than 50% of their workloads in the cloud; 29% anticipate moving up to
75%
of workloads to the cloud in 12-18 months.[9]

76%
of enterprises
are now using two or more cloud providers.[9]

54%
believe that cloud security
from an independent security vendor is better than that provided by CSPs.[9]

Consider these solutions

Cloud Security Models

When discussing cloud security with your customer, it's important to understand the shared responsibility model. For example, in an on-premises datacenter, your customer typically owns security for their entire stack. As they increasingly migrate to the cloud, however, this model changes. Cloud service providers (CSPs) typically become responsible for infrastructure security (software, computing, storage, database, networking, hardware, infrastructure, etc.) while your customer is almost always responsible for securing their account, identities, devices/endpoints, and data—including how they access that data, But this will vary from provider to provider. Make sure to go over the agreement thoroughly with your customer to ensure they understand what they're responsible for and fill in any gaps where they may need additional security assistance.

SaaS vs. IaaS vs. PaaS: Choosing the Right Service Model

Cloud Services: On-Premises, Private Cloud and Public Cloud

Securing the Hybrid Model: Having the Best of Both Worlds

Cloud Security Compliance Standards: Thriving in Alphabet Soup

Consider these solutions

Check Point

- **CloudGuard for Cloud Network Security –** Get unified security management—including advanced threat prevention and automated cloud network security—across all multi-cloud and on-premises environments via a virtual security gateway.
- **CloudGuard CNAPP –** Drive pragmatic remediation with richer, more actionable context and smarter prevention, from code-to-cloud, across the application lifecycle.
- **Unified Cloud Security Compliance –** Simplify the public cloud compliance process and cut time to compliance by up to 80% with end-to-end compliance management for public cloud environments—which includes automated data aggregation and in-place remediation—with the CloudGuard Compliance Engine.

Cisco

- **Cisco+ Secure Connect –** Simplify how users, things, and applications are securely connected with a unified, fast-deploying, cloud-managed SASE solution that enables your customer to deliver unparalleled hybrid work experiences, anywhere—with no upfront investment.
- **Cisco Umbrella for MSSPs –** Establish the first line of defense against internet threats with a cloud-delivered service that gives customers on- and off-network protection from cyberattacks, including malware, phishing, ransomware and command and control callbacks.
- **Secure Cloud Analytics –** Monitor for threats and policy violations and quickly respond to security incidents in on-premises, public and hybrid cloud environments, with automated analysis and seamless workflows with the Cisco XDR platform.

CyberArk

- **CyberArk Cloud Entitlements Manager –** Reduce risk by centralizing visibility and control of permissions across your customer's cloud environments—using a dashboard to deploy remediations based on Least Privilege—and strategically remove excessive permissions.
- **CyberArk Privileged Access Management –** Address a wide range of use cases to secure privileged credentials and secrets wherever they exist—on premises, in the cloud and anywhere in between.
- **CyberArk Workforce Identity –** Secure enterprises against threats targeting cloud, mobile, on-prem, and hybrid IT environments and protect against the leading point of attack—compromised credentials—through single sign-on, multi-factor authentication (MFA) and identity lifecycle management.

Dell Technologies

- **Dell APEX Compute and HCI –** Simplify multi-cloud by providing a secure, consistent experience everywhere with the best-of-breed features and performance your customers' workloads require.
- **Dell APEX Data Protection Services –** Help customers make smarter technology choices that will improve business results and ensure their data and infrastructure stay protected and secure.

Symantec

- **Symantec Cloud SOC CASB –** Get unequaled cloud app security with the deepest visibility, tightest data security, and strongest threat protection—while simplifying and enhancing your customer's security infrastructure with built-in integrations for industry-leading Symantec DLP, Secure Web Gateway and Endpoint Security.
- **Symantec Web Protection –** Increase business agility and enhance the ROI of existing investments, policies, and expertise by supporting any mix of centrally-managed cloud and on-premises users with a complete turnkey solution—includes Cloud Secure Web Gateway (SWG), Edge SWG, Intelligence Services, Management Center, Content Analysis sandboxing, SSL inspection and high-risk isolation.
- **Symantec Network Protection –** Help customers start their SASE journeys with a comprehensive set of core SSE features that can be deployed how, when and where they see fit and provide follow-the-user protection across both cloud and Edge SWG—includes Zero Trust Network Access (ZTNA), Full Browser Isolation, Advanced Cloud Sandboxing and industry-leading SSL Decryption and Deep Content Inspection.

Trend Micro

- **Trend Vision One™ Server and Workload Security –** Optimize prevention, detection, and response for endpoints, servers and cloud workloads.
- **Trend Vision One™ Container Security –** Simplify security for your customer's cloud-native applications with advanced container image scanning, policy-based admission control and container runtime protection.
- **Trend Cloud One™ File Storage Security –** Enjoy peace of mind knowing that data files are not impacting internal systems or external reputation by leveraging innovative techniques—for example, malware scanning, integration into custom cloud-native processes and broad cloud storage platform support—to protect downstream workflows.

Veritas

- **Veritas Alta View –** Easily manage all critical data protection requirements at scale, across hybrid cloud, multi-cloud and on-premises environments, with a unified view and control over the data estate via a centralized cloud-based management console.
- **Veritas Alta Data Protection –** Get centralized control and protection across the entire data estate with the industry's broadest protection for cloud workloads, powered by Cloud Scale Technology—along with AI-powered automation, flexible recovery options, cloud-native storage technology and elastic infrastructure.
- **Veritas Alta SaaS Protection –** Protect the full range of data stored across your customer's SaaS platforms and ensure their data is quickly and easily recoverable in the event of unplanned deletion or a ransomware attack.

VMware

- **VMware NSX –** Ensure consistent networking and security for applications running in both private and public clouds by enabling micro-segmentation and a range of network and security services in this security and network virtualization platform.

The Value of Recurring Revenue for MSPs and MSSPs

Historically, MSPs and MSSPs relied on revenue from hardware sales. You sell a box, you get paid. But with typically long sales cycles, it could take months—even years—to recognize revenue. And with those hardware boxes becoming increasingly commoditized and software becoming increasingly important, wise MSPs and MSSPs have turned to new business models.

In a recurring revenue model, your company provides services (and sometimes products) to your customers in exchange for a periodic fee—sometimes known as pay as you go (PAYGO), consumption-based, or subscriptions—which are typically charged monthly, quarterly or annually. Recurring revenue is typically billed per-user, per-device or some combination. It can also be billed by type of service or as a flat fee. Finally, most companies operate on either a monthly recurring revenue (MRR) or annual recurring revenue (ARR) basis, or both.

Benefits of recurring revenue: Faster payments and financial predictability

If you haven't already, now's the time to ensure that your business incorporates some kind of recurring revenue stream. Here are some key benefits:

- **Better revenue forecasts –** Provides the ability to accurately predict future income, which helps build trust among investors and boosts corporate fundraising.
- **Better growth measurement –** Easily measure growth rates, plan recruitment and expansion, plan expenses and increase or decrease expenditures to adjust revenue.
- **Better customer relationships –** Selling to existing customers is more cost-effective than acquiring new customers who need to be educated. Plus, recurring revenue creates a standing relationship with customers which increases retention.
- **Greater financial stability –** As it represents financial stability, recurring revenue helps establish your company's worth and can guide overall decision-making.

But your customers benefit, too. Perhaps most importantly, your customer can ramp up services much more quickly. That makes it a lot easier for them to not only scale existing operations, but it also allows them to start up services without a large upfront investment—or stop them if they no longer need them. They also have better budget predictability and can much more accurately forecast their costs.

A recurring revenue model also helps your customers to continually (and proactively) assess and improve the security and compliance of their IT systems, people and processes. It gives them expert security advice that likely isn't available in all but the very largest enterprises. Regardless of the recurring revenue model used, recurring revenue is critical for successful MSPs and MSSPs as they make the move from hardware-based revenue to services revenue.

Cloud-Controlled Wi-Fi: Removing the Burden on Your Customer

Today's organizations manage an increasing array of wireless devices—laptops, smartphones, mobile devices, IoT devices, etc. For these devices to work best (and for a better user experience), organizations must have a reliable and high-performing wireless network infrastructure. But which type of wireless network will work best for your customer?

While an on-premises WLAN or cloud-managed Wi-Fi might be the ticket, a better option—typically monitored and managed by you as your customer's service provider—is cloud-controlled Wi-Fi.

With cloud-controlled Wi-Fi, your customer can skip the time and cost of running their own on-premises wireless network. Instead of taking time to procure costly Wi-Fi controllers, access points, boosters and wireless network adapters—and hiring hard-to-find network teams—your customer can put their resources to better use by having an MSP/MSSP do it for them.

An MSP/MSSP can configure, monitor and manage faraway access points, no matter where they reside. The Wi-Fi controller stretches bandwidth to enable many devices to go on the network from farther away. And by monitoring and managing the network from a single interface, access points for all your customer's sites will have the same configuration.

From a security standpoint, a cloud-controlled Wi-Fi network also reduces time and cost for your customer—and increases their productivity—by eliminating the need for them to perform their own firmware upgrades, security updates, lifecycle management and 24×7 support. They can be assured that their Wi-Fi equipment is secure and performing optimally—without their intervention.

Cloud Service Brokers: Serving Up What Customers Need: Predictability

Cloud services brokerage (CSB) is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including:

1. Aggregation
2. Integration
3. Customization Brokerage

A CSB enabler provides technology to implement CSB, and a CSB provider offers combined technology, people and methodologies to implement and manage CSB-related projects.

As with real estate and insurance brokers, cloud service brokers act as links between the customer and the provider to provide information and grease the sales process. Traditionally they've been the intermediaries between cloud providers and enterprises—for example, between AWS and your customer.

But the cloud services broker model has now shifted in response to an increased use of cloud within most organizations. IT teams, once the procurer, provisioner and manager of legacy IT systems have now shifted into the role of cloud service broker, facilitating the services that their end-users demand. Instead of brokering hardware to fit all, they're now able to provide a wealth of options to give end-users what they need.

> *Threat actors continue to find success with known and proven exploitable vulnerabilities that organizations have failed to patch or remediate successfully.*

> *...Four of the first five zero-day vulnerabilities exploited in the wild in 2022 were disclosed to the public on the same day the vendor released patches and actionable mitigation guidance.*

Cloud-Controlled Wi-Fi: Removing the Burden on Your Customer

Today's organizations manage an increasing array of wireless devices—laptops, smartphones, mobile devices, IoT devices, etc. For these devices to work best (and for a better user experience), organizations must have a reliable and high-performing wireless network infrastructure. But which type of wireless network will work best for your customer?

While an on-premises WLAN or cloud-managed Wi-Fi might be the ticket, a better option—typically monitored and managed by you as your customer's service provider—is cloud-controlled Wi-Fi.

With cloud-controlled Wi-Fi, your customer can skip the time and cost of running their own on-premises wireless network. Instead of taking time to procure costly Wi-Fi controllers, access points, boosters and wireless network adapters—and hiring hard-to-find network teams—your customer can put their resources to better use by having an MSP/MSSP do it for them.

An MSP/MSSP can configure, monitor and manage faraway access points, no matter where they reside. The Wi-Fi controller stretches bandwidth to enable many devices to go on the network from farther away. And by monitoring and managing the network from a single interface, access points for all your customer's sites will have the same configuration.

From a security standpoint, a cloud-controlled Wi-Fi network also reduces time and cost for your customer—and increases their productivity—by eliminating the need for them to perform their own firmware upgrades, security updates, lifecycle management and 24×7 support. They can be assured that their Wi-Fi equipment is secure and performing optimally—without their intervention.

Cloud Service Brokers: Serving Up What Customers Need: Predictability

Cloud services brokerage (CSB) is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including:

1. Aggregation
2. Integration
3. Customization Brokerage

A CSB enabler provides technology to implement CSB, and a CSB provider offers combined technology, people and methodologies to implement and manage CSB-related projects.

As with real estate and insurance brokers, cloud service brokers act as links between the customer and the provider to provide information and grease the sales process. Traditionally they've been the intermediaries between cloud providers and enterprises—for example, between AWS and your customer.

But the cloud services broker model has now shifted in response to an increased use of cloud within most organizations. IT teams, once the procurer, provisioner and manager of legacy IT systems have now shifted into the role of cloud service broker, facilitating the services that their end-users demand. Instead of brokering hardware to fit all, they're now able to provide a wealth of options to give end-users what they need.

> *Threat actors continue to find success with known and proven exploitable vulnerabilities that organizations have failed to patch or remediate successfully.*

> *...Four of the first five zero-day vulnerabilities exploited in the wild in 2022 were disclosed to the public on the same day the vendor released patches and actionable mitigation guidance.*

Consider these solutions

Cisco

- **Cisco+ Secure Connect –** Simplify how users, things and applications are securely connected with a unified, fast-deploying, cloud-managed SASE solution that enables your customer to deliver unparalleled hybrid work experiences, anywhere—with no upfront investment.

Dell Technologies

- **Dell APEX Storage –** Respond to your customers' changing business needs with scalable and elastic storage as a service that removes complexity and reduces risk.
- **Dell APEX Compute and HCI –** Simplify multi-cloud by providing a secure, consistent experience everywhere with the best-of-breed features and performance your customers' workloads require.

Symantec

- **Symantec CloudSOC CASB –** Get unequaled cloud app security with the deepest visibility, tightest data security and strongest threat protection—while simplifying and enhancing your customer's security infrastructure with built-in integrations for industry-leading Symantec DLP, Secure Web Gateway and Endpoint Security.

Veritas

- **Veritas Alta View –** Easily manage all critical data protection requirements at scale, across hybrid cloud, multi-cloud and on-premises environments, with a unified view and control over the data estate via a centralized cloud-based management console.

VMware

- **VMware Cloud Foundation –** Combine compute, storage, networking and management capabilities, which can be deployed in both private and public cloud environments, in a comprehensive cloud infrastructure solution.
- **VMware Tanzu Kubernetes Grid –** Enable a consistent, flexible, upstream-compatible, enterprise-grade Kubernetes environment across different clouds for a multi-cloud strategy.

Bringing It All Together: Unifying Cloud Cybersecurity

Companies have been moving data, applications and development to the cloud in greater numbers for the past several years—a trend that's been boosted since the move en masse to remote work. Today, more than ever, organizations are expanding their cloud strategies as they advance their digital transformation.

Managing multiple cloud providers in a single environment poses some challenges, such as: determining the right cloud for each workload, making cloud services fit together like a puzzle, managing costs amid complexity, ensuring data protection and privacy and keeping up with the pace of change. To address these challenges, you may want to consider a unified cloud cybersecurity platform.

Unifying your customer's cybersecurity across public, private, hybrid and multi-cloud environments provides end-to-end visibility into threats, along with a programmatic approach to addressing cloud security.

Instead of multiple disconnected dashboards, you can focus on one and receive aggregated, correlated data and analytics that bring meaning to thousands of alerts to speed resolution.

With one platform, you can pinpoint high-priority threats, calculate a risk score and receive recommended actions that relieve your customer of the manual burden of ferreting out what's important and finding a fix. The most advanced platforms can even automate remediation.

Organizations can also do more with the teams they have—an essential considering that many already face staffing shortages. Instead of acquiring specialized expertise, your customer can use automated, intelligent, integrated technology to assess and prioritize risk, integrate with leading cloud providers and cover cyberthreats across the attack surface.

A truly unified cybersecurity platform simplifies cloud security, helps detect and stop threats faster and improves your customer's security maturity.

Network Virtualization: Using Virtualization as Security

Securing a virtual network is more important than ever and network virtualization takes a comprehensive approach to securing your customer's systems and data. Network virtualization abstracts physical network hardware, creating a software-based network that essentially simulates physical network functions. These environments are often used as test environments where new network configurations or applications can be put on trial without deploying them on physical hardware. It's also a great way to create isolated environments for security testing without impacting live systems.

Network virtualization helps improve security in several ways:[10]

- **Server virtualization –** Segment sensitive data via server virtualization, reducing the risk of a data breach and making it easier to contain and remediate issues.
- **Virtual private networks (VPNs) –** Improve security by routing all network traffic through a central gateway, making it easier to monitor and control the VPN and prevent malware or denial-of-service (DoS) attacks.
- **Desktop virtualization –** Improve security by keeping all data and applications on a central server, preventing data leaks and unauthorized access to sensitive information.

Some of the most common network virtualization measures include:[10]

- **Implementing a firewall –** Block unauthorized access to your customer's network, control traffic flows and protect against malware.
- **Using encryption –** Protect data in transit as well as at rest.
- **Monitoring activity –** Monitor activity on your customer's network to detect suspicious activity and take appropriate action.
- **Creating user accounts and permissions –** Control access to your customer's network by creating user accounts and assigning permissions.

While not a "be-all, end-all," network virtualization—when used in the right way—can help segment networks, simplify network management and secure data and applications.

Bringing It All Together: Unifying Cloud Cybersecurity

Companies have been moving data, applications and development to the cloud in greater numbers for the past several years—a trend that's been boosted since the move en masse to remote work. Today, more than ever, organizations are expanding their cloud strategies as they advance their digital transformation.

Managing multiple cloud providers in a single environment poses some challenges, such as: determining the right cloud for each workload, making cloud services fit together like a puzzle, managing costs amid complexity, ensuring data protection and privacy and keeping up with the pace of change. To address these challenges, you may want to consider a unified cloud cybersecurity platform.

Unifying your customer's cybersecurity across public, private, hybrid and multi-cloud environments provides end-to-end visibility into threats, along with a programmatic approach to addressing cloud security.

Instead of multiple disconnected dashboards, you can focus on one and receive aggregated, correlated data and analytics that bring meaning to thousands of alerts to speed resolution.

With one platform, you can pinpoint high-priority threats, calculate a risk score and receive recommended actions that relieve your customer of the manual burden of ferreting out what's important and finding a fix. The most advanced platforms can even automate remediation.

Organizations can also do more with the teams they have—an essential considering that many already face staffing shortages. Instead of acquiring specialized expertise, your customer can use automated, intelligent, integrated technology to assess and prioritize risk, integrate with leading cloud providers and cover cyberthreats across the attack surface.

A truly unified cybersecurity platform simplifies cloud security, helps detect and stop threats faster and improves your customer's security maturity.

Network Virtualization: Using Virtualization as Security

Securing a virtual network is more important than ever and network virtualization takes a comprehensive approach to securing your customer's systems and data. Network virtualization abstracts physical network hardware, creating a software-based network that essentially simulates physical network functions. These environments are often used as test environments where new network configurations or applications can be put on trial without deploying them on physical hardware. It's also a great way to create isolated environments for security testing without impacting live systems.

Network virtualization helps improve security in several ways:[10]

- **Server virtualization –** Segment sensitive data via server virtualization, reducing the risk of a data breach and making it easier to contain and remediate issues.
- **Virtual private networks (VPNs) –** Improve security by routing all network traffic through a central gateway, making it easier to monitor and control the VPN and prevent malware or denial-of-service (DoS) attacks.
- **Desktop virtualization –** Improve security by keeping all data and applications on a central server, preventing data leaks and unauthorized access to sensitive information.

Some of the most common network virtualization measures include:[10]

- **Implementing a firewall –** Block unauthorized access to your customer's network, control traffic flows and protect against malware.
- **Using encryption –** Protect data in transit as well as at rest.
- **Monitoring activity –** Monitor activity on your customer's network to detect suspicious activity and take appropriate action.
- **Creating user accounts and permissions –** Control access to your customer's network by creating user accounts and assigning permissions.

While not a "be-all, end-all," network virtualization—when used in the right way—can help segment networks, simplify network management and secure data and applications.

Consider these solutions

Check Point

- **CloudGuard for Cloud Network Security –** Get unified security management—including advanced threat prevention and automated cloud network security—across all multi-cloud and on-premises environments via a virtual security gateway.

Cisco

- **Cisco+ Secure Connect –** Simplify how users, things and applications are securely connected with a unified, fast-deploying, cloud-managed SASE solution that enables your customer to deliver unparalleled hybrid work experiences, anywhere—with no upfront investment.
- **Cisco Umbrella for MSSPs –** Establish the first line of defense against internet threats with a cloud-delivered service that gives customers on- and off-network protection from cyberattacks, including malware, phishing, ransomware and command and control callbacks.
- **CyberArk Workforce Identity –** Secure enterprises against threats targeting cloud, mobile, on-premises and hybrid IT environments and protect against the leading point of attack—compromised credentials—through single sign-on, multi-factor authentication (MFA) and identity lifecycle management.

Dell Technologies

- **Dell APEX Storage –** Respond to your customers' changing business needs with scalable and elastic storage-as-a-service that removes complexity and reduces risk.
- **Dell APEX Compute and HCI –** Simplify multi-cloud by providing a secure, consistent experience everywhere with the best-of-breed features and performance your customers' workloads require.

Symantec

- **Symantec Web Protection –** Increase business agility and enhance the ROI of existing investments, policies and expertise by supporting any mix of centrally-managed cloud and on-premises users with a complete turnkey solution—includes Cloud Secure Web Gateway (SWG), Edge SWG, Intelligence Services, Management Center, Content Analysis sandboxing, SSL inspection and high-risk isolation.
- **Symantec Network Protection –** Help customers start their SASE journeys with a comprehensive set of core SSE features that can be deployed how, when and where they see fit and provide follow-the-user protection across both cloud and Edge SWG—includes Zero Trust Network Access (ZTNA), Full Browser Isolation, Advanced Cloud Sandboxing and industry-leading SSL Decryption and Deep Content Inspection.

VMware

- **VMware Cloud Foundation –** Combine compute, storage, networking and management capabilities, which can be deployed in both private and public cloud environments, in a comprehensive cloud infrastructure solution.
- **VMware NSX –** Ensure consistent networking and security for applications running in both private and public clouds by enabling micro-segmentation and a range of network and security services in this security and network virtualization platform.

Industry Cloud Platforms: Catering to Your Customer's Needs

Industry cloud platforms (ICPs) are cloud-based software solutions that cater to the specific needs of your customer's industry—needs not typically met by generic solutions or platforms. They're a collection of relevant industry solutions built and optimized for the most common industry uses.

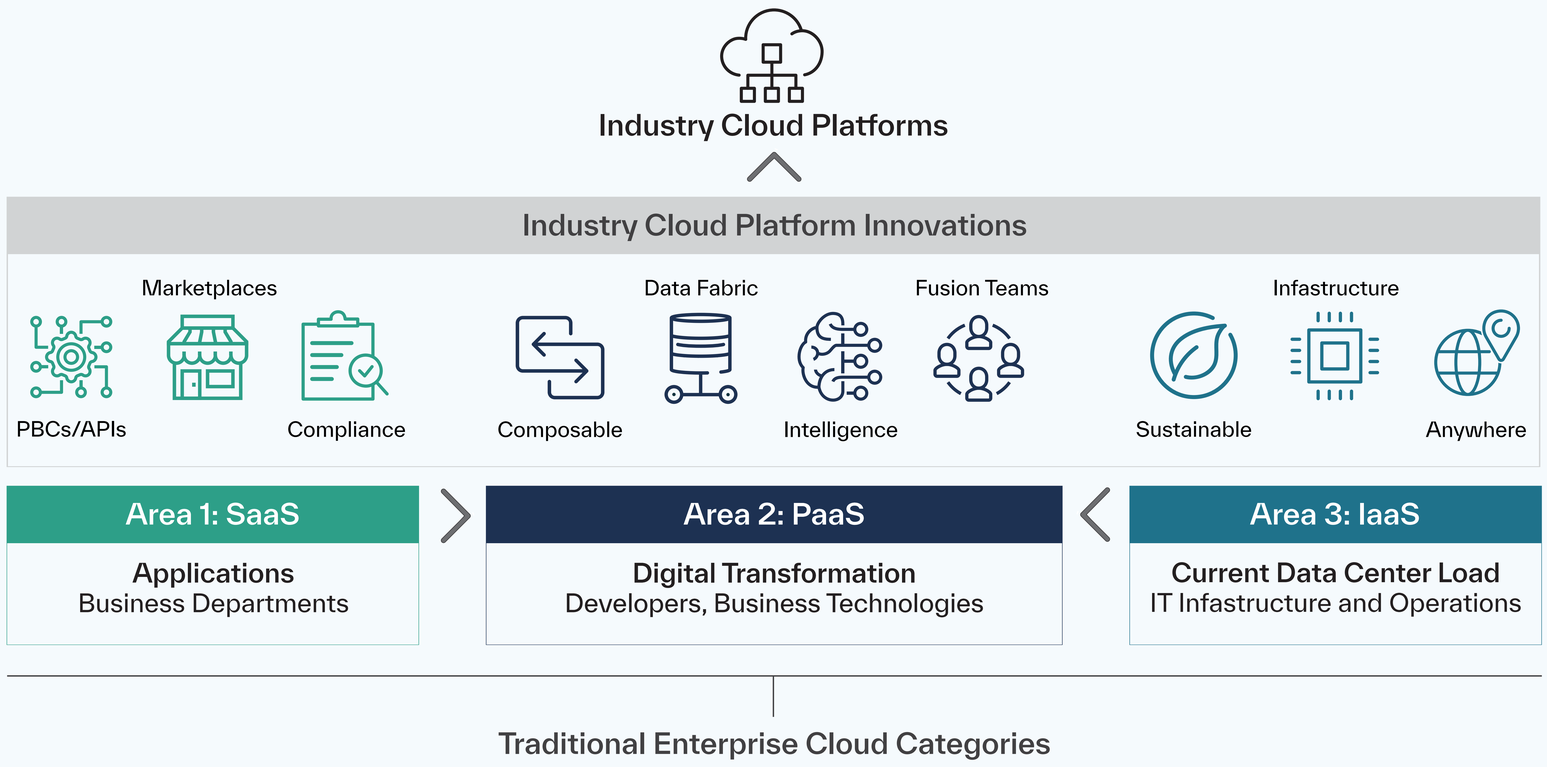
With industry cloud platforms, customization is key. Your customer can pick and choose what modules they want to use, enabling them to combine business capabilities from multiple software vendors for a custom-fit solution that fits their needs.

Address industry-relevant business outcomes by combining underlying SaaS, PaaS and IaaS services into a product offering with composable capabilities. These industry solutions typically use public cloud services, but with a more agile way to manage workloads and accelerate change given business, data, compliance or other industry needs.

In addition to increased organizational agility, faster innovation and accelerated time to value, industry cloud platforms put security first by offering enhanced security and reliability.

For example, industry cloud platforms provide a secure, private environment for your customer's data and applications, without a costly investment in infrastructure. One of the big benefits—particularly for highly regulated industries—is that they can help your customer comply with industry regulations, such as HIPAA and GDPR, to reduce the risk of non-compliance penalties.

Industry Cloud Platform Evolution



> *"...industry cloud platforms turn a cloud platform into a business platform, enabling an existing technology innovation tool to also serve...not as predefined, one-off, vertical SaaS solutions—but rather as modular, composable platforms supported by a catalog of industry-specific packaged business capabilities."*[11]

By 2027, more than 50% of enterprises will use industry cloud platforms to accelerate their business initiatives, up from less than 15% in 2023.[12]

Why Are Today's Organizations Adopting Hybrid Cloud?

What is Hybrid Cloud?

When Should I Use Hybrid Cloud?

Why Implement Hybrid Cloud?

Consider these solutions

Why Are Today's Organizations Adopting Hybrid Cloud?

What is Hybrid Cloud?

Why Implement Hybrid Cloud?

When Should I Use Hybrid Cloud?

Consider these solutions

Dell Technologies

- **Dell APEX Storage –** Respond to your customers' changing business needs with scalable and elastic storage-as-a-service that removes complexity and reduces risk.
- **Dell APEX Compute and HCI –** Simplify multi-cloud by providing a secure, consistent experience everywhere with the best-of-breed features and performance your customers' workloads require.

Veritas

- **Veritas Alta View –** Easily manage all critical data protection requirements at scale, across hybrid cloud, multi-cloud and on-premises environments, with a unified view and control over the data estate via a centralized cloud-based management console.

VMware

- **VMware Cloud Foundation –** Combine compute, storage, networking and management capabilities, which can be deployed in both private and public cloud environments, in a comprehensive cloud infrastructure solution.
- **VMware Tanzu Kubernetes Grid –** Enable a consistent, flexible, upstream-compatible, enterprise-grade Kubernetes environment across different clouds for a multi-cloud strategy.

Why are Today's Organizations Adopting Hybrid Cloud?

What is Hybrid Cloud?

Hybrid cloud is a unified, yet distributed computing model in which the network integrates various public and private cloud services—often from more than one cloud service provider—to help organize, secure, manage and optimize various workloads.

When Should I Use Hybrid Cloud?

Why Implement Hybrid Cloud?

Consider these solutions

Why are Today's Organizations Adopting Hybrid Cloud?

What is Hybrid Cloud?

When Should I Use Hybrid Cloud?

Why Implement Hybrid Cloud?

Hybrid cloud is a unified, yet distributed computing model in which the network integrates various public and private cloud services—often from more than one cloud service provider—to help organize, secure, manage and optimize various workloads.

Artificial Intelligence and Machine Learning (AI/ML): To implement cutting edge technology like AI/ML, IT leaders need cloud environments that can support these data-intensive workloads—and they're more likely to use multiple cloud providers in a hybrid structure to get all the capabilities they need.

Cost Savings: Hybrid cloud deployments provide better cost management for infrastructure based on needs, significantly lowering IT costs in the long run. In fact, a recent IDC study showed enterprises can save over $895,000[13] annually by utilizing a hybrid cloud structure.

Flexibility: Hybrid cloud powers up infrastructures so they have the capacity to meet dynamic requirements. This includes the flexibility to access a wider span of resources and switch between public and cloud environments to support business needs.

Control: Instead of entrusting all aspects of IT infrastructure to a third-party cloud provider, organizations can customize the private end of their hybrid cloud model to their specific needs and adjust them accordingly as they see fit.

Security: A good security strategy must involve the proper management of all activities which an organization needs to carry out to maximize the protection of the information it processes. Hybrid cloud networks are especially attuned forthis need, making them an ideal choice for optimizing security strategies.

Scalable: With hybrid cloud architectures, organizations have the best of both world, allowing organizations to respond to dynamic resource requirements and scale up or down depending on their peak workload periods.

Data Management: By merging infrastructure under a hybrid model, databases, applications and components are governed under a single data management umbrella that enables interoperability, enabling a simpler, more unified approach.

Why Are Today's Organizations Adopting Hybrid Cloud?

What is Hybrid Cloud? ›

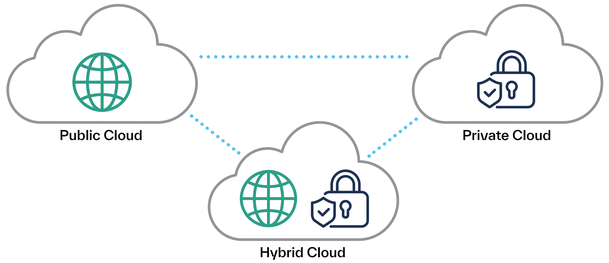
Why Implement Hybrid Cloud? ›

When Should I Use Hybrid Cloud? ›

There are six key scenarios you should look out for that can be easily addressed with a hybrid cloud computing model:

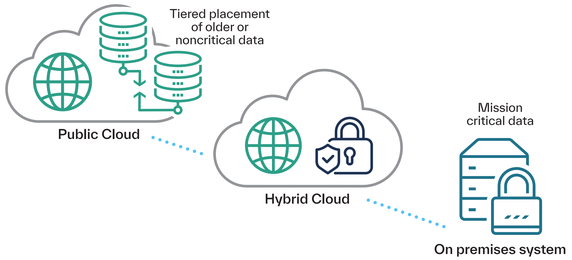
Best-of-Breed Infrastructure

Use of public cloud or on-premises infrastructure for specific workloads or components, based on what serves their needs best.



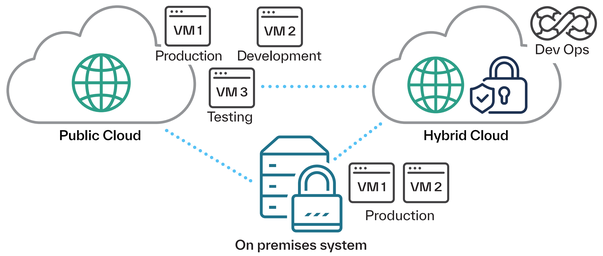
Tiering and Archive

Use of public cloud for tiered placement of older or noncritical data or workloads from on-premises infrastructure.



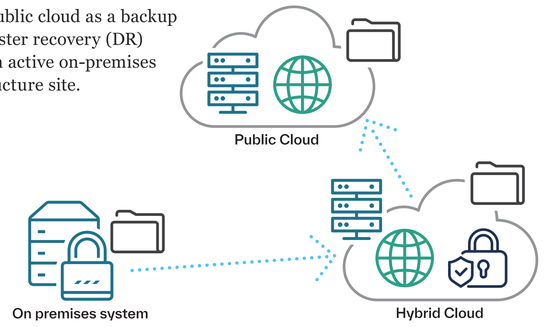
Testing, Development and Staging

Use of public cloud for development, testing and startup phases of application or upgrades, with production being placed into on-premises infrastructure.



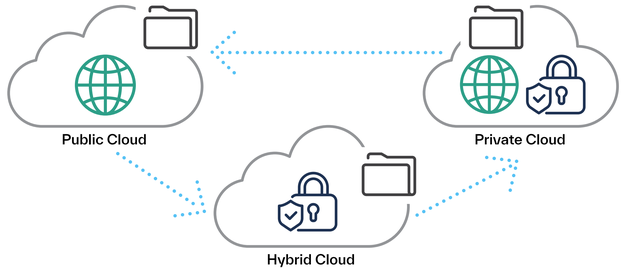
Backup and Disaster Recovery

Use of public cloud as a backup and disaster recovery (DR) site to an active on-premises infrastructure site.



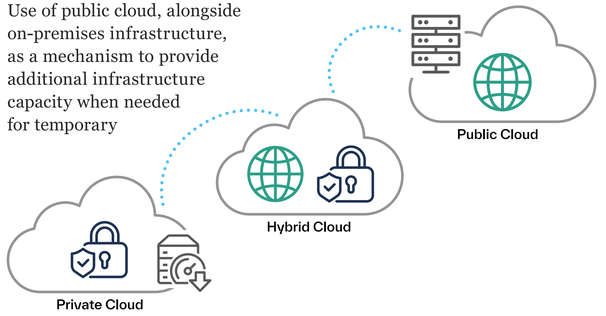
Migration

Use of hybrid infrastructure to execute a gradual migration from on-premises into public cloud infrastructure.



Bursting

Use of public cloud, alongside on-premises infrastructure, as a mechanism to provide additional infrastructure capacity when needed for temporary



Want to learn more about hybrid cloud strategy and how it can change the way you build networks? Contact our Hybrid Cloud team at MSPFAETeam@tdsynnex.com.

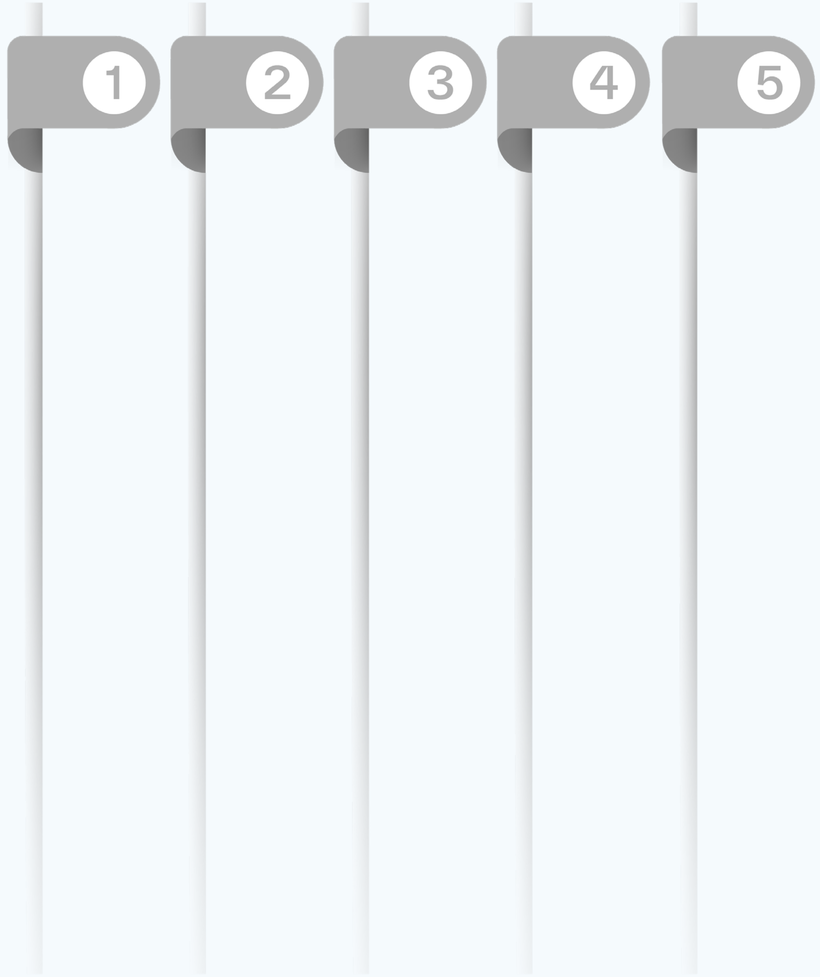
26% reported reported using multiple public clouds in 2022, up from 21% in 2021. Hybrid cloud use also **increased from 25% to 42.5%.**[14]

36% say that ensuring security across multi-cloud environments is the **greatest challenge their organization faces by using multiple CSPs.**[15]

Consider these solutions ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:



Consider these solutions

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:

1 Build a Zero-Trust Roadmap

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer's zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester or others. TD SYNNEX can help you select the right vendors to help you craft a zero-trust vision.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero-trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.

2 3 4 5

Consider these solutions

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:

1 | 2 | 3 | 4 | 5

2 Refine the Business Continuity Plan

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems (and prioritize them by the criticality of their stored data) to make it easy to structure actions in the case of a threat or attack. Create playbooks, conduct tabletop exercises and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Consider these solutions

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:

1 2 **3 Assess Their Environment** 4 5

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments and many others.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:

1 2 3

4 Offer Comprehensive Services

5

Help customers focus on their core business by leveraging our advanced managed and other security services:

- **Incident Response Services –** Comprehensive Incident Response (IR) services—including Plan Development, Readiness Review and Emergency Response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA, HITRUST, PCI-DSS, NIST 800-171, ISO 27001, NERC-CIP, SOC 1 and 2, GDPR and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations and staff augmentations to help you design the best solution for them.
- **Managed Security Services –** These managed services help you maximize limited resources:
  - **SOC as a Service:** Have a bench of cyber experts who can monitor, analyze, manage and act on threats across your customer's business.
  - **Firewall Services:** Help your customer focus on their core business while you administer, monitor and maintain their firewall infrastructure.
  - **ISAO Threat Feed:** Join a very large community of companies, local governments and security professionals to collaborate, share intelligence and participate in training and conferences and leverage competent collaborative analysis.

Consider these solutions

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:

1 2 3 4

5 Engage Through Training and Engagement Experiences

Finally, engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment.

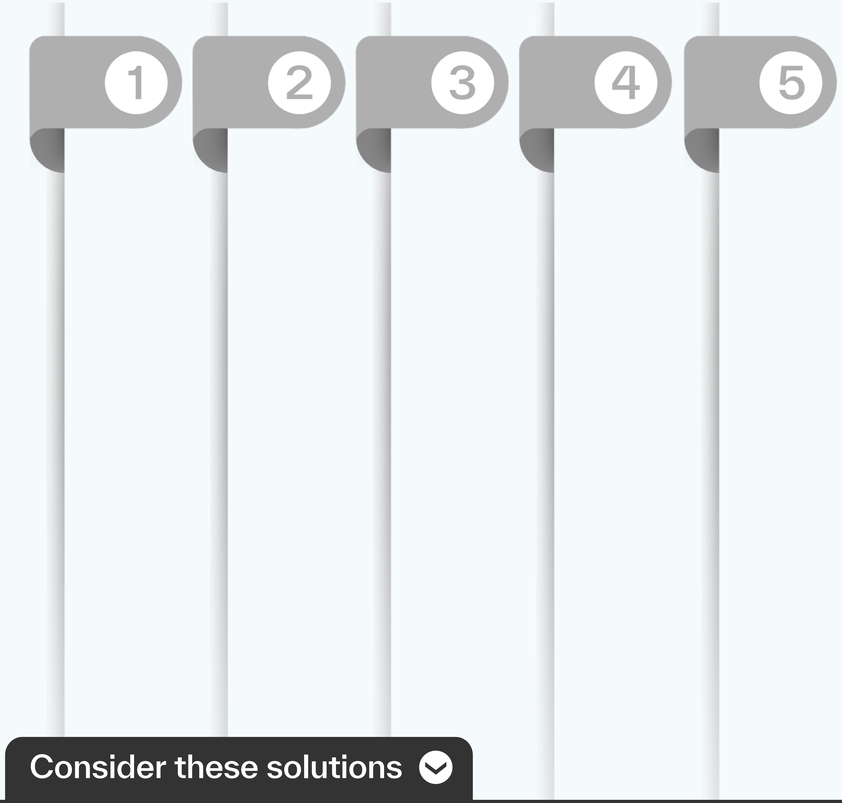
Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Consider these solutions

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Here's a plan to ensure they are well on their way:



Consider these solutions

Check Point

- **CloudGuard for Cloud Network Security –** Get unified security management—including advanced threat prevention and automated cloud network security—across all multi-cloud and on-premises environments via a virtual security gateway.
- **Unified Cloud Security Compliance –** Simplify the public cloud compliance process and cut time to compliance by up to 80% with end-to-end compliance management for public cloud environments—which includes automated data aggregation and in-place remediation—with the CloudGuard Compliance Engine.

Cisco

- **Cisco Umbrella for MSSPs –** Establish the first line of defense against internet threats with a cloud-delivered service that gives customers on- and off-network protection from cyberattacks, including malware, phishing, ransomware and command-and-control callbacks.
- **Secure Cloud Analytics –** Monitor for threats and policy violations and quickly respond to security incidents in on-premises, public and hybrid cloud environments, with automated analysis and seamless workflows with the Cisco XDR platform.

Veritas

- **Veritas Alta Data Protection –** Get centralized control and protection across the entire data estate with the industry's broadest protection for cloud workloads, powered by Cloud Scale Technology—along with AI-powered automation, flexible recovery options, cloud-native storage technology and elastic infrastructure.
- **Veritas Alta SaaS Protection –** Protect the full range of data stored across your customer's SaaS platforms and ensure their data is quickly and easily recoverable in the event of unplanned deletion or a ransomware attack.

We're Here to Help...

If your team is short on time, budget or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help to address most critical cybersecurity needs.

Our sponsors are listed on the next page, along with contact information to reach a TD SYNNEX security professional. Contact us... we're here to help.

Contact the Team

Thank You to Our Sponsors!

For more information on any one of these or other TD SYNNEX security solutions or services, contact the security professionals below.

CHECK POINT™

Ready to kickstart your security business with Check Point?
Contact us today at CheckPointBD@tdsynnex.com!

CISCO Distributor

To learn more, download
Cisco+ Secure Connect infographic, Cisco Umbrella for
Managed Security Service Providers (MSSP) datasheet
and Cisco Secure Cloud Analytics datasheet.

Or visit our Cisco Security site.

CYBERARK®

To learn more about securing identity in cloud
environments, visit our CyberSolv page
or reach out to the TD SYNNEX CyberArk Team
at CyberArk@tdsynnex.com.

DELL Technologies
AUTHORIZED DISTRIBUTOR

To learn more,
visit our Dell APEX page .

Symantec™ by Broadcom

To learn more, visit our CyberSolv page
at Symantec—CyberSolv (tdsynnex.com)
or reach out to the TD SYNNEX Symantec team
at BroadcomBD@tdsynnex.com.

TREND MICRO™

To learn more and get in touch with the team,
visit the Trend Micro page on the TD SYNNEX website.

VERITAS™

To learn more, visit our TD SYNNEX page
or contact us at Veritas@tdsynnex.com.

vmware® by Broadcom

Reach out to TeamVMware@tdsynnex.com
for more information.

References and Further Reading

1. Kaseya.com. 2022 Global MSP Benchmark Survey Report. Feb. 28, 2022.
2. Gartner. Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences. Nov. 10, 2021.
3. Tenable.com. 2022 Threat Landscape Report. 2022.
4. Zscaler. 2022 Cloud (In)Security Report. Feb. 15, 2023..
5. Google. Cloud Brand Pulse Survey Wave 5. 2022..
6. Gartner. Forecast Analysis: Cloud Security Posture Management, Worldwide. July 18, 2023
7. Gartner. Top Strategic Technology Trends for 2022: 12 Trends Shaping the Future of Digital Business. 2022.
8. Zscaler. What Is Hybrid Cloud Security? Oct. 25, 2023.
9. Check Point. 2022 Cloud Security Report. 2022.
10. ECCouncil.org. What Is Virtual Network Security, and How Can It Help Thwart Threats? Oct. 4, 2022.
11. Gartner. What are Industry Cloud Platforms? Sept. 21, 2022..
12. Gartner. Top Strategic Technology Trends 2024. 2023.
13. eIDC. The Business Value of Running Applications on VMware Cloud on AWS in VMware Hybrid Cloud Environments. October 2020.
14. Google. 2023 State of DevOps Report. 2023.
15. ESG.com. Addressing the Top Three Drivers of Multicloud Complexity. June 2023.