

Sweet Security Runtime CNAPP -A Solution Brief



www.sweet.security

Sweet Simplifies Cloud Security

Sweet is a **runtime powered CNAPP** that unifies insights from applications, workloads, and cloud infrastructure to surface key risks, enabling teams to detect incidents and resolve threats faster.

Challenges



Sweet Solution

By adding a new "flavor" to traditional CNAPP frameworks, Sweet's CNAPP focuses on three key principles:

Runtime Z Monitoring	Cloud environments need to be secured 24/7, not just periodically. Continuous runtime monitoring ensures that security teams can detect and respond to active threats in real time.
True Platform	Security should not be fragmented within a platform. Sweet Security correlates data across cloud, workloads, applications, networks, and user/machine identities to provide holistic, unified detection and response.
Application- Layered Security Focus	✓ The application layer is a prime target for attackers. Sweet Security integrates application visibility into the same framework as cloud visibility, ensuring that both security and development teams have the context they need to protect cloud-native applications.

With this approach, **Sweet Security has built a CNAPP that protects against modern cloud attacks**– one that doesn't just shut down attacks, but prevents them in real time with zero performance impact.

sweet.

What Makes Sweet Different

5 → 1 No Tool Sprawl

Reduce tool count from 5>>1

300%[↑] SOC Efficiency

Increase SecOps team efficiency by 300% 80% J Cloud Sec Costs

Drop security costs by 80%

2 = 5 min MTTR

Detect and respond to threats in minutes

Key Capabilities

Features

Full-Stack Runtime Monitoring	Kuntime CSPM
Unified Detection and Response (CDR, CWPP, ADR in One)	🗀 Cloud Visibility
Vulnerability Management	ldentity & Secrets Security
API Security	Data Security

Monitor Your Could Environment 24/7

Sweet provides boots-on-the-ground eBPF sensors for real-time detection of runtime signals. These sensors collect telemetry and security data directly from the cloud infrastructure, workloads, containers, and serverless environments and require minimal CPU and RAM consumption. The sensor data is then correlated with real-time cloud logs and Layer 7 data to provide deeper visibility and complete context.

							d ^a in
Dashboard + Displaying data from the previou	is week						L Expor
Risk Management					Resilie	nce Score = B	enchmark 80
Critical Sensor-based incidents	6	\blacksquare In-use critical vulnerabilities with fixes \rightarrow	8	Chromanaged active secrets on public facing \rightarrow 1 workloads		6	1
\bigcirc Critical Log-based incidents \rightarrow	0	In-use critical vulnerabilities on public facing workloads	→ 7	$\textcircled{\ } \text{ Expand secrets on public facing workloads } \rightarrow \qquad 1$		84 Best	
Threat Center			•	In Use Vulnerabilities O Plain	text Secrets I	бу Туре	
ALAS-2025-2783 = 1 Workloads (0 Public f sm03includeAddNode in sinclude.c in literal 2	efore 2.11.0 has a us	ue-after-free. (CVG-2022-49043)	c				
CVE-2025-27152 = 1 Workleads (0 Public F axios Requests Vulnerable To Possible SSRF a	acing) (Roable) (b nd Credential Leaka	oodeed ge vie Absolute URL	c	96% Not in use 04% 5.4K Loaded Not Exec., 121	4 Total	Basic S Auth Auth	ecret
ALAS-2025-2774 = 1 Workloads (0 Public F An issue was discovered in Reepart before 2.6	acing) (Reable) .4. There is a crash r	within the XML_ResumeParser fu	c				
ALAS-2025-2780 + 1 Workloods 10 Public F Issue summary: A timing side-channel which o	ould potentially allow	w recovering the priv Show mane	С	Top Incidents			
ALAS-2025-882 = 1 Workleads (0 Public Fe base summary: A timing side-channel which c	cing) Foable ould potentially allow	a recovering the priv Show more	c	Name Attempted AWS credential theft and service disruption via 'payload.sh'	Aronaly	Instances 1 Instance	Severity Dritcel
CVE-2023-52968 + 1 Workloads (1 Public F	acing) (Feable)		c	Kabernetes Token Harvesting and Exploitation with 'can-they.sh'	Anomaly	1 instance	Critical
manimum antiver rook Dillone 10.4.33, 10.5 Dillon	e rouaue, RUD Deltor	a nano, no mango. anal mare		Persistent 'xmrig' Execution in Random Directories	Asonaly	1 instance	Critical

Detect & Respond to Threats with a MTTR of 2-5 Minutes

Sweet's LLM-driven detection and response combines Cloud Detection and Response (CDR), Cloud Workload Protection Platform (CWP), and Application Detection and Response (ADR) into one cohesive platform. This means security teams can detect real-time threats in seconds as all the pieces of a lateral attack are available in a single pane of glass.

🔎 Key Highlights:

- **LLM-powered Detections and Investigations:** Sweet identifies known TTPs and zero-day attacks in a mere 30 seconds, leveraging LLMs to spot anomalies within cloud activity sessions. In addition, Sweet's LLM provides a comprehensive story of every incident and lists every action taken by the attacker. This story helps security analysts understand if the incident is a false positive, what team or team member needs to investigate, and what's the urgency of the incident.
- **Unified Attack Views:** Sweet's unified attack view correlates insights from across the cloud infrastructure, workloads, and applications, ensuring defenders have a complete picture to quickly identify, investigate, and mitigate threats.
- Al Response Playbooks: Respond to attacks with complete confidence with an Al playbook that adapts to the specific context of each incident.
- Manual or Automated Responses: Shut down attacks as they unfold by manually or automatically terminating malicious processes.

		③ Create	a ticket O Comments	• Open v
An attacker gained access to an EC2 Instance and attempted to escalate privileges by assuming roles acress AWS accounts. They executed a malicious acress (r/(fus/payload, in) to access sensitive \$3 data				
and delete VPC flow logs, but were blocked by proper UAM configurations.				
		Even general Getan		
Stry		Consumer	Time created	
1 Initial Reconsistance The attacker begins by exploring the system, running 1s commands on various directories (2, 781e/, 7etc., 7hare). This indicates an attempt to understand the system's structure and potentially locate sensitive files.		G cdr-unified-s3-w	tbapp-aa3c2f6 Feb 10, 2025, 11	23.54 AM
2 System Update and Payload Preparation The statickin updates the system using apt updatey and then extracts a payload using tarxmf C /txp. They make the payload executable with chand +x /txp/payload.sh , suggesting preparation for the main attack.		Target	Time ended Feb 10, 2025, 11	25 22 AM
3 Payload Execution The attacker executes the payload script with the command bash -c /tmp/payload.sh annawsilam:1272/464678/26:role/cdr-unified-i3-webape-aa)c/44-e790-11ef-8017-e8016f-806fe anniawsilam:100185122064irole/cdr-unified-i3-data-access-aa)c	ec2.amazonawa.c	com (+6) Time resolved		
eb8f8fe35f4e s3;//internal-passwerds/admin-passwerds/a	Accounts	Resolve		
4 AWS CLInstalation The script installs the AWS CLI and jo with apt install nescli jq -y, preparing the environment for AWS interactions.		a sweet-security-de	mo-production	
EXS Service Account Token Retrieved The attacker attempts to retrieve the EXS service account token by running cat /var/run/secrets/eks.amazonaws.com/serviceaccount/token_iRely to use 8 for authentication.		Sweet-security-de	ino-development	
8 Cross-Account Role Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 081051228884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 08105128884 using the Assumption A CloudTrail event shows the attacker successfully assuming a role from account 727646487209 to 08105128884 using the Assumption A CloudTrail event shows the attacker successfully assumption A CloudTrail event shows the attac		Machines	B100 117/70	
7. Attempted \$3 Access The attacket tries to access an \$3 bucket named "app-cathe" using the assumed role, but the access is deried due to proper MAN configurations.		Contraction of the	happ marcane.	
8 VPC Flow Log Detection Attempts The attacker attempts to detect VPC flow logs using the AVIS CLI targeting flow log IDs 11-11223344556571899 and 11-11223344556571899. Both attempts fail due to lisk of permissions.		G S. United		
9 Sensitive Data Access Attempt The attacket triss to read the contents of admin-assistent's bit. Haiv retrieved from the S3 bucket, using the cat. command with an AMS session token.		Labels		
		8 3 🐨		
• THE BULKIES SUBJECT THE BULKIES WHE FASTER VE BULKIES HAVE FUNDED AND THE PROPERTY AND ADDRESS AND ADDRE				
The attacker attactpoted, but failed, to access the S3 bucker. appl-cache, and delete VPC flow logs.				
IN 24.21 Const-Account SI Activity Detected	Consumer	op-aa3c2144-e790-11e1	Tarpet	
The series and an access a new amply so owners and called, including the same a same and so proper second Contract.			sweet-security-demo-development	м 🖲
13223 Cross-Account Assumethols Activity Detected	Consumer		Target	2164
10/02/2023 🍟 This CloudTrail event demonstrates the successful cross-account role assumption, a key step in the attacker's attempt to esculate privileges.	Con-united-s3-webi	pp-88302744-8790-1181	sweet-security-demo-production	•1
Tip reass -				
			e de la de la de la 🖬	Investigate
Second Second Band Second Seco				
Construction Const	2 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -			
Manual Manu Manual Manual Manu	·			
Construction C	·			
Accessed and accessed and accessed acce	1 2			

Reduce Risk and Prioritize CVEs According to Runtime Context

Sweet's Vulnerability Management combines runtime insights and LLM-powered analysis to assess and prioritize vulnerabilities based on the behavior of the vulnerability, in addition to the risk and impact it will have on the business.

Key Highlights:

- **CVE Prioritization Based on Runtime & LLM Analysis -** Evaluate vulnerabilities based on runtime factors, including whether the vulnerability is loaded into memory, actively executed, its exploitability potential, and whether it is public-facing.
- **Supply Chain Risk Management** Identify and mitigate harmful packages associated with third-party dependencies before exploitation.
- **Pinpointing of Executed Vulnerable Functions –** Identifies vulnerable functions that are actually executed at runtime.
- Software Bill of Materials (SBOM) A comprehensive inventory of packages and dependencies that includes both vulnerable and non-vulnerable components.
- Image Scanning for Vulnerabilities Sweet's image ad-hoc scanning extends vulnerability management from the runtime phase to the registry phases so teams can identify vulnerabilities in an image before it enters the CI/CD pipeline, in addition to verifying that patched images are free of known vulnerabilities before pushing them to production.

Vulnerabilities		ID10022 aetectea PM aetectea PM glibc vulnerable to Stack Buffer Overflow
● Critical ● High ● Medium ● Low		Investigation Remediation Overview
4.4K (100%) Total	1.7K (38%) 1. Loaded E	1.5K (33%) Base Score Sweet Score Parameters Sweet Score
		9.8 -2.8 0 -2.1 0 -1 0 0 Rurtime Public Exploitation in the Workload • Critical Utilization Facing wild Exploitation
		Sweet Score Reasoning
Group By Vulnerabilities Packaç Q. 101 x 1	ges OS Images Workloads None Risk Indicators • Package Manager •	The risk level can be significantly reduced due to multiple factors: Package was not loaded or executed, indicating it might be a build dependency. No observed public inbound connections, limiting external attack vectors. The vulnerability is considered a non-security issue by upstream maintainers and has very low exploitation probability in the wild as indicated by EPSS score.
Uulnerability	Sweet Sc ↓₹ Package	Image Technical impact
CVE-2019-1010022	(\$, 3.9) ↓ -5.9 (P) libc6-dev 2.31-13+deb11u6	docker/lib 3.818-bute integrity and confidentiality
CVE-2019-1010022	5. 3.9 ↓ -5.9 @ libc6 2.36-9+deb12u9	osskuben v1307
CVE-2019-1010022	S. 3.8 ↓ -6 @ libc6 2.36-9+deb12u7	ossjkuben Graph ^
CVE-2024-37371	S. 3.6 ↓ -5.5 O libk5crypto3 1.19.2-2ubuntu0.3	ndnb/cve- istiest Stack buffer overflo
CVE-2024-3596	5. 3.6 ↓ -5.4 () libk5crypto3 1.19.2-2ubuntu0.3	ndnb/cve-
🗍 😽 CVE-2023-20863	5. 3.5 ↓ -3 5.3.18	mongo IID66-dev CVE-2019-1010022 latest 2.31-13+deb11u6 Explorability probability Low Low Low
CVE-2023-20861	(\$. 3.5) ↓ -3 5.3.8	in ndnb/cve-
CVE-2022-4899	\$, 2.3 ↓ -5.2 (? libzstd1 1.4.8+dfsg-3build1	ndnb/cve- liatest
CVE-2024-37370	\$.2.2 ↓ -5.3 ○ libk5crypto3 1.19.2-2ubuntu0.3	ndnb/cve- iutest
	libc-bin	ndnb/cve-

sweet.

Detect and Prioritize Toxic Combinations & Runtime Misconfigurations

Sweet's Runtime CSPM & Issues Hub delivers real-time and immediate alerts on any misconfiguration or deviation from best practices, enabling proactive remediation and minimizing the risk of an attack due to the toxic combination of misconfigured resources.

Key Highlights:

- **Posture Management:** Detect misconfigurations instantly, establish a behavioral baseline to differentiate normal activity from anomalies, and dynamically adapt your security posture in real-time.
- Toxic Combination Assessment: Get a unified view of toxic combinations by cross-correlating misconfigurations, exposed assets, and over-permissive access. Examples include identifying exposed APIs tied to vulnerable IAM roles, assessing lateral movement risks through East-West traffic analysis, and more.
- **Compliance Management:** Continuously check compliance against frameworks like HIPAA, GDPR, the CIS Kubernetes Benchmark, NIST, SOC 2, ISO 27001, and more, offering pre-built compliance rules for quick policy adherence, and issuing alerts for configuration drifts to enable timely corrections.

Map Your Cloud Environment

Sweet provides comprehensive, real-time visibility into your cloud environment. The platform maps runtime activities and dependencies, providing insight into how resources interact and depend on each other across your cloud infrastructure. This enables teams to monitor critical interactions and maintain control over how data and workloads flow within their environment.

Key Highlights:

- **Topology Mapping:** Map hybrid and multi-cloud environments, offering both bird's-eye and worm's-eye views to understand runtime communications, dependencies, hierarchy, and structure.
- **Asset Inventory:** Sweet catalogs your environment in real-time by tracking clusters, networks, databases, compute types, and any other cloud resources the moment they spin up.
- **Network Insights:** Detect unauthorized ports, suspicious connections, and communication with malicious IPs and domains.

Manage and Protect Your Applications

Sweet provides deep Layer 7 visibility into API traffic, enabling comprehensive application-layer threat protection. By analyzing API requests and responses, Sweet can detect common application-layer attacks such as SQL injection, cross-site scripting, and other exploits targeting APIs and microservices. Our solution helps protect these critical communication channels, ensuring that they are secure against both known and unknown threats.



Identify Compromised or Mismanaged Identities and Secrets

Sweet's ITDR capability monitors and responds to identity-based threats across your cloud environment. By tracking user credentials, access patterns, and privilege misuse, Sweet helps identify potential insider threats or external attackers targeting your identities.

Key Highlights:

- Identity Threat Detection and Response (ITDR): Enables rapid detection of anomalies such as privilege escalation, credential abuse, and suspicious login patterns, allowing security teams to respond immediately and prevent further exploitation.
- **Runtime Insights:** Monitor identity usage, permissions, and privileged statuses to enhance security, including:
 - Privilege Adjustments for reducing over-permissioned identities based on actual usage patterns.
 - Secret and Identity Management for deleting unused or dormant secrets and identities to minimize attack surfaces.
 - Non-Human Identity Management for securing service accounts, tokens, and API keys to ensure safe operations.
 - Human Identity Monitoring for detecting unauthorized access attempts, unusual privilege escalations, and irregular usage patterns.

Track Data in Motion to Prevent Exfiltration

Sweet focuses on securing data in motion, ensuring that sensitive information is protected as it moves across your cloud environment. This allows security teams to pinpoint where data may be exposed to unauthorized access or manipulation. With Sweet, you can be confident that your data is protected, regardless of where it resides or how it moves within your cloud environment.

Supported Architectures & Deployment

	• AWS: Full support for services like EC2, Fargate, and ECS.
	• Google Cloud: Integration with Compute Engine and GKE.
	• Azure: Coverage for Azure Virtual Machines and AKS.
	• Private Cloud: Supports any private Kubernetes environment.
	Managed Kubernetes: EKS, GKE, AKS.
Orchestration and	Self-Managed Kubernetes: Any Kubernetes version >= 1.20.
Containerization	Container Management Services: ECS, Azure Container Apps.
	Serverless Compute for Containers: AWS Fargate
Virtual Machines	• Virtual Machines: Linux-based (amd64/arm64) with kernel >= 5.10.

Sweet's lightweight eBPF sensor can be deployed as a privileged pod, sidecar container, or Lambda layer, depending on your environment. It's optimized to trace only relevant system calls and runtime events, ensuring minimal impact on application performance. Additionally, updates are seamless, with automatic remote fetching of configurations and features to keep everything running smoothly.

Runtime Event Collection

Captures processes, file accesses, network traffic, and memory usage.

Baseline and Deviation Analysis

Establishes normal behavior and identifies anomalies.

MITRE Classification

Tags events using MITRE ATT&CK framework for standardized threat analysis.

IOC and TTP Detection

Continuously updated from external security vendors.

