CHECKLIST

Secure Your Cloud in Minutes

Your Checklist for Meeting the 555 Benchmark

As cloud environments grow, the speed and sophistication of attacks in the cloud have grown just as much. So how can security teams keep up?

Sysdig's 555 Benchmark for Cloud Detection and Response offers a standard to use when measuring how fast your security teams can counter attackers. Specifically, the benchmark finds that to outpace attacks, your security teams need to detect threats within **5 seconds**, correlate and triage data within the first **5 minutes**, and initiate a tactical response within the next **5 minutes**.

This may sound daunting, but it can be done. We've created this guide to help guide your security strategy so you can operate with the speed and efficiency you need. Paired with our 555 Benchmark guides, this resource lays out the steps to tackling modern cybercriminals and improving your threat detection and response readiness in the cloud.

STEP 01

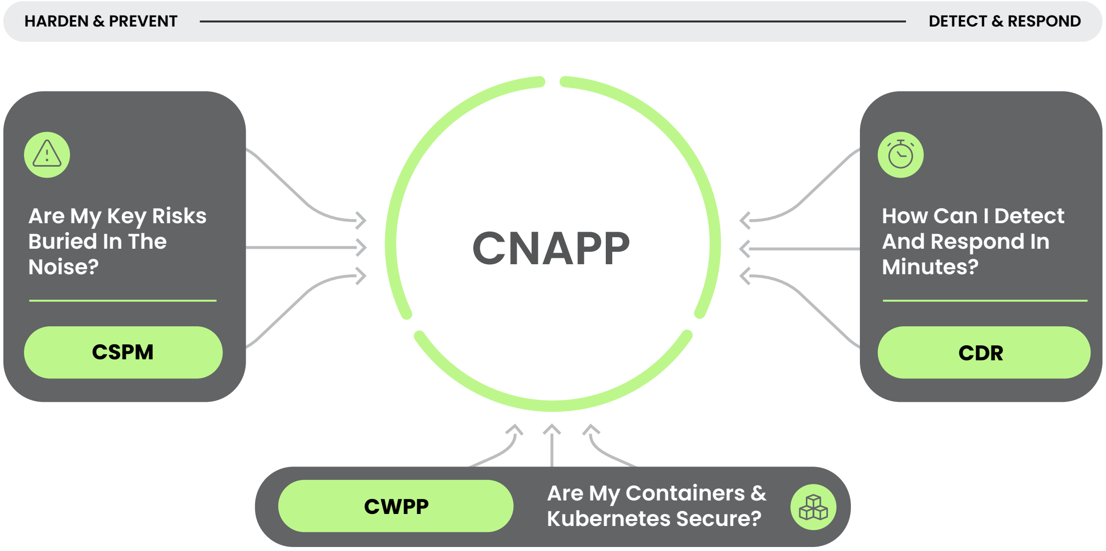
Consolidate your security tools

Securing the cloud comes with challenges like data volume management, monitoring ephemeral containers and microservices, and maintaining compliance standards across your IT estate. The unwieldy stack of individual point solutions many organizations use can make it even harder to meet these challenges, as they make it difficult to gather information, act on threats, and communicate across teams in a timely manner. To rapidly detect and respond to cloud attacks, you need an integrated technology stack across your entire environment.

How to make it happen

A Cloud-Native Application Protection Platform (CNAPP) brings previously separate security functions together in one tool that spans the many stages of the modern software supply chain. For best results, make sure the CNAPP you implement is capable of artifacts scanning, cloud configuration, cloud infrastructure entitlement management (CIEM), infrastructure-as-code (IaC) scanning, runtime protection, cloud workload protection (CWP), and cloud detection and response (CDR). The benefits of this unified approach to cloud security include:

- → Consolidation of previously siloed cloud capabilities to provide a comprehensive protection platform.
- → Minimized cloud complexity to visualize MITRE ATT&CK tactics, techniques, and procedures (TTPs).
- → Improved overall risk visibility, a hardened attack surface, and better security for assets across multi-cloud environments.
- → Easier collaboration between teams, including DevOps, SecOps, and infrastructure operations.


HARDEN & PREVENT
DETECT & RESPOND
Are My Key Risks Buried In The Noise?
CSPM
CNAPP
How Can I Detect And Respond In Minutes?
CDR
CWPP
Are My Containers & Kubernetes Secure?

STEP 02

Harden your defenses

In the ever-changing infrastructure of the cloud, traditional tools are slow and may risk introducing security gaps, or even worse, miss valuable insights. Organizations need automatic discovery, correlation, and behavioral analysis of cloud logs to quickly and effectively detect and respond to threats. Furthermore, their technology stack must reduce complexity, adhere to compliance standards, and collaborate with other programs.

How to make it happen

You most likely already have a SIEM (Security Information and Event Management), CIEM (Cloud Infrastructure Entitlement Management), and SOAR (Security Orchestration, Automation, and Response), but you need to ensure you're using them as effectively as possible. Here are just a few ways you can harden the defenses these traditional tools provide:

- → Enrich cloud telemetry with the data collected from your EDR (installed on workstations), email security, and network detection and response (NDR).
- → Corroborate your findings with trusted intel sources to derive in-depth insights and visualize the attack genealogy.
- → Incorporate workflows that are impactful to reduce employee churn and increase overall productivity.
- → Develop, practice, and implement a tailored cybersecurity plan your teams can use in the event of an attack.

STEP 03

Work with DevOps to adopt automation

During an active breach scenario, a significant amount of time is lost before security teams can engage and respond to suspicious activities. These teams are typically stretched thin and buried under huge volumes of noisy alerts and false positives. To keep up with the steady rise of threats, automation is needed at every step to detect, investigate, and remediate cyber attacks to streamline workflows across the multitude of events. To make that happen, collaboration is non-negotiable.

How to make it happen

DevOps teams can help design, develop, deploy, and maintain tools and scripts for security automation. These automated workflows limit the blast radius of attacks and reduce their impact on security. Here are just a few of the benefits of adopting DevOps workflows within your SOC:

→ Improved ease of response tasks to stop an adversary in its tracks, including process termination, permission optimization, container drift prevention, and network isolation.

→ Automated, repeatable, and auditable workflows that improve internal metrics like Service Level Agreements (SLAs), Mean-time-to-Detect (MTTD), Mean-time-to-Investigate (MTTI), and Mean-time-to-Respond (MTTR).

→ Improved code hygiene, with vulnerabilities and misconfigurations addressed at the infrastructure level via a CI/CD flow.

Meet the 555 Benchmark

Attacks in the cloud are speeding up, but that doesn’t mean your security team can’t speed up with them. By taking these measures, your security team will be well prepared to detect, correlate, and respond to threats faster than they can execute in your cloud environment.

Want to learn more?
Read all about the 555 Benchmark for Cloud Detection and Response in our report.

LEARN MORE →

sysdig

CHECKLIST