IDC

SPOTLIGHT

Sponsored by: Google Cloud

Threat intelligence delivered within a cloud-native application protection platform wrapper enriches and prioritizes risk scoring to deliver on a promise of holistic, unified security.

Identifying and Prioritizing Cloud Risks with a Cloud-Native Application Protection Platform

March 2024

Written by: Philip Bues, Research Manager, Cloud Security, and Michelle Abraham, Research Director, Security and Trust

Introduction

The proliferation of digital technologies and multicloud computing has given rise to an ever-expanding attack surface, with cyber-risk looming as a formidable challenge. IDC research shows that risk grows exponentially as additional clouds or software-as-a-service (SaaS) applications are added. A fast-evolving threat landscape, migration of business-critical workloads to the public cloud, and the chronic cloud security talent gap create vulnerabilities and attack exposures that increase cloud risks. Once organizations recognize the environmental factors that contribute to cloud risk, and that security is fundamentally provisioned differently in the cloud, they must come to terms with defining "risk." It's in this exercise that cultural nuances of teams can sometimes lead to friction (e.g., between cloud security and SecOps). The key is achieving a shared understanding and agreement of risk that can reduce friction.

For example, a threat or vulnerability discovered in a test environment with no sensitive assets or data may not be a high priority for SecOps teams. However, a low-severity vulnerability in the path of a database containing sensitive customer data may be considered high risk and prioritized by the security analyst.

Today's organizations are faced with alert fatigue, which poses as great a risk as the actual vulnerabilities and threats. A radical change in philosophy is required. Organizations need a unified, holistic cloud security framework, infused with threat intelligence (TI), which prioritizes and remediates based on risk. It's a new strategy that is not just about meeting compliance requirements but also about analyzing real-world risks to cloud environments and building a common understanding of risk across teams.

AT A GLANCE

KEY STATS

In IDC's November 2023 *North American Vendors and Tools Consolidation Survey,* organizations were asked, "What are the top objectives for security tools consolidation efforts in your organization?" The top five responses were:

- Improve threat detection
- Reduce costs
- Speed up incident response time
- Streamline operations and workflow
- Simplify compliance

KEY TAKEAWAY

As IDC has reported, while there have been efforts to consolidate cloud security point products, organizations prefer a unified, holistic, multicloud security platform approach, where the primary objective is to improve threat detection, prioritize alerts, lower risk, and enable cost reduction.

Consolidation, Platformization, and Risk

Adoption rates of cloud security posture management (CSPM), cloud workload protection platforms (CWPPs), and cloud infrastructure entitlements management (CIEM) point to the industry's desire for a consolidated platform approach — in this case, a cloud-native application protection platform (CNAPP).

While CNAPP solutions address the misconfigurations, vulnerabilities, and compromised credentials — all recognized as the leading causes of breaches — nation-state attackers and malicious insiders are constantly creating new attack vectors that target critical infrastructure. Examples include high-profile supply chain disruptions and breaches, including the Colonial Pipeline ransomware attack, Log4J, and exploits seen throughout the Russia-Ukraine War.

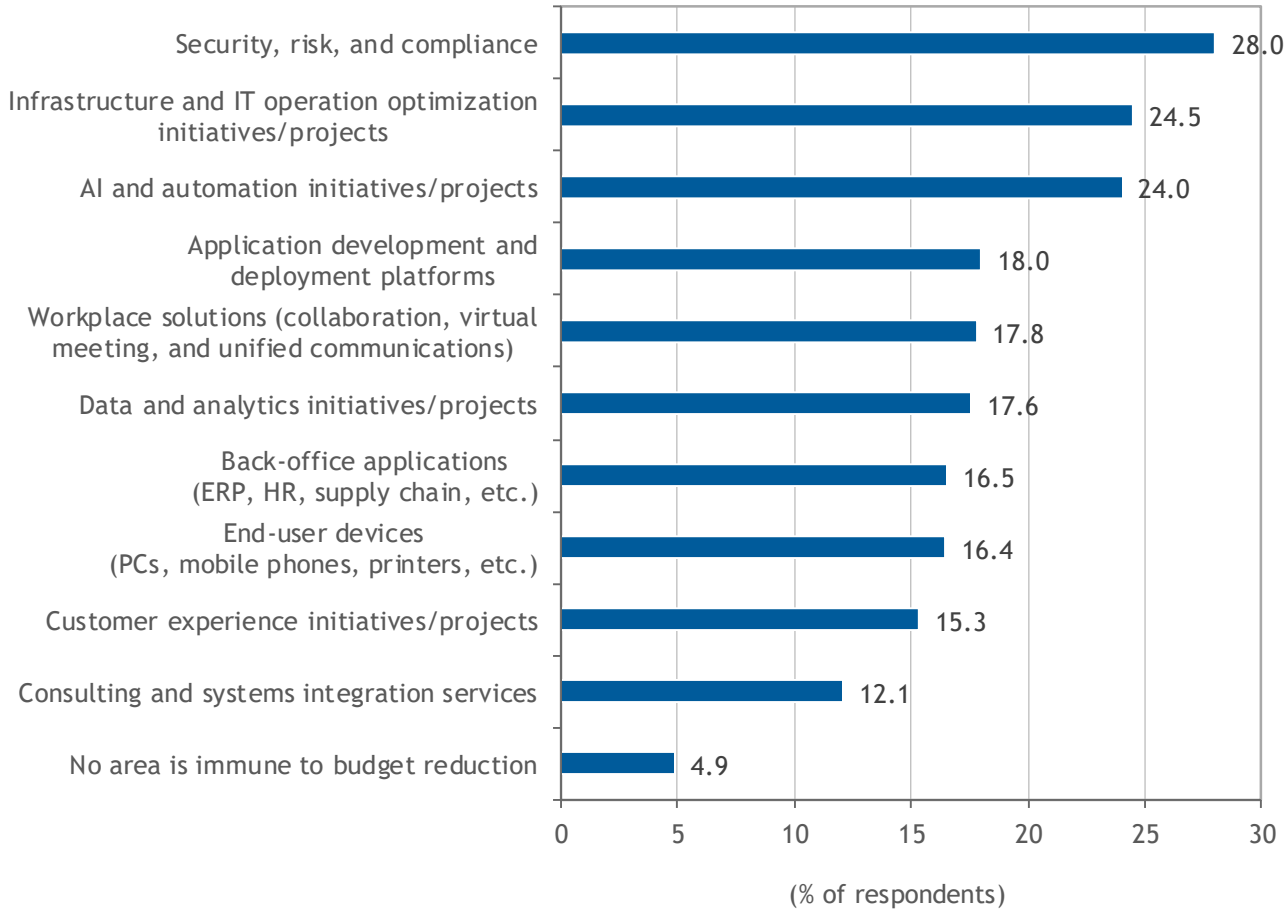
Threat intelligence products take in a variety of threat intelligence sources and provide a way for organizations to analyze their own data against various threat intelligence feeds. Not all TI feeds are created equal, so it's important to understand the differences from security investment, geographic footprint, and in-house research perspectives to transform and curate raw threat intel into actionable data ingested by CNAPP products. Intelligence feeds should be used (along with other security data) to inform risk assessment. That's the real payoff.

Threat intelligence plays a distinctive role by bolstering both preventive measures and detection capabilities in the field of cybersecurity. When a threat intelligence vendor identifies adversarial tactics in the real world, or characterizes an exploited vulnerability, the goal is to contribute this information to CNAPP products, adding valuable context to discovered vulnerabilities and threats so that teams can understand the real-world risks to specific cloud environments. In instances where a business encounters a series of indicators of compromise (IoC), the expectation is that these IoCs can be cross-referenced with the threats, tactics, and procedures (TTPs) employed by adversaries, proving vital for effective detection against ransomware, data exfiltration, crypto mining, and compromised identities.

It's a high-wire balancing act for today's CIO and CISO given that it is essential to understand these challenges against an uncertain global economy. Even as technology spending becomes more strategic, IDC's December 2023 *Future Enterprise Resiliency and Spending Survey, Wave 11,* confirmed that the security, risk, and compliance field is the most immune to budget reductions regardless of the economic environment and shows continued investment over the next 12 months (see Figure 1). After all, security risk is business risk.

FIGURE 1: ***Areas Most Immune to Budget Reduction***

Q ***Which of the following areas are most immune to budget reduction regardless of the economic environment?***



n = 881

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2023

Definitions

Cloud Risk

Because no two cloud environments are the same, an analysis of cloud risks must be unique to the organization's specific cloud. A risk analysis must consider the criticality of the cloud resources to the business, as well as the threat intelligence that is relevant to the organization's industry, environment, and exposures. This includes knowledge of attacker techniques and exploitability of exposures — both singularly and in combination. To make the risk analysis actionable, all risk exposures must be prioritized and aggregated into a holistic risk view of the organization.

Benefits

A proper defense begins with understanding risk. The total risk is the sum of downside risks, including knowledge of the assets and resources that are under active threat, the vulnerabilities and misconfigurations and the ability to exploit them, and the attack paths an attacker may use to reach sensitive data or assets. These risks are not easy to explain in a static sequence and are difficult to assemble manually. The consolidation of this information, with the right threat intelligence, provides a means to calculate the probability of exploitation, so the security team knows where to focus their efforts. Fixing high-risk exposures first can drive the greatest reduction in overall risk. Teams should also be able to track changes in risk posture over time.

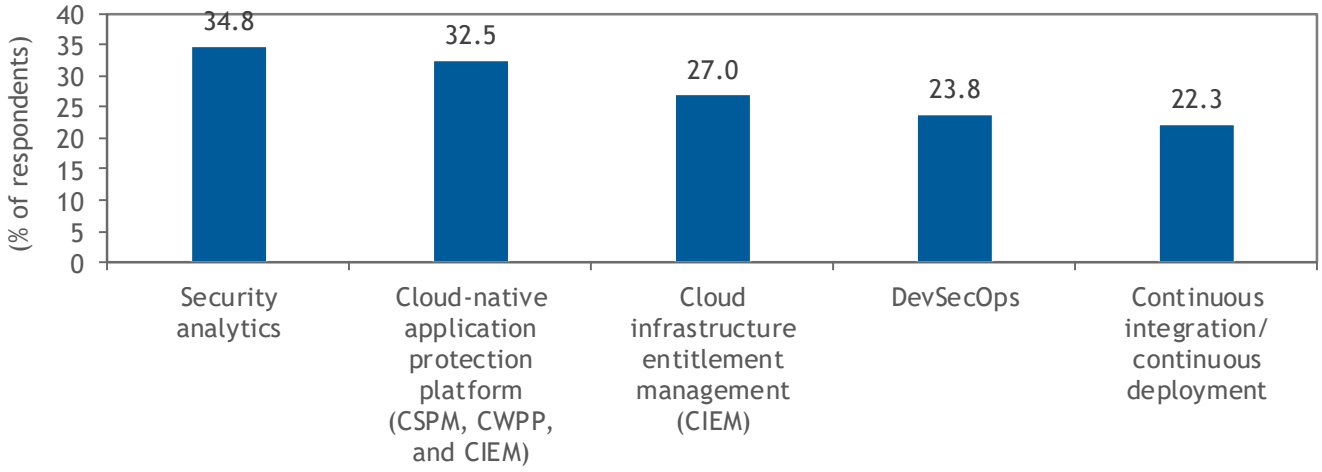
There are many benefits of converging CNAPP with actionable threat intelligence, as this combination may:

- Help dismantle siloed tooling between SecOps and other teams so they can build a single view of risks, based on the same threat intelligence inputs.
- Infuse frontline threat intelligence feeds, enriching risk prioritization algorithms and attack simulation engines to better prioritize response efforts.
- Remediate misconfigurations and vulnerabilities by automatically creating cases, enriched with up-to-date threat intelligence, so a security analyst team can resolve posture issues before an attacker exploits them.
- Curb tool sprawl by encouraging organizations to consolidate point solutions in order to prioritize the high-risk issues that matter and avoid alert fatigue at the same time.
- Enable continuous compliance with various industry best practices, benchmarks, and regulations with the aim of reducing cyber insurance premiums.

Organizations know they need to be proactive and want protection from emerging threats, groups using new techniques, and malware and ransomware, including fileless and living off-the-land attacks. This was tested in IDC's December 2022 *U.S. Cloud Security Survey*, where organizations were asked, "Which technologies/solutions are most important to keep your current cloud environment secure?" The top 5 responses reveal that a holistic, unified cloud security strategy is optimal (see Figure 2). The use of CSPM, CWPP, and CIEM delivered as a CNAPP was acknowledged by 32.5% of the respondents, with the largest response being 34.8% for security analytics.

FIGURE 2: ***Top Technologies for Securing Cloud Environments***

Q ***Which technologies/solutions are most important to keep your current cloud environment secure?***



n = 400

Source: IDC's U.S. Cloud Security Survey, December 2022

Combining security analytics with CNAPP allows security teams to use the knowledge of cloud risk exposure to activate the most appropriate response playbook, for the specific cloud environment, to remediate exposures before attackers make use of them.

Trends

Hybrid and multicloud environments are the reality for most organizations, but they increase the overall attack surface. As clouds increase complexity, the attack surface expands, and risks increase. The consistency of security rules and policies across environments mitigates — but doesn't eliminate — this risk.

As companies move from on-premises monolithic business applications to microservices, their security profile must adapt to the new environment. Many more intrusion points must be tracked and secured to provide a comprehensive view of cloud risk. The potential is for CNAPP to combine vulnerability management, attack surface management, asset visibility, application security, and data security posture management to provide unified visibility and control of exposures. When integrated with security operations capabilities (e.g., threat investigation, case management, and playbook-driven response), the proactive discovery and assessment of risk gets melded with the reactive ability to remediate the risks, thereby improving the organization's overall risk posture.

Considering Google Cloud

Security Command Center

Security Command Center is Google Cloud's multicloud security solution, purpose built to manage and reduce cloud security risks. It converges modern SecOps capabilities into a single platform to find and fix cloud security issues quickly.

It incorporates a continuous risk engine that automatically builds a deep understanding of an organization's cloud environment, then simulates thousands of possible attack vectors to identify the highest risk issues.

Security Command Center is powered by Google AI and threat intelligence from Mandiant to get to the right security outcomes fast.

The solution helps organizations with life-cycle risk management in the ways described in the sections that follow.

Build and Deploy Securely

- Cloud security posture management is used to detect misconfigurations and vulnerabilities in runtime to keep cloud environments in a secure state.
- Shift-left security is available that includes:
  - Security posture controls that detect if cloud configurations drift from defined guardrails and/or compliance standards
  - Infrastructure as code (IaC) scanning to find security issues in pre-deployment
  - Tested and validated software packages to mitigate supply chain risks introduced during the software development process

Detect and Manage Threats

- Threat detection discovers and identifies attacks against cloud environments.
- Frontline threat intelligence is integrated and operationalized to keep cloud defenses up to date, capable of detecting and blocking the latest attacks.
- Threat investigation is used for efficient, context-based searches across petabytes of data to get a full picture of who did what and when.
- Managed hunt service proactively searches for undetected attacks missed by traditional detection mechanisms.

Respond to Security Issues and Protect Identities and Data

- Automated case creation and management can get high-risk issues to the right teams, and it includes out-of-the-box and custom playbooks.
- CIEM manages identities and privileges in cloud environments to find excessive and dormant access that could compromise cloud security.

- Sensitive data protection is used to find, categorize, and manage sensitive data in cloud environments so data risk can be actively managed.

Who Benefits?

- Developers can use thousands of software packages tested and validated by Google Cloud.
- DevOps and DevSecOps teams can use shift-left capabilities to design and monitor security guardrails for their cloud infrastructure and scan infrastructure configurations during preproduction so issues can be found early.
- Cloud security teams can manage cloud security operations, monitoring for misconfigurations, vulnerabilities, and threats in runtime environments.
- Security analysts and SOC managers can investigate security events with enriched data that incorporates valuable context about what is happening in a customer's multicloud environment.
- Vulnerability and incident response teams can accelerate security remediation efforts with automated case assignment and management as well as out-of-the-box and custom response playbooks.
- Risk and compliance professionals can manage their organization's overall risk posture and monitor compliance with regulatory mandates.

Challenges

It's never easy blazing a new trail. Customer and vendor challenges will be:

- Getting cloud security and security operations teams to use a single source of truth for their cloud security data and leverage common workflows that span traditional team boundaries (Google Cloud believes the "operational" convergence of the two teams — so it has a unified security view of its multicloud environment and can leverage common workflows — will be a benefit to customers.)
- Taking a risk-centric approach to cloud security (Yes, compliance will remain necessary as will elevating the importance of identifying and assessing true risks that threaten to compromise sensitive cloud resources and disrupt the business.)
- Making sure that frontline threat intelligence is used to inform cloud security defenses to stay head of hackers (Static defenses may be easier to operate, but they don't work as well in a fast-changing threat environment.)

For Google Cloud, there is also the challenge of making sure that cloud security findings (threats, vulnerabilities, and misconfigurations) are melded into a SecOps product so that analysts do not have to change their day-to-day operations and can continue to remediate issues using the case management and playbooks that they're used to.

Conclusion

Organizations need to know their points of exposure and what assets and resources may be at risk in the new multicloud reality. Recognizing that managing risk is an increasing challenge for machine learning, cloud security solutions should be capable of handling vast amounts of data for comprehensive risk analysis, enrichment, and mitigation of vulnerabilities and threats. Infusing intelligence-driven prioritization risk scoring and automatically assigning cases simplifies and streamlines the CNAPP workflow leading to the right alerts being investigated and remediated in a timely fashion, reducing an organization's risk.

Risk is the sum of downside risks, including attack paths, vulnerabilities, misconfigurations, and the ability to exploit.

About the Analysts

Michelle Abraham, *Research Director, Security and Trust*

Michelle Abraham is the research director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM) and Vulnerability Management practice. Ms. Abraham's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device and application vulnerability management alongside related topics.

Philip Bues, *Research Manager, Cloud Security*

Phil Bues is the research manager for IDC Cloud Security. Phil drives research, provides thought leadership, and advises clients on complex issues, including cybersecurity in the cloud. His insights address the benefits and challenges of what's been called the "shared responsibility model" and how that model may change going forward.

MESSAGE FROM THE SPONSOR

Make Google Cloud part of your security team

Google Cloud Security provides multi-cloud protection with its Security Command Center solution, frontline intelligence and assistance from Mandiant to help you prevent and respond to security incidents, a modern, cloud-native platform to drive your security operations, and a secure-by-design, secure-by-default cloud platform for your organization's digital transformation. And we have built our platforms and products to defend your most critical data, applications and communications to work as you do — across the cloud, your enterprise, and any type of device, at any scale.

For more information about multi-cloud security and risk management, please visit Google Security Command Center.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com