Mitigate Risks from Managed Service Providers in Cloud Environments

Executive summary

Managed service providers (MSPs) are businesses that deliver, operate, or manage IT services to and for customers under contract. The growth of the public cloud has encouraged the development of numerous MSPs that primarily provide these services within the cloud rather than in customer on-premises networks. Both cloud resellers and other IT vendors offer such third-party services. These MSPs offer a diverse set of services including:

- Backup and system recovery,
- Infrastructure management, and
- Security monitoring.

Because of their focus and scale, MSPs have the potential to provide services that are better tailored (e.g., higher availability or scalability, improved security, cheaper) than an organization could deliver for itself.

Using the capabilities provided by MSPs, organizations can accomplish their business objectives, including their responsibilities related to increased remote work and other changes to operating conditions. However, using an MSP can also increase an enterprise's attack surface and introduce new factors when managing risk. This cybersecurity information sheet outlines five important aspects to consider when choosing and using MSP services.

Exercise due diligence

Security in the cloud is a shared responsibility. This principle extends to the use of third-party services and capabilities as offered by MSPs. Malicious cyber actors (MCAs) are known to have an interest in targeting MSPs and using compromised MSPs to target customers. [1] Incidents have involved both MCAs associated with nation-states and others with no known affiliation. [2], [3]

MSPs, by their nature, must have access to their customers' data and resources. In many cases, MSPs will have privileged access. An MCA who has compromised an MSP may be able to use the access to pivot into customer environments. The potential for a successful pivot is increased if privileged access has been granted. Such activities are less likely to be detected because they come through a trusted MSP.

As illustrated in Figure 1, the use of managed services can open new conduits for potential malicious activities. Applying the shared responsibility model to MSPs involves understanding how MSPs protect themselves, auditing MSP activity within an organization's tenants, and incorporating use of MSP services into organizational security plans and operations.

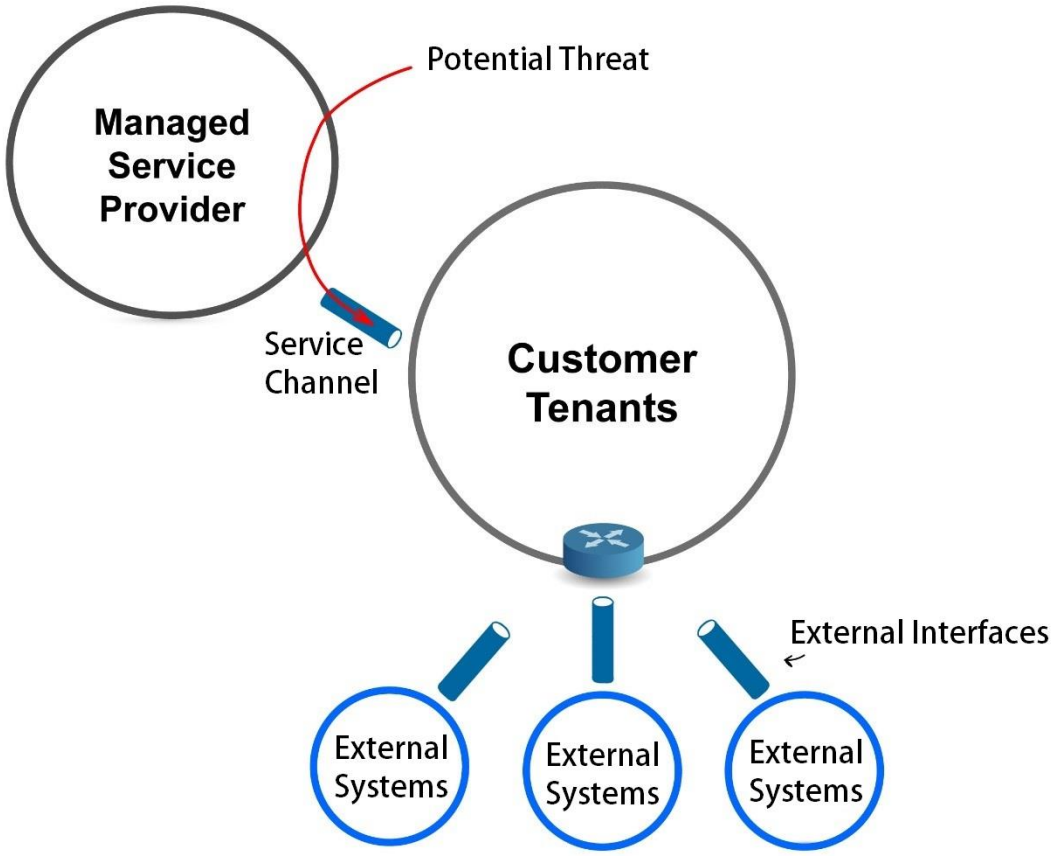

Figure 1: Impact of an MSP on an organization's attack surface

Include security considerations when choosing MSPs

When selecting an MSP, organizations should consider security and risk management as part of their criteria. Choose providers that provide visibility into their operations in

customer environments through cloud-native logging and audit mechanisms. Recognize that some services may not provide the level of visibility required. Consider what agreements, if any, related to notification and recovery if a suspected security breach occurs that different providers offer. Select providers that fit the organization's security posture.

The security posture taken by an MSP has an impact on their customers' security, particularly when the MSP has privileged access within customer tenants. Organizations often require multifactor authentication for privileged accounts and may impose additional constraints for logins by privileged users. For instance, they may restrict such logins to specific, trusted devices or from certain locations. If a customer gives an MSP privileged access, and that MSP employs less stringent access requirements, using the MSP can reintroduce risks that the customer previously mitigated.

Various organizations (including public cloud service providers, government entities, and non-profit organizations) have published security baselines and standards that provide guidance on securing cloud environments and resources. [4], [5], [6], [7] The Defense Information Systems Agency (DISA) has developed a guide that provides security controls and requirements for cloud-based solutions for use by the Department of Defense. [8] Organizations should consider which standards, policies, or practices are important to them and choose from MSPs that can attest to complying with them.

Establish auditing mechanisms

To review an MSP's activities in an organization's tenant or tenants, organizations must first understand their expected operations and how these operations trace to specific, viewable artifacts. Identity and access management (IAM) systems provide one key mechanism: the ability to view and manage security principals and their associated privileges. Consider using IAM services to audit privileges between the MSP and organizational cloud environments. See the joint CSI: Use Secure Cloud Identity and Access Management Practices for recommendations on IAM usage.

Cloud log management and analytic systems supply a second tool for auditing and monitoring MSP actions. Commercial cloud providers have services for:

- Centralizing logs from multiple sources,
- Managing storage and aging off events, and
- Querying across multiple logs.

NSA and CISA recommend MSP customers discover how the MSP's operations are reflected within cloud-native logs and audit those events. Organizations should understand the identities, accesses, and actions that an MSP makes.

Organizations must consider multiple aspects when setting up logs and analytics, including:

- Deciding the desired retention period for different logs,
- Investigating whether specific service levels impact log data availability and choosing the best level for organizational needs,
- Completing any configuration or development needed to integrate log data into the existing security infrastructure, and
- Considering measures such as the use of immutable storage to protect the integrity of critical log data.

There may be cases where security operation teams want or require data, but the MSP or cloud service provider does not provide it. Enterprises must consider operational requirements, costs, and security together to determine the best trade-offs. See the NSA CSI: Manage Cloud Logs for Effective Threat Hunting for cloud logging recommended practices.

Failure to monitor MSP accounts, privileges, or actions may leave an organization blind to their abuse by cyber adversaries. The following table lists relevant MITRE ATT&CK® tactics and techniques to consider.

ATT&CK Tactic(s)	Technique
Initial Access	Trusted Relationship [T1199]
Initial Access, Privilege Escalation, Persistence	Valid Accounts [T1078]

Integrate auditing into security operations

Once an organization establishes the information and events to track MSP services, security teams can incorporate this as part of standard security operations. For example, events that trigger an alert should be prioritized, evaluated, and resolved according to standard procedures. Hunt teams can develop baselines describing normal activity and develop analytics that trigger alerts when suspicious activity occurs.

Privileged accounts and actions associated with an MSP should be reviewed in the same manner as other privileged accounts.

Organizations may choose to build much of their base security structure upon cloud-native capabilities provided by their cloud service provider. Such services include log aggregation and centralization, security information and event management, threat intelligence information, and alerts. MSPs can also provide other security services that organizations can consider. However, organizations should consider alternatives in case MCAs find ways to disrupt them and not to depend solely on such services.

Adjust planning to incorporate MSPs

Organizations should consider how they will respond to unusual, high-impact events, such as security incidents, extended outages, or system failures. When using services from an MSP, NSA and CISA recommend considering how high-impact events might affect incident response or system recovery and adjust plans as appropriate.

In contingency planning, organizations should identify and understand the agreements provided by MSPs. Areas to consider include the responsibility of an MSP regarding the notification of suspected security incidents, such as potential breaches, and service level agreements related to remediation or recovery from security incidents or outages. Incident planners should consider what incident responders might need from an MSP in terms of data or support and how to achieve this. System recovery planners should consider how to respond if a capability failure occurs on the part of an MSP.

Recommendations

When organizations choose MSPs, NSA and CISA recommend the following:

- Adhere to important security standards as part of selection criteria when choosing MSP services.
- Choose services and service levels that provide visibility into MSP actions via IAM and log analytic systems.
- Perform and test configurations to ensure that logs and IAM information related to MSP actions are integrated into the organizational security infrastructure.
- Regularly review MSP accounts and privileges in IAM systems and investigate unusual or unexpected changes.

- Audit MSP actions via log analytics and prioritize procedures for alerting on and investigating unusual activity.
- Consider the need for MSP services if an incident occurs, and choose service levels that provide the necessary level of support.
- Perform tabletop exercises around incident response or system failures related to the MSP and incorporate the findings into incident response and system recovery plans.

Works cited

[1] ACSC, CISA, CSE, FBI, GCSB, NCSC, NSA. Cybersecurity Advisory: Protecting Against Cyber Threats to Managed Service Providers and their Customers. 2022. https://media.defense.gov/2022/May/11/2002994383/-1/-1/0/CSA_Protecting_Against_Cyber_Threats_to_MSPs_and_their_Customers_05112022.PDF

[2] Microsoft Threat Intelligence Center. NOBELIUM targeting delegated administrative privileges to facilitate broader attacks. 2021. https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

[3] N-able. White Paper: State of the Market: The New Threat Landscape. 2022. https://n-able.com/resources/state-of-the-market-the-new-threat-landscape

[4] Center for Internet Security (CIS). CIS Benchmarks List. 2023. https://cisecurity.org/cis-benchmarks

[5] Center for Internet Security (CIS). CIS Critical Security Controls version 8. 2023. https://cisecurity.org/controls

[6] Cybersecurity and Infrastructure Security Agency (CISA). Secure Cloud Business Applications (SCuBA) Project. 2023. https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

[7] National Institute of Standards and Technology (NIST). Special Publication 800-53 revision 5. 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[8] Defense Information Systems Agency (DISA). Cloud Computing Security Requirements Guide (CC SRG). 2023. https://public.cyber.mil/dccs/

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademarks

ATT&CK and MITRE and are registered trademarks of The MITRE Corporation.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk:
NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
CISA Media Inquiries: 703-235-2010, CISAMedia@cisa.dhs.gov