sysdig | Microsoft Azure

Cloud Security for Microsoft Azure

The speed of cloud-based attacks has surged as adversaries leverage automation and AI. In as little as 10 minutes, damage can be done. This guide offers a framework to help you navigate solutions for reducing risk and securing your Microsoft Azure investments, using solutions available from Azure as well as Sysdig's own CNAPP solution.

Table of Contents

Introduction

In the cloud, every second counts. Organizations using Microsoft Azure gain the ability to innovate faster, but must also ensure security keeps pace.

The speed of cloud-based attacks has surged as adversaries leverage automation and AI. In as little as 10 minutes, damage can be done. To stay secure, cloud security teams must find new ways to detect, investigate, and remediate threats faster than ever before.

Security practices are continuously evolving to address the unique challenges of the cloud. Even newer workloads like generative AI solutions are shifting the security landscape. Point solutions have evolved to address a range of capabilities, from vulnerability and posture management to workload protection. At the same time, organizations are finding value in consolidating cloud security techniques with a platform approach to achieve a single view of risk across cloud, containers, and hosts.

Cloud-native application protection platforms (CNAPP) integrate a set of security capabilities that correlate signals to gain a more complete and efficient picture of your cloud and compliance from development and production. Unifying vulnerability management, posture management, permissions and entitlement management, threat detection, and incident response increases efficiency and helps you stay ahead of cloud risk.

This guide offers a framework to help you navigate solutions for reducing risk and securing your Microsoft Azure investments. It provides insight into solutions available from Microsoft Azure and highlights how the capabilities of Sysdig's CNAPP solution complement Microsoft security solutions.

Key challenges in securing the cloud

The cloud enables teams to configure infrastructure and deploy workloads with the click of a button. This pace of change opens the door to risk, especially as threat actors are also exploiting the speed of cloud automation to launch attacks in minutes. New and unforeseen visibility gaps can complicate security and compliance. Major challenges include:

- **Misconfigurations and human error:** Misconfigurations are a significant concern in the cloud. Improperly configured cloud resources, permissions, and services can expose sensitive data or allow unauthorized access.
- **Software supply chain risk:** Adversaries target software during the development, distribution, or deployment process. Organizations often fail to implement effective security measures to prevent the introduction of malicious code or the exploitation of vulnerabilities.
- **Evolving cyber threats:** Cybercriminals are constantly evolving techniques to target cloud environments. Complex infrastructure with numerous entry points, including web applications, APIs, and user interfaces, can expose enterprises to risk if left improperly configured and unmonitored.

Microsoft Azure security approaches

Successful cloud security requires breadth of coverage across the software development lifecycle, as well as depth of analysis to protect against known and unknown threats. Coverage from hosts and containers to serverless and cloud services is key, as is the ability to correlate information about what's happening in real time.

Cloud security programs often emphasize two approaches: shift left and shield right.

- **Shift left** approaches focus on processes and tooling that are intertwined with DevOps practices. This approach promotes secure design and pre-release testing to identify security issues before they become production problems.
- **Shield right** approaches focus on operational practices, security monitoring, and mechanisms to prevent security incidents and detect and respond to events as they occur.

Shift left and shield right security practices are both essential to securing your Microsoft Azure estate, and require the following solutions:

- **Cloud workload protection (CWP)**: Identify and prioritize vulnerabilities and detect threats to containers, Kubernetes, and cloud hosts.
- **Cloud security posture management (CSPM)**: Flag misconfigurations and automate their remediation. Continuously track security and compliance progress.
- **Cloud detection and response (CDR)**: Detect attack patterns across containers, Kubernetes, and cloud. Protect workloads against runtime threats.

The key practices incorporated in the above solutions all come together with a cloud-native application protection platform (CNAPP) for Microsoft Azure. The following sections highlight the key capabilities of CNAPP — all of which contribute to helping you achieve end-to-end security in your Microsoft Azure environment.

Vulnerability management

Vulnerability management is a crucial aspect of security for workloads running in the cloud, and is considered key to both CSPM and CWPP practices. Scanning for software flaws and known security issues is a must-have step in the application lifecycle to prevent security breaches.

New vulnerabilities are constantly being disclosed. Adopting a comprehensive vulnerability assessment approach is key to identifying and addressing issues throughout the software development life cycle (SDLC).

Assessing the security of modern applications requires finding and fixing problems early. This means scanning during development phases and continuing to scan for vulnerabilities through runtime. Checking for issues at each stage helps identify vulnerabilities missed during earlier stages or introduced during runtime, as well as risks disclosed after your last scan.

Full lifecycle vulnerability management means scanning for issues at different stages and locations:

- Local scans on developer machines
- Continuous integration and continuous delivery (CI/CD) pipeline scans
- Registry scans
- Runtime scans

Shift-left security challenges

Shift-left security has a noise problem. Organizations start their journey with pre-release scanning tools and quickly drown in a deluge of scanner output. It's a struggle to find an efficient way to pass or fail application releases.

Development and security teams must sift through and vet findings to prioritize flaws that are severe and actionable. The work is tedious, stealing time from more important tasks. Addressing the pitfalls of security testing isn't simple. Teams need as much contextual information as possible to begin to reason about the risk associated with each finding.

Microsoft Azure vulnerability management solutions

Microsoft Azure provides solutions that focus on identifying vulnerabilities to help cloud users remediate known issues and minimize the window of opportunity for attackers.

Microsoft Defender Vulnerability Management delivers asset visibility, intelligent assessments, and remediation recommendations to mitigate risks.

Microsoft Defender for Cloud scans images that are pushed to a registry or imported into a registry, or any images pulled within the last 30 days.

Vulnerability management for Microsoft Azure with Sysdig

Sysdig incorporates vulnerability management into the various stages of the development process and runtime. In addition, it helps Microsoft Azure users prioritize risk and consolidate host and container image scanning into a single workflow to save time and money.

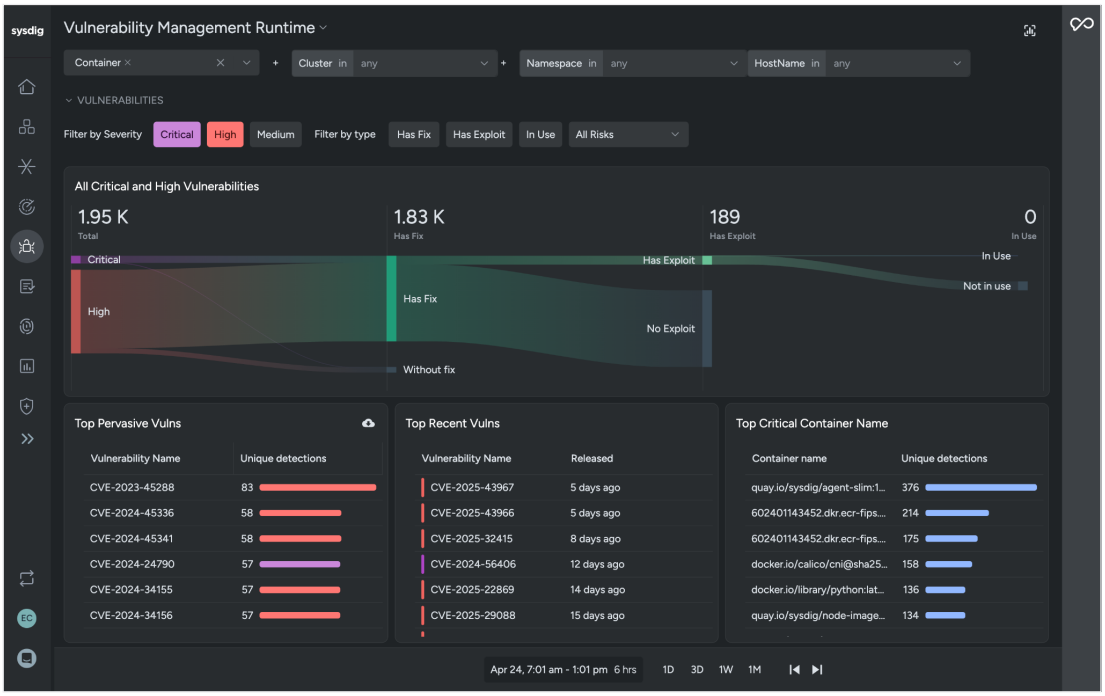
- CI/CD pipeline scanning: Vulnerability scanning in the CI/CD pipeline evaluates container images as a build step before pushing to a registry. As an additional gate, you can fail builds that don't pass the security policy evaluation.
- Registry scanning: Registry scans ensure that container images and artifacts are checked for vulnerabilities before running in production on Microsoft Azure.
- Runtime scanning: Scans for vulnerabilities at runtime to identify issues not identified during earlier stages, introduced during runtime, or disclosed after the last scan occurred.

Prioritizing vulnerabilities with runtime insights

To help teams stay ahead of vulnerability threats, adding context to identify in-use vs. dormant vulnerable packages helps reduce noise and spotlight actual risk. Sysdig's runtime insights deliver this visibility by profiling containers and making this information available to vulnerability management and application security (AppSec) tools.

Runtime insights are accessible within Sysdig's CNAPP, but are also used by third-party AppSec solutions. Industry AppSec leaders, including Snyk, Checkmarx, Mend.io, and Docker, have integrated with Sysdig to prioritize in-use vulnerabilities and eliminate threats faster.

Figure 1:
Runtime vulnerability management



Agentless and agent-based scanning

Organizations are often hesitant to install and maintain agents to deliver needed functionality. Where possible, teams want to utilize an agentless approach. Agentless security scanning relies on cloud provider APIs to collect information and perform vulnerability assessments.

The drawback of agentless scanning is that it typically lacks real-time visibility. This means that teams may lack information about intermediate states of the system between scans. In addition, agentless is typically unable to provide insights into whether a vulnerable package is used in a running environment.

Sysdig integrates both agentless and agent-based options:

- Agentless scanning leverages Microsoft Azure APIs to discover and scan resources.
- Agent-based scanning uses a lightweight package to provide both node-based scans and runtime visibility.

Both options can be used in tandem. With this approach, the agent profiles workloads to identify in-use packages. This information is used by the agentless scanner to prioritize vulnerabilities.

To learn more, read Securing the Cloud: A Guide to Effective Vulnerability Management.

Cloud security posture management

According to Gartner®, "through 2025, over 99% of cloud breaches will have a root cause of a customer misconfiguration or mistake.[1]" Cloud security posture management (CSPM) helps provide visibility into your cloud configurations to identify and remediate risks, and to proactively safeguard your Microsoft Azure environment.

Ensuring secure cloud configurations

Posture management is a cornerstone of any cloud security strategy. Cloud misconfigurations leave your business exposed to risk. Wrongly configured hosts, container runtimes, clusters, storage, or cloud resources create an easy way to escalate privileges and perform lateral movement. Evaluating your Microsoft Azure accounts and services against benchmarks and posture controls helps you detect when resources deviate from security best practices.

Rather than performing manual evaluation and remediation of cloud configurations, CSPM solutions can automatically assess the state of your cloud configurations and provide a readout of risky misconfigurations. In some cases, CSPM will also automate remediation by updating or disabling flawed configurations.

Securing infrastructure as code (IaC)

Tools like Terraform that enable infrastructure as code (IaC) have become a core component of IT provisioning and administration in the cloud. Validating IaC configurations is another key component of CSPM.

IaC security tools and practices allow engineers to find and remediate security problems within IaC templates. The goal is to minimize the risk of inadvertently introducing security problems via IaC. IaC security is a part of posture management in that it introduces governance designed to mitigate security risks.

Kubernetes security posture management

Kubernetes security posture management, or KSPM, is the use of security automation tools to discover and fix security and compliance issues within any component of Kubernetes. You can think of KSPM as CSPM for Kubernetes environments. KSPM analyzes Kubernetes resources and host configurations, in addition to Kubernetes audit logs, to help you prevent and remediate security risk in your cloud-native infrastructure.

With a cloud-managed Kubernetes service such as Azure Kubernetes Service (AKS), Microsoft Azure manages the Kubernetes control plane. Therefore, security posture is managed by Microsoft Azure. For other aspects of an AKS environment, such as worker nodes, your organization is responsible for hardening, patching, and managing the security updates. For a fully self-hosted Kubernetes environment, you'll have to manage the security posture of the complete environment.

1 Gartner, Risk-Based Evaluations of Cloud Provider Security, Charlie Winckless, Jay Heiser, 16 January 2023.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Managing permissions and entitlements

Overly permissioned cloud accounts and roles pose another critical security problem. Identity and access management (IAM) is critical for helping Microsoft Azure users lock down access to avoid the risk of data breach, privilege escalation, and lateral movement.

As you increase the use of services and features on Microsoft Azure, it becomes harder to know exactly what the least privileged entitlements should be. Permissions are often misconfigured, allowing unnecessary access rights.

Carefully assigning the correct permissions is fundamental to addressing identity risks in the cloud and achieving the practice of least privilege in your Microsoft Azure environments. Cloud infrastructure entitlement management (CIEM), considered a key CSPM capability, is specifically designed to address the complexity of maintaining permissions in cloud environments.

98%

Sysdig's 2024 Cloud-Native Security and Usage Report found that 98% of permissions granted are unused.

Microsoft Azure CSPM, IaC, and CIEM solutions

Microsoft Azure solutions for posture management and code security help cloud teams aggregate security findings, analyze configurations and code, and identify permission issues.

Microsoft Defender for Cloud provides a range of security capabilities to help you secure your Azure cloud, including:

- Visibility into the security state of your cloud assets and workloads and hardening guidance to help you improve your security posture.
- IaC scanning for repositories in Azure DevOps to find vulnerabilities in code.
- Identity discovery, permissions visibility, and entitlement governance to address risks associated with permission misconfigurations.

Posture management for Microsoft Azure with Sysdig

Sysdig's CSPM solution continuously manages cloud infrastructure and identity risks by identifying and enabling the remediation of misconfigurations in the cloud control plane, cloud resources, cloud-deployed workloads, and permissions.

Security best practices and compliance

Sysdig helps you proactively assess target environments against security and compliance standards, common frameworks, regulatory requirements, and your internal company policies.

Sysdig features over 80 built-in posture assessments, including the following standards:

CIS Microsoft Azure Foundations Benchmark	CIS Azure Kubernetes Service (AKS) Benchmark	Center for Internet Security (CIS) Benchmarks for Linux, Kubernetes, Docker, etc.	Defense Information Systems Administration (DISA) Security Technical Implementation Guide (STIG)	Digital Operational Resilience Act (DORA)
Federal Risk and Authorization Management Program (FedRAMP)	General Data Protection Regulation (GDPR)	Health Insurance Portability and Accountability Act (HIPAA)	Health Information Trust Common Security Framework (HITRUST CSF)	ISO/IEC 27001
National Institute of Standards and Technology (NIST)	Network and Information Security (NIS) Directive (NIS2)	NSA/CISA Kubernetes Hardening Guide	Payment Card Industry Data Security Standard (PCI DSS)	System and Organization Controls (SOC)

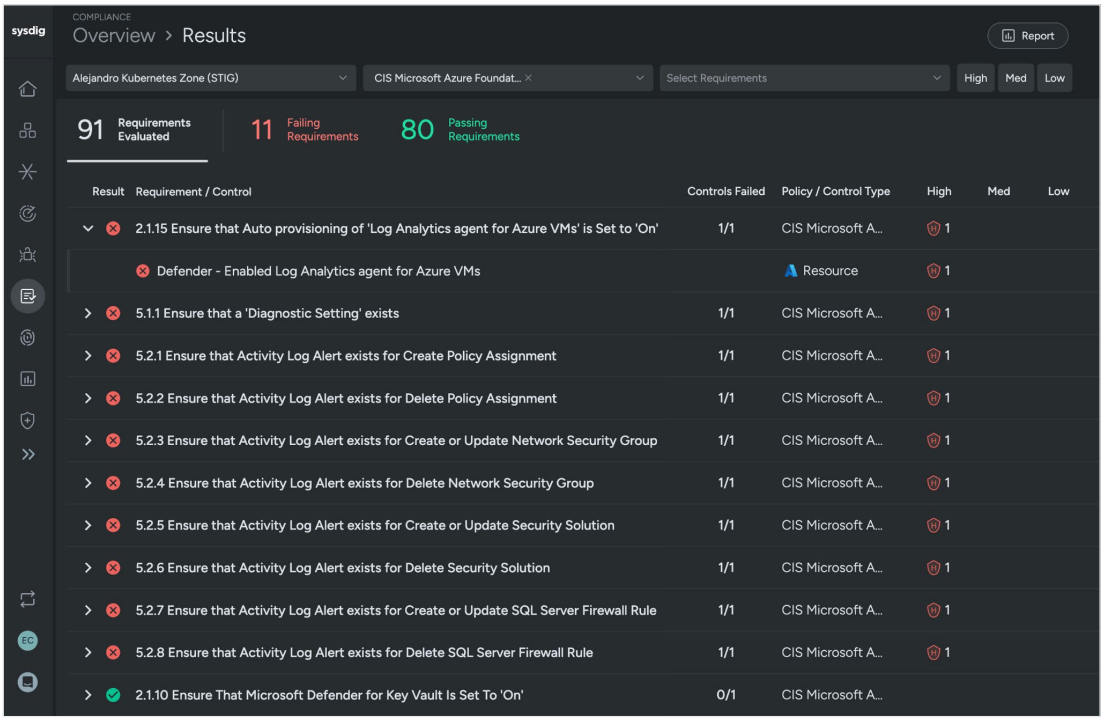


Figure 2: Microsoft Azure security posture report

The Sysdig platform discovers and presents you with a full cloud inventory so you can assess risk and compliance for assets, including IaaS, PaaS, hosts, containers, vulnerabilities, identities, and more. You can search and filter assets based on both static risk factors (e.g., public exposure, permissions) and dynamic ones (e.g., in-use packages).

Active cloud risk

CSPM requirements have shifted as cloud adoption has accelerated. The industry is moving beyond periodic posture checks to continuous posture assessments to identify, prioritize, and mitigate active cloud risks. Static checks are important, but given the speed of attacks in the cloud, these periodic point-in-time assessments can leave visibility gaps of hours or more.

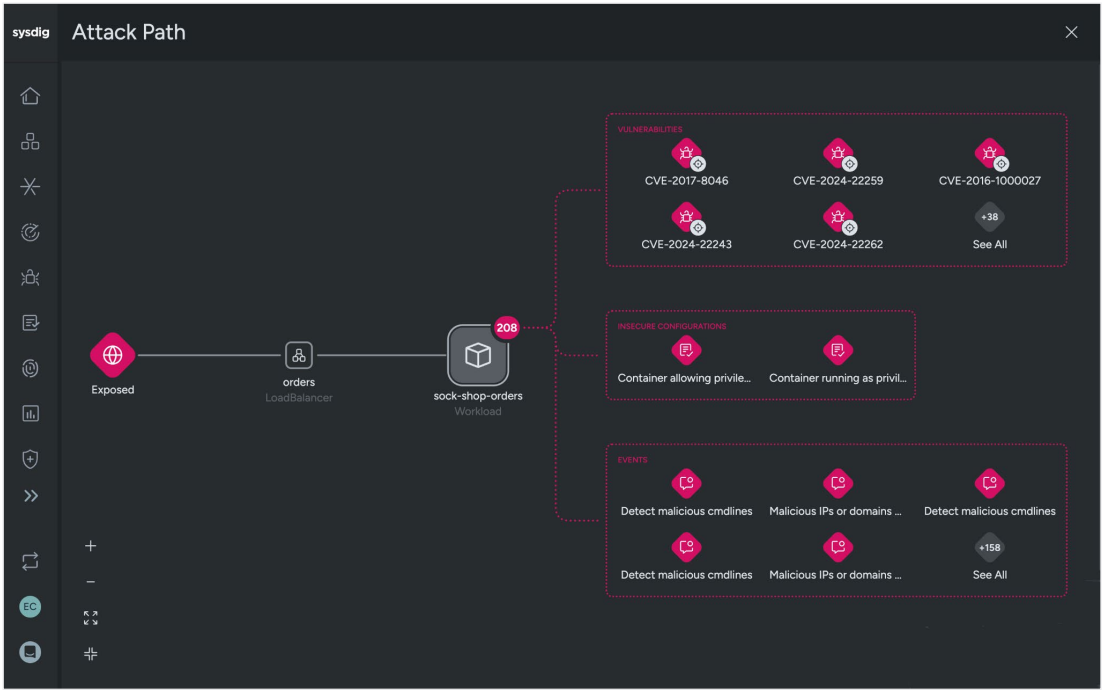
Sysdig enables practitioners to spot active movement and dynamic changes to mitigate active cloud risk. Active cloud risk includes real-time activities and dynamic changes in your environment, such as:

- Risky identity behavior (e.g., user actively logging in with no MFA)
- Real-time configuration changes (e.g., connecting to a known malicious network)
- In-use permissions (e.g., high-privilege access activated with no prior use)
- In-use packages with critical vulnerabilities (e.g., actively running software packages with high CVSS vulnerabilities)
- Workload threats (e.g., public encryption key uploaded)

Sysdig enriches static risk findings and overlays active risk information for prioritization, investigation, and remediation. The riskiest combinations of static and active risks to your Microsoft Azure are surfaced and attack path visualization helps speed up investigations. Guided remediation is integrated into the workflow to help security teams fix issues quickly.

With Sysdig's Attack Path Analysis visualization, you can view interconnected risks and exploitable links across resources, with active risks and events overlaid on static risks.

Figure 3:
Visualizing a cloud attack path with real-time insights



Infrastructure-as-code security

Sysdig maps assets and resources to your IaC manifest files to provide security insights, enable drift detection, and support the remediation of violations in your environment. For discovered violations, Sysdig generates tailored remediation suggestions that you can use to fix issues via pull requests and integration with your Git tooling.

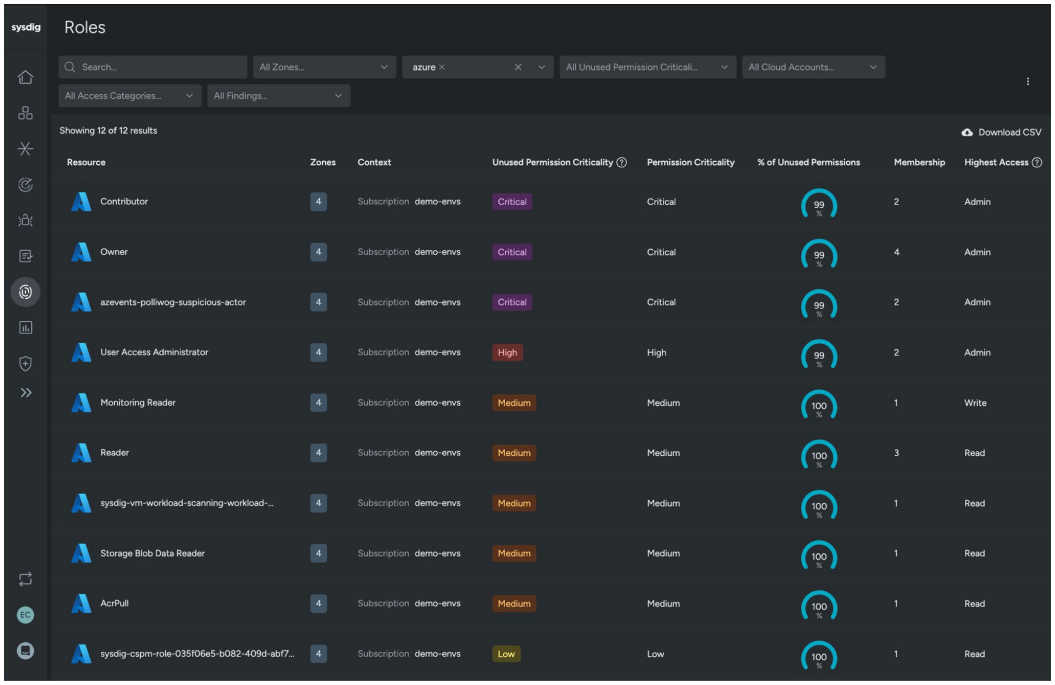
Entitlement management

Sysdig analyzes your cloud permissions to create a profile of your cloud users, roles, and policies. Audit logs analysis reveals the executed cloud commands in your Microsoft Azure accounts and correlates this activity with policies, roles, and users. This visibility gives you insight into overly permissioned identities that may present the risk of credential misuse.

An identity and access dashboard informs you about:

- The total permissions given and used.
- How many users are inactive, and which users to consider deleting.
- The averages of permissions per policy and policies per user.
- The policies, users, and roles with the worst cases of unused permissions.

Figure 4: Microsoft Azure entitlement and permission management



Sysdig translates its permission analysis into policy suggestions that you can use to reduce excessive permissions and limit granted access to only what is needed.

To gain more insight into effective posture management for Microsoft Azure, read 5 Essential Capabilities for a Modern CSPM Solution.

Cloud detection and response

The ability to stop cloud attacks is critical as organizations continue to shift into larger and more complex cloud estates. Detection and response have been disrupted by alert noise and visibility gaps, often due to legacy EDR tooling. Cloud services, ephemeral containers, and identity sprawl create a dynamic and complex environment that can prove difficult to protect.

Cloud detection and response (CDR) provides proactive defense against cyberattacks that target cloud infrastructure and data. It involves the continuous monitoring of cloud systems for potential threats, the assessment of severity, investigation capabilities, and the implementation of countermeasures to prevent or mitigate impact.

Adversaries can exploit weaknesses in minutes of exposure. The key to effective CDR is the ability to identify, in real time, any malicious activity across workloads, identities, cloud services, and third-party apps, thereby detecting threats across the cloud fabric.

Microservice architectures running on containers and orchestrated by solutions like Kubernetes make applications faster to develop and easier to scale. However, monitoring container activity is exponentially more complex. Containers may be distributed across multiple instances and hosts and run programs in an isolated context. Getting visibility into activity requires unique instrumentation. Security instrumentation should be able to collect data in real time, but also shouldn't require modification to your container images to gain visibility.

Beyond having the right technology, organizations also need to establish processes and ensure staff have the skills required to act swiftly to keep cloud systems and data secure.

With a sound CDR strategy in place, Microsoft Azure users can:

- Reduce the risk of breaches
- Meet compliance requirements
- Reduce time to detect and respond
- Reduce cost, increase productivity, and securely accelerate innovation

One of the key security frameworks cloud teams can leverage to guide detection and response security strategies is the MITRE ATT&CK framework. It offers detailed, actionable information about attacker behaviors and techniques to help security teams proactively secure their cloud assets in an evolving landscape.

Read MITRE ATT&CK and D3FEND for Cloud and Containers to learn more.

10 Minutes to Pain

Targeted cloud attacks occur on average within 10 minutes of credential discovery.

Microsoft Azure threat detection, investigation, and response solutions

Microsoft Azure solutions for detection, investigation, and response enable you to detect cloud threats and gain a more complete understanding of the security of your workloads, applications, and data.

Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to protect against attacks.

Microsoft Azure Sentinel is a cloud-native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution that provides security collection, detection, investigation, and response capabilities

Cloud detection and response for Microsoft Azure with Sysdig

CDR capabilities for Microsoft Azure from Sysdig focus on empowering analysts to guard against accelerated and complex cloud threats. Security teams gain deep visibility, context, and real-time detection capabilities built for the cloud and cloud-native workloads.

Built on Falco open source software, Sysdig's CDR provides advanced detection and response capabilities across cloud logs, containers, Kubernetes, serverless computing, and cloud hosts. It detects threats in real time and correlates context across multiple domains to help analysts rapidly investigate, identify, and respond to threats.

Security for Microsoft Azure services

Microsoft Azure provides over 200 cloud services — including compute, storage, databases, analytics, networking, developer tools, management tools, security, and enterprise applications — to meet a wide range of use cases. To help you enable operational and risk auditing of your Microsoft Azure accounts, Microsoft Azure Platform Logs record actions taken by users, roles, and cloud services. This is a key component of security for Microsoft Azure services.

As your use of cloud services and infrastructure grows, Sysdig helps you automate the evaluation of Cloud Audit Log events in real time using a flexible set of security rules. By continuously monitoring CloudTrail logs, you can detect and report suspicious cloud activity and events across a wide range of Microsoft Azure services.

In addition, Sysdig correlates identity behavior with security events to help identify and manage compromised identities. Sysdig Cloud Identity Insights enables teams to outpace attackers by swiftly prioritizing and responding with suggested containment actions.

Security for Microsoft Azure container services

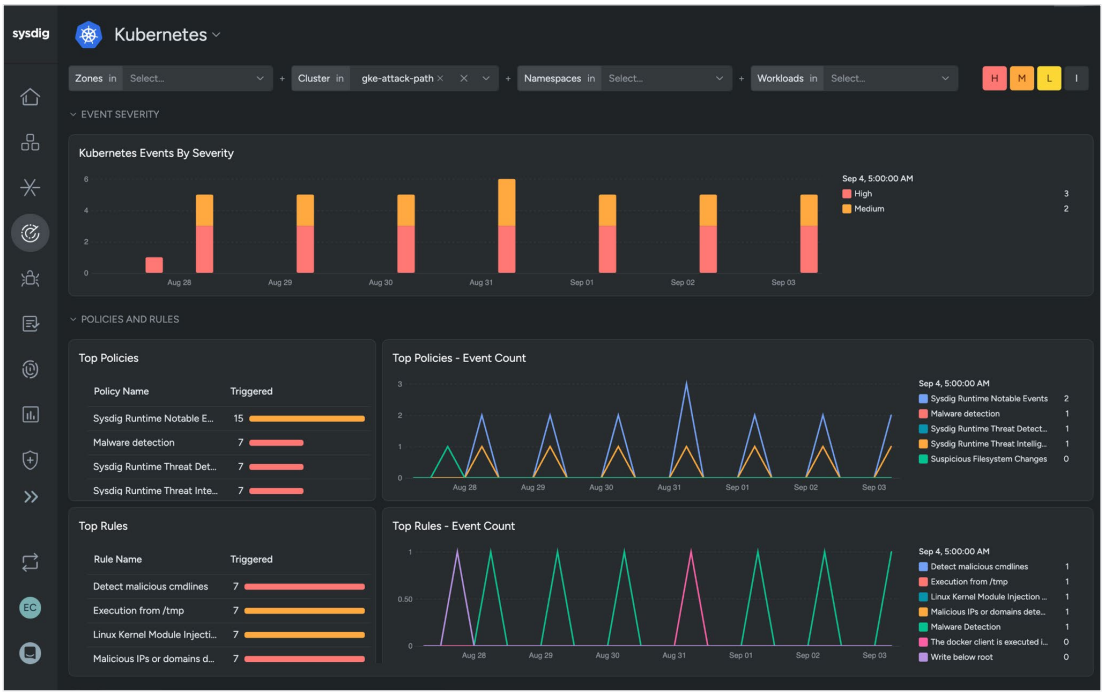
Sysdig has extensive expertise in container security and provides deep visibility to more easily detect threats, block attacks, and speed incident response for containers on Microsoft Azure, including **Azure Kubernetes Service (AKS)** and **Azure Red Hat OpenShift**.

Sysdig employs kernel-level instrumentation to provide the most comprehensive runtime security for containers, including visibility into process creation, file system activities, network traffic, and more. It incurs a low overhead compared to user-space techniques, reducing impact on the overall system.

The Sysdig agent natively integrates into the container runtime API and Kubernetes API, enabling metadata collection and enrichment of generated events. Any event detected includes extensive information about affected assets, including the container name, Kubernetes cluster to which it belongs, pod, namespace, and service/deployment. Further enrichment is possible if you connect your Microsoft Azure accounts to correlate things like cloud account, cloud resource type, security group, and region.

Runtime security policies can be configured to stop containers to immediately block a threat if specific activities are detected. In addition, a capture file that records all system activity from before, during, and after an event can be saved to enable post-event forensics and investigation.

Figure 5:
Kubernetes and container security overview



Serverless container security for Microsoft Azure Container Apps

Serverless computing brings unique requirements for detection and response. Without access to a server host operating system, traditional agent-based instrumentation cannot be utilized. Sysdig uniquely solves the serverless visibility challenge for Microsoft Azure Container Apps.

- Serverless workload agents monitor each Azure Container Apps job for security events and enforce security and compliance policies.
- A serverless orchestrator agent collects information from serverless workload agents and sends it to Sysdig SaaS so security teams can view events and take action.

Forwarding security events to SIEM and security data lakes

Security information and event management (SIEM) and data lake solutions are used by security operations teams to store massive amounts of security-related data from various sources within an organization, and are used for security monitoring, analysis, and compliance use cases.

Sysdig integrates with numerous SIEM and data lake solutions, including Microsoft Sentinel, enabling you to store enriched multi-platform cloud security events on Microsoft Azure where you can use your preferred analytics tools to analyze your security data.

The 555 Benchmark for Cloud Detection and Response

Given the speed of attacks in the cloud, users must measure their effectiveness in new ways. The 555 benchmark — 5 seconds to detect, 5 minutes to triage, 5 minutes to respond — challenges Microsoft Azure users to acknowledge the realities of modern attacks and to push their cloud security programs forward. Achieving 555 requires the ability to detect and respond to cloud attacks faster than adversaries can complete them.

- Detect threats within 5 seconds. Organizations should be able to gather detection signals from their cloud security tools in real time to ensure visibility into ephemeral assets.
- Correlate and triage within 5 minutes. Teams should be able to gather full context for all correlated signals within 5 minutes of receiving the first relevant alert.
- Initiate a response within 5 minutes. Organizations should be able to initiate a tactical response within 5 minutes of confirming that an attack is in progress.

Visit the 555 benchmark page to learn more.

Cloud security and generative AI

Generative AI (GenAI) is a top priority for organizations seeking to increase productivity and solve business problems. AI has the potential to aid cloud security by helping teams get a better understanding of risks and security issues, and even making security operations and response times faster. At the same time, organizations must find ways to manage the unique cybersecurity risks associated with operating GenAI and large language model (LLM) applications.

AI security risks

GenAI presents great potential, but also comes with numerous security risks spanning privacy, cyberattacks, regulatory compliance, and breach of intellectual property. Some believe that AI may lower the barriers for threat actors to carry out sophisticated attacks and manipulate AI systems to compromise the system's integrity.

Because vast amounts of data are used and produced by AI, companies need to guard against issues such as unauthorized access and misuse, potentially breaching privacy regulations. To address these risks, enterprises must move toward maintaining the security, confidentiality, and integrity of AI, and carefully determine how best to prevent, detect, and respond to unauthorized access and adverse events.

Compliance frameworks for GenAI and LLMs

With AI becoming integral to countless aspects of business and society worldwide, concern over its impact on areas such as privacy, consumer rights, and national security has emerged. Governance frameworks and best practices intended to ensure the safe, private, and ethical use of AI are being developed to manage AI's expansive influence and mitigate associated risks.

Frameworks from organizations like NIST, MITRE, and OWASP seek to help those adopting AI guard against known risks and misuse. In addition, AI security regulations from around the world are in development or have already been implemented. These initiatives support a broader global trend towards addressing both the opportunities and challenges posed by AI.

Read The Race for Artificial Intelligence Governance to learn more.

AI as a security assistant

Microsoft Azure users are looking toward generative AI (GenAI) and large language models (LLMs) to enhance security operations by prioritizing risks, speeding response, and simplifying cloud security. AI can generate actionable insights that help teams get a better understanding of risks and security issues, and make security operations and response times faster. In addition, they can enable less experienced security personnel to handle complex tasks and improve overall cyber defenses through proactive risk investigation.

Microsoft AI solutions for security

Microsoft Azure provides solutions and recommendations for both securing AI use and using generative AI to aid cloud security.

Microsoft Security Copilot helps summarize data signals into insights with AI-driven guidance and analysis across identities, devices, data, clouds, and apps

Sysdig security solutions and AI

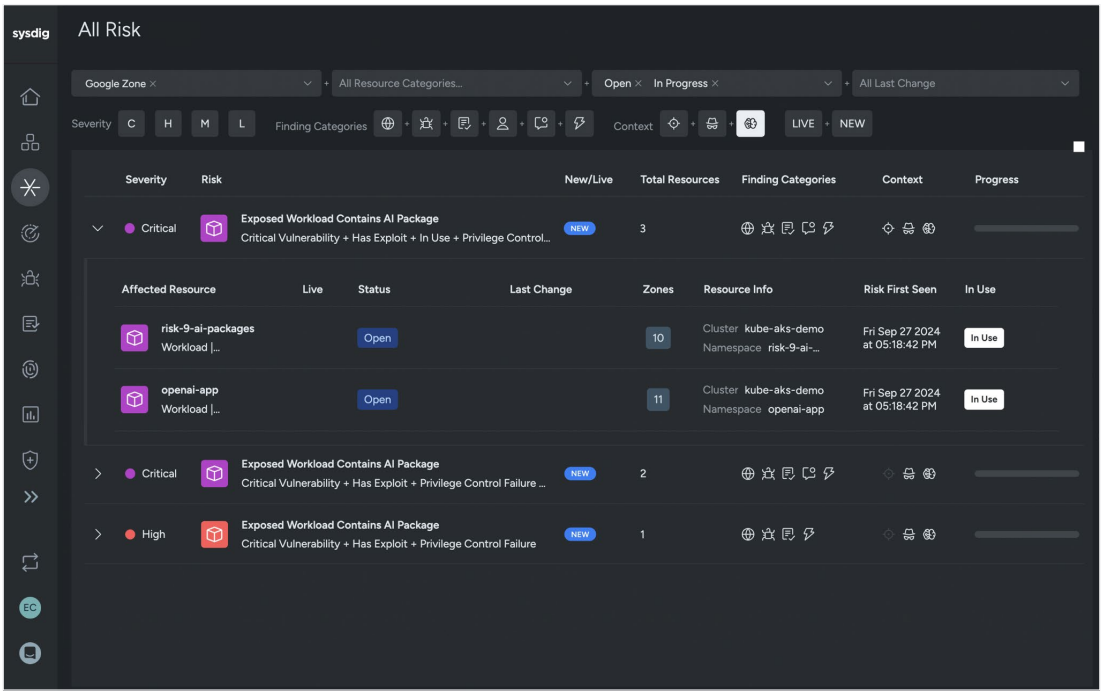
AI workload security with Sysdig

Sysdig provides AI workload security that helps companies securely adopt GenAI. Sysdig's solution allows security teams to identify and prioritize AI workloads in their environment. This includes support for the leading AI engines and supporting software packages, including OpenAI.

AI workload security provides the visibility needed to establish data security measures that combat the risk of ungoverned AI deployments and shadow AI that may expose trade secrets, proprietary information, and customer data through unauthorized access to AI workloads. A comprehensive view of correlated risks and events helps you quickly understand risk factors, including:

- Publicly exposed AI workloads
- In-use AI packages with critical vulnerabilities
- High-confidence threat events

Figure 6:
AI Workload Security



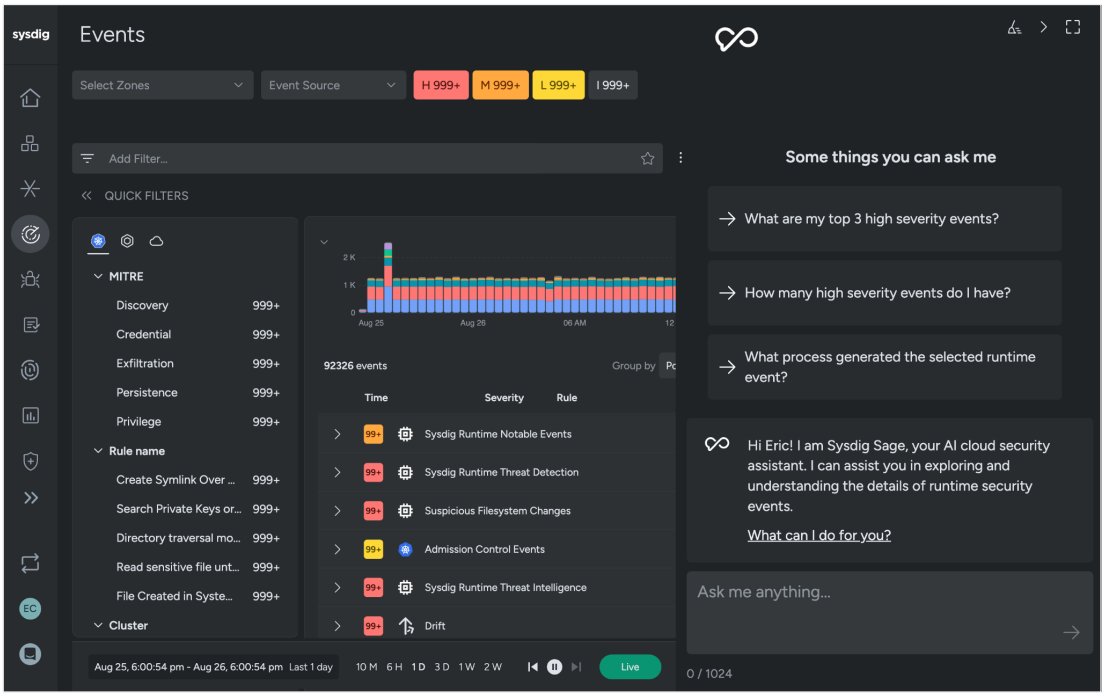
Learn more about Sysdig's AI workload security.

Sysdig Sage™: The first AI cloud security analyst

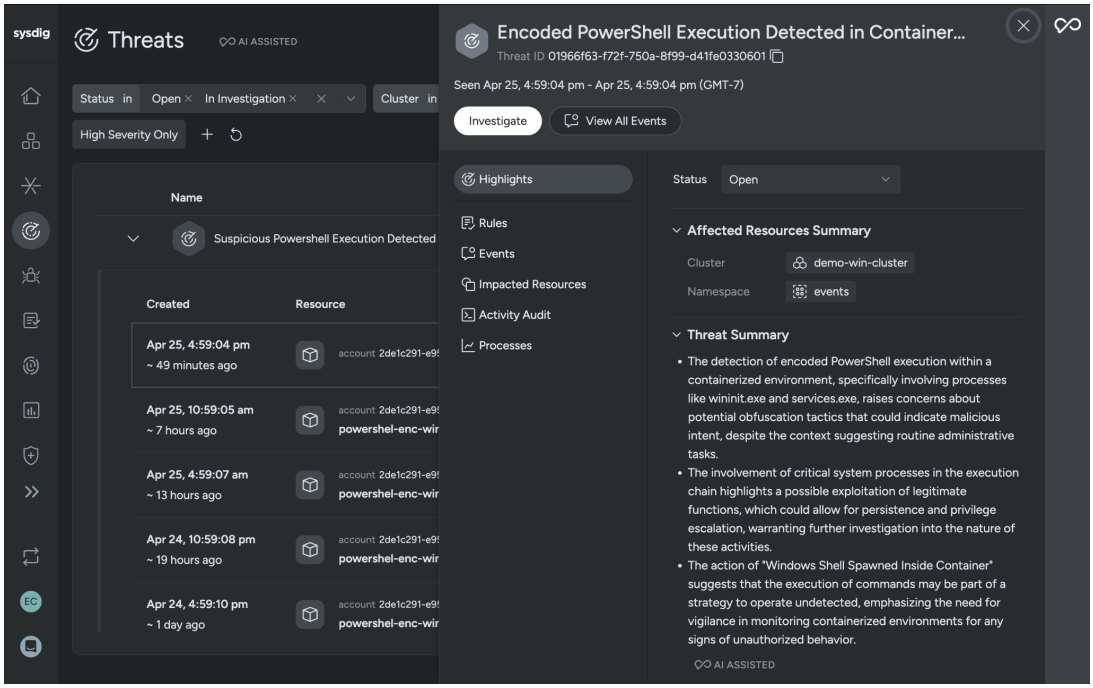
Navigating the intricacies of securing public and private clouds, containers, and Kubernetes can be complex. Even seasoned professionals can find it challenging to stay ahead of the latest cloud threats.

Sysdig Sage is Sysdig's AI cloud security analyst. Sysdig Sage interacts with users through human-like conversations, helping to peel back the layers of security events. Sysdig Sage instantly delivers the collective wisdom of human experts and the continuous learning of AI models to help Microsoft Azure users accelerate their response to security issues.

Figure 7:
Sysdig Sage AI Cloud Security Analyst



Sysdig Sage delivers clear threat summaries paired with detailed, actionable context. Armed with precise situational awareness, security teams can swiftly prioritize and address critical threats.



Learn more about Sysdig Sage.

Conclusion

Microsoft Azure is helping organizations move fast and innovate to deliver solutions that meet customer and market needs. As you scale your use of the cloud, your security practices must evolve to adapt to a growing array of threats. Robust cloud security enables real-time visibility and consolidates capabilities to correlate insights and accelerate response. CNAPP solutions like the Sysdig platform help Microsoft Azure users modernize security, preemptively diffuse threats before they escalate, and stay secure in the cloud.

In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.

Sysdig. Secure Every Second.

LEARN MORE →

sysdig

GUIDE

GUIDE-011 REV D 5/25