aws marketplace

Sweet Security

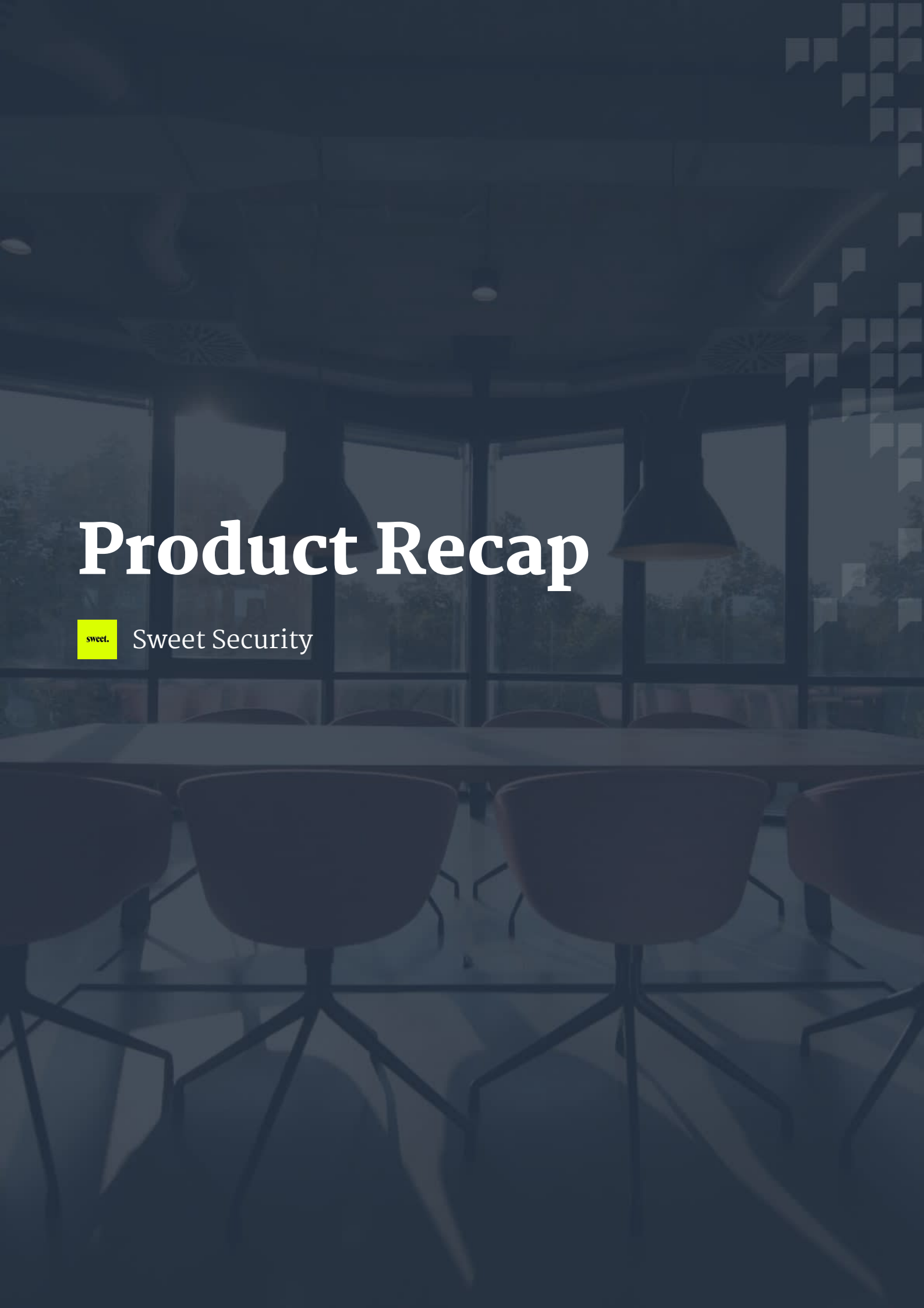
Reviews, tips, and advice from real users






Powered by PeerSpot

Contents



Product Recap

sweet. Sweet Security

Sweet Security Recap

Sweet Security offers advanced cybersecurity measures designed to protect enterprise-level networks from complex threats, providing efficient monitoring and robust protection capabilities.

Focused on sophisticated threat detection and network security, Sweet Security provides an enterprise-grade solution for cybersecurity challenges. It integrates seamlessly with existing systems, offering real-time analytics and threat intelligence. Its comprehensive approach ensures high-level data protection and security management, allowing organizations to focus on core functionalities.

What features make Sweet Security stand out?

- Real-time Threat Monitoring: Ensures proactive identification and response to emerging threats.
- Seamless Integration: Easily integrates with current systems for enhanced security without disrupting operations.
- Advanced Analytics: Provides insightful data for efficient threat management and decision-making.
- Threat Intelligence Capabilities: Robust mechanisms to enhance awareness and preparedness against attacks.

What benefits or ROI can users expect from Sweet Security?

- Enhanced Security Posture: Offers improved protection for sensitive data and assets.
- Cost Efficiency: Reduces potential loss from security breaches by preemptively protecting systems.
- Productivity Improvement: Frees up resources by automating threat detection and response processes.
- Scalability: Supports growth and expansion without the need for constant re-evaluation of security resources.

Implementation of Sweet Security across industries like finance, healthcare, and e-commerce demonstrates its versatility and effectiveness. In finance, it safeguards sensitive financial data; in healthcare, it ensures patient data privacy; and in e-commerce, it protects online transactions from fraud, making it an invaluable asset in today's digital landscape.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"Sweet Security represents the next generation of CNAPP that differentiates through a runtime-first approach and focuses on detecting and responding to real attacks in environments."

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

"We have seen an 80 to 90% reduction in vulnerability noise, a 60 to 80% reduction in triage and patching time, and managed to save 50% of costs because many things are handled by Sweet Security itself."

NavnathSolanke

senior executive at a tech vendor with 10,001+ employees

"For the time I have been using Sweet Security, I feel a bit more safe in the sense that there is something that continuously scans my infrastructure for issues."

Filippos Malandrakis

Infrastructure & Dev Ops Lead at Babylon Labs

"Before we had Sweet Security, upon any type of detection of activity, we needed to conduct lots of investigations in different platforms and logs until we could build the larger picture, but once we inserted Sweet Security, we are able to actually see each and every request being made from the application level towards the infrastructure, making it much easier and reducing the time for an analyst to understand what's really happening."

Verified user

Director of Security Operations at a tech vendor with 501-1,000 employees

"Sweet Security is a better tool and provides layer-by-layer protected environments, and with Sweet Security for cloud, security is totally under control."

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

"The value we see from having real-time visibility into our cloud environment is significant, as Sweet Security serves as our eyes and ears inside AWS, telling us what we are doing wrong so we can fix it."

Elior Duanis

Cloud and compute team leader at a manufacturing company with 1,001-5,000 employees

"The value of having real-time visibility in our cloud environment with Sweet Security changes everything because it differentiates between identifying and reacting to something that is not really a risk and something that is truly a risk that needs to be treated."

Reviewer302234

Works at a tech services company with 201-500 employees

What users had to say about valuable features:

“I really love the feature within Sweet Security platform that allows you to visualize the specific packages or functions that are being loaded to the memory and are actually being executed by the operational system. The fact that they know how to filter those really helps to reduce our time invested in the triage and also in the remediation and mitigation steps for which vulnerability. This is an amazing feature. It's not the main feature of the platform, but that's something I really love about it.

Before we had Sweet Security, upon any type of detection of activity, we needed to conduct a lot of deep investigations in different platforms and in different logs until we could build the larger picture. Once we inserted Sweet Security in the runtime protection, we are able to actually see each and every request being made from the application level towards the infrastructure.

For example, there might be an API that gets a request, then ingests it into the backend and the backend processes it. We were able to see an API request being made and the exact method that it was infiltrated into the infrastructure. Previously, we were not able to correlate between an application layer event to an infrastructure layer event, but with Sweet Security, it's much easier. It reduces the time for an analyst to understand what's really happening. Any suspicion of an incident or something similar will not be a standalone. It will be part of a chain where you can see what happens from the application layer, then what it caused within the infrastructure layer..”

Verified user

Director of Security Operations at a tech vendor with 501-1,000 employees

Read full review

"What stands out about my main use case and how my partners use Sweet Security is the deep runtime visibility and application layer security, particularly for APIs and microservices. This is where most traditional CNAPP solutions are weakest, and this is where Sweet Security performs exceptionally well. Additionally, in production environments, Sweet Security is focused on detecting and responding to real-life effects in live production environments. It correlates signals across cloud, apps, identity, and data into a single attack story. The way it contextualizes information in story form is another real positive, which I found mentioned by other reviewers as well.

"Before Sweet Security, partners and customers needed to conduct extensive investigations when they found detection of activity across all different platforms and security logs until they could identify what was actually wrong in the bigger picture. Sweet Security enabled teams to see each detection of activity upon every request made from the application level towards the infrastructure, making it much easier and reducing the time for an analyst to understand what is really happening. It provides real-time visibility in the cloud environment, which is a massive differentiator because teams are seeing events as they happen, live in real time.

"Sweet Security's capabilities in runtime coverage impact my overall security strategy and the strategies of my partners by allowing us to capture threats as they occur in the live production environment in real time. We are capturing code-level events because we have shifted right in our approach. This is a key point to add: we are not traditional tools on the left side of the shift. We shift right, which means we operate in production and in real time. We are not pre-code or pre-cloud. We have shifted right, and this is a massive positive for time efficiency, workload efficiency, and more importantly, being proactive rather than reactive across the cyber landscape.."

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

“In terms of the best features of Sweet Security, I haven't had any threat detected in the sense that there hasn't been any incident so far while Sweet Security is in place. In terms of vulnerabilities, I got some good findings and some good vulnerabilities were detected. Software that was on my infrastructure had known vulnerabilities and I was able to patch it timely. These things I was unaware of before installing Sweet Security on my infrastructure. So it was pretty good.

The Layer 7 network traffic inspection in Sweet Security has been pretty good. It can understand the traffic that's coming and can find potential credentials from users in this traffic, for example. Overall, it can detect sensitive data in this traffic very well.

Having runtime coverage with Sweet Security is also one of my audit requirements toward getting a certification. So having this in place will help me toward getting a certification in the future.

Having real-time visibility into my cloud environment with Sweet Security has changed the way my team detects and responds to threats. I didn't have a tool in place before. I have established a process for potential real-time threat findings, but I haven't had any yet, so I was not able to test this process yet.

Sweet Security helps unify various aspects of security detection into a single platform. It provides real-time infrastructure security and vulnerability management. It also monitors Layer 7 traffic for credential leaks and helps with vulnerability management on cloud accounts to detect if something is not configured properly. It's a lot of different functionality.

For the time I have been using Sweet Security, I feel a bit more safe in the sense that there is something that continuously scans my infrastructure for issues. I didn't have a solution in place for that before. So it has provided me peace of mind. In terms of actual findings, it found several vulnerabilities in my software. This has been definitely a benefit toward operating more secure software on infrastructure..”

Filippos Malandrakis
Infrastructure & Dev Ops Lead at Babylon Labs

Read full review

“I find the UX/UI to be comfortable. The insights that it brings us are related to the business logic of our company, which is important. If something is flagged as a critical alert, this indicates that it must be observed closely.

We have used the real-time monitoring feature of Sweet Security, and this specific solution has given us real detection that helps us find what is actually important against what is not important. It saves us a lot of investigation time that isn't required anymore. It's a very good product, I'm happy we have it. We looked into the CPU consumption and it's the lowest against the benchmark.

The time savings from Sweet Security have varied, but the impact has been significant. It has reduced the need for back-and-forth discussions between teams such as Security, DevOps, and R&D. It only flags the important and critical risks. It saves developers time from looking into fixes for false positives. We use the customizable dashboards in Sweet Security. These dashboards have helped in managing our security posture by presenting all the relevant information that the security team needs to see. The correlation between the information is very efficient. They made a lot of improvements to this over the last year. It's a lot better now than it was a year ago. The insights are good.

The reporting is very good because we can customize it to what we actually want to see.

The value of having real-time visibility in our cloud environment with Sweet Security changes everything because it differentiates between identifying and reacting to something that is not really a risk and something that is truly a risk that needs to be treated.

Sweet Security has had a big impact on mitigating risks and aiding development..”

Reviewer302234

Works at a tech services company with 201-500 employees

Read full review

"Sweet Security is a good tool for governance and security. It is a very reliable and secure tool because most cloud infrastructure has been integrated into it, and it has all the security plugins and policies in place to prevent data leaks. It is a reliable solution for cloud native application security.

"Sweet Security is a next-generation application security tool with AI capabilities. The alerting functionality is continuously integrating and evolving. Whenever we found something needed in the tool, we contacted customer support and they implemented it. They are very helpful and ready to take feedback and make changes to the tool. Sweet Security is well-scalable throughout multi-cloud environments and Kubernetes clusters because it relies on lightweight runtime telemetry and cloud native architecture, allowing it to support growing cloud infrastructure of any size.

"Sweet Security reduced most false positives and combines all alerts and events into a single alert or incident, which is helpful for the security team to review everything together. Initially, we had Defender for Cloud integrated with Sentinel, which did not provide complete visibility into SharePoint and all other cloud resources. After implementing Sweet Security, we were able to integrate all logs configured with our SIEM and Defender XDR, which was very helpful for fine-tuning incidents and creating organization-specific analytical tools.

"Sweet Security combines all alerts into one single incident, which majorly addresses most of the problems that SOC environments face. We experienced an incident where a user was sharing multiple resources with third-party vendors. We received an alert about someone outside the organization sharing confidential data and project details with a vendor we had no prior communication with. Through the security team's investigation using Sweet Security, we discovered there was a new deployment plan happening with that vendor involving major confidential data sharing. Sweet Security is a value for money solution that helped us track cloud transactions and activities that we were previously unable to monitor.."

Prajwal Chougale
SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

"Detection and response is one of the best features I could observe. Cloud detection and response continuously monitors runtime events across all virtual machines, containers, and Kubernetes clusters. It flags live attacks as soon as they happen. Vulnerability management is another best feature I can recall at this moment because it evaluates whether the flagged CVEs are loaded into memory or actively executing, which allows our security teams to address those vulnerabilities on live data. I have seen cases where workload protection was handled by Sweet Security. It establishes behavior baselines for containers and serverless functions to identify anomalous process executions. It has played a huge role in terms of detection and response components. Runtime checking of runtime vulnerabilities and workload protections have been particularly valuable.

"The vulnerability management feature scans all our container images and has flagged 500 critical vulnerabilities. Our developers were overwhelmed fixing all 500 flaws, requiring multiple weeks of patching, testing, and updating dependencies. Out of these 500 flagged vulnerabilities, 480 of them belong to unused background libraries that are never loaded or called by our application code. 15 of them are loaded into memory but are isolated behind strict internal firewalls and cannot be reached from the internet. Five of them are actively loaded in our memory. Sweet Security has helped us analyze the correct vulnerabilities in our systems. It helps us focus patching efforts strictly and not pay attention to unwanted vulnerabilities that are sometimes flagged by our internal security system. It has saved multiple weeks of our developers, testing teams, and product teams time. We gained scalability in our bandwidth and were able to observe the same number of employees and developers maintain another application in the same timeframe. It does not only flag genuine vulnerabilities, but it helps detect genuine and false cases as well. It has definitely played a huge role in terms of cybersecurity for me.

"When we talk about effectiveness, I can provide a quick example. During the August sprint, it transformed our risk prioritizations by shifting our focus from static CVE severity across real-world runtime. Instead of treating every critical static vulnerability as an emergency, Sweet Security evaluates live execution contexts for us. Runtime reachability is inspected by Sweet Security to determine whether the vulnerability code is actually loaded into system memory, actively

executed, or connected to exposed internet-facing endpoints. If the vulnerability library is sitting dormant on a risk, it is safely deprioritized. We do not consider every attack as fatal. It has helped us establish true prioritizations for us. The impact could be seen when we specifically talk about mitigating risk and development fixes. We have seen a low number of tickets. Our developers no longer receive endless spreadsheets of thousands of static CVE alerts. They receive a clean prioritized queue containing only active reachable risks. We obtained precise guidance since it is integrated with CI/CD pipelines to map runtime risks back to specific container images, commits, or pull requests. It provides contextual recommendations rather than generic patch lists. It also restores developer trust and faster SLAs because my team knows every assigned ticket represents verified executable vulnerabilities. Alert fatigue disappears, so patching velocity increases drastically, lowering our overall mean time to remediate..”

NavnathSolanke
senior executive at a tech vendor with 10,001+ employees

Read full review

Other Solutions Considered

"Sweet Security is the first application security solution that we implemented. Previously, security was totally managed by Defender for Cloud, but we later moved to Sweet Security based on client specifications.."

Prajwal Chougale
SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

"We didn't evaluate other tools as we were moving from a purely manual process. Implementing Sweet Security automated our monitoring and alerts, saving us approximately 20% in time compared to our previous manual methods.."

Filippos Malandrakis
Infrastructure & Dev Ops Lead at Babylon Labs

Read full review

"I evaluated other options before choosing Sweet Security, including Wiz and Palo Alto. I also work with Tenable as a CNAPP platform, as they have released a new cloud component as part of their Tenable One platform.."

Verified user
Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

"We evaluated other solutions before choosing Sweet Security, including big names like Wiz and Orca, but Sweet Security stood out for their amazing pricing and because they were much cheaper than Ermetic while providing approximately the same capabilities.."

Elior Duanis

Cloud and compute team leader at a manufacturing company with 1,001-5,000 employees

Read full review

"There are related security monitoring tools. Sweet Security is a better tool and provides layer-by-layer protected environments. It is a key competitor compared to others including Palo Alto, Wiz, and Microsoft Defender for Cloud. With Sweet Security for cloud, security is totally under control.."

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

“The first product we tried was GuardDuty. We had the EKS protection runtime. It was okay, but not more than that. I needed something more than just okay, because I wanted to know each and every event or everything that happens on the operational system we are running on, whether it's an EC2 with Linux or a Kubernetes environment.

The customization that Sweet Security brought was the option to not only cover all of the GuardDuty features but also create their own threat detection rules, and they allow us to create our own. Two years ago, I joked with them, saying that this is the next generation SIEM. The reason being that the old legacy SIEM solution is not really adjusted to the cloud environment.

If you have a solid CDR or runtime protection tool that also gives you options to write those rules and integrate business logic into the tool, it allows you to detect anything specific to your company.

During our examination of the product, we conducted a POC not just with Sweet Security, but also brought Defender for Cloud to run against Sweet Security. Our team created a testing platform with a few servers installed with Sweet Security and Defender on them. During red teaming tests, Sweet Security consistently won over GuardDuty and Defender for Cloud, confirming that this was the correct decision..”

Verified user

Director of Security Operations at a tech vendor with 501-1,000 employees

Read full review

ROI

Real user quotes about their ROI:

"Regarding return on investment, I cannot say how much time or resources Sweet Security has saved since we are a very small team, but I am guessing it saves some time because it's a good tool.."

Elior Duanis

Cloud and compute team leader at a manufacturing company with 1,001-5,000 employees

Read full review

"Sweet Security has positively impacted my organization by providing faster incident response in minutes versus hours, reducing alert fatigue through significant noise reduction because of the prioritization feature, giving better prioritization of exploitable risk, and providing better coverage for both traditional and AI-based apps. Sweet Security also improves visibility across multi-cloud environments and provides a unified visible platform. Most of the cyber landscape is moving toward platform plays, so Sweet Security is well-positioned in this direction. Most importantly, it moves from finding misconfigurations to detecting and stopping threats in real time in the environment.

"Alert fatigue is always happening because at the end of the day, what we look for is not swimming through noise. Therefore, time is saved by the analyst or security team. The ROI is that we are not waiting for a breach but being proactive rather than reactive. Most people in that proactive phase find that it gives them the ability to find their infrastructure's breach attack paths and understand where they are most vulnerable to exposure. Sweet Security really does provide that proactive rather than reactive mentality within the cyber landscape.

"Sweet Security has helped my team and my partners prioritize risks and threats more effectively because everything that comes out represents real-life detects and threats. Every time we see a threat, we push it through to our first-line support team so they can action it. Everything we see on Sweet Security then gets pushed and actioned because it represents real-time threats, and we are getting ahead of the curve. We can then over time as an ROI see where we are best suited and where we are finding most risks. From there, in our security stack or platform, we can assess whether we need to invest in a new tool, giving us ROI to take through the board to explain that this is where we are getting breached most and that having a tool like X will help with Y.

"I have seen a return on investment where time saved is the best benefit because we are not working through hundreds of vulnerabilities. Sweet Security condenses it down, contextualizes it, and allows us to identify what is really going to breach us in real time. That is the best ROI. Additionally, we can spend less time worrying about where we will not get breached with vulnerabilities that might not be anywhere near breachable. However, if we find that certain cloud vulnerabilities

come up time and time again, we can look into a tool that will help that as well. We can invest in that tool and go to the board or executive level explaining that we need this tool because Sweet Security has pinpointed specific issues, and we need to have this to prevent that from happening because we are seeing that as an ongoing problem we keep finding using Sweet Security..”

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

Use Case

"I'm mostly using Sweet Security for real-time infrastructure security. If there is any threat, I want to detect it in real time. That's the main use case. Vulnerability management is one other benefit I am getting from Sweet Security as well.."

Filippos Malandrakis
Infrastructure & Dev Ops Lead at Babylon Labs

Read full review

Our primary use case for using Sweet Security is to have more eyes and visibility to be able to catch things at runtime and not in a static way. I believe this offers more effective control.

Reviewer302234
Works at a tech services company with 201-500 employees

Read full review

"We are cloud native and are using Sweet Security for call runtime protection. It is much bigger than just runtime protection, but the main use case was bringing Sweet Security for runtime protection services and it grew into a platform that we can utilize for many different things.

We are using it instead of a CSPM and for visualizing what we call code-to-cloud, our code-to-cloud vision, to better understand the different packages and different dependencies that we have within the cloud runtime. It helps us a lot in understanding which vulnerabilities we should tackle from the code perspective.."

Verified user

Director of Security Operations at a tech vendor with 501-1,000 employees

Read full review

"I have been using Sweet Security for approximately one and a half years. For our organization, Sweet Security blocks injection attacks and model manipulations in our production environment. With its help, we detect and respond to runtime errors that occur on our system. Most of the time, static scanners flag thousands of theoretical vulnerabilities, causing alert fatigue for our security operations team. Sweet Security helps us track execution memory and active process behaviors and system calls to catch live attacker movements from all parts of the world.

"I can provide a specific example. I observed a scenario where attackers discovered a flaw in our systems on our public website. The attacker was running malicious code snippets inside our container, our static container, because no files were written to the disk. With the help of Sweet Security runtime sensor, which hooks directly into the Linux kernel, we noticed a process inside the container calling system admin privileges, something a simple web server would never do. It also detects crypto miners via runtime reachability for us. My software has 100,000 old stacks with unpatched security vulnerabilities. One of the attackers discovered that Sweet Security does not let any attacker into our systems to run any Bitcoin miners in the background.."

NavnathSolanke
senior executive at a tech vendor with 10,001+ employees

Read full review

"My main use case for Sweet Security as a distributor is to distribute to our partners within the UK channel, and they then take it to their customers who are looking for a cloud-native platform that offers advanced threat detection and incident response capabilities to provide deep runtime context to security teams, enabling them to quickly extract actual attack narratives. Sweet Security is designed to protect sensitive data in cloud environments, understand the environment, and respond to any threats as they occur. The platform leverages runtime insights to deliver comprehensive protection across all layers of the security stack.

"I can provide a specific example of how one of my partners' customers has used Sweet Security in practice. Organizations primarily utilize Sweet Security for VM vulnerability management on cloud assets, particularly with AWS, which enhances runtime visibility and enables effective threat detection. Sweet Security is integrated for runtime protection and has evolved to support broader security ranges. It allows users to visualize cloud relationships, understand dependencies, and manage vulnerabilities from a code perspective. Sweet Security provides real-time security event response for security teams.."

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

"Sweet Security is evolved for the cloud native application protection platform. It focuses specifically on protecting cloud workloads by combining runtime telemetry with cloud security postures, identity, and data deployed in AWS, Azure, Kubernetes, or any cloud environment. Sweet Security plays a crucial role in providing runtime visibility and helping security teams prioritize real-time threats that are actively occurring in production. It provides dynamic runtime information for application security rather than just static analysis.

"Sweet Security gives runtime visibility into cloud workloads and Kubernetes environments, correlates cloud infrastructure, workloads, identities, and application activity into a single investigation. It combines all activities related to a single identity and correlates all those alerts to make one incident, which helps SOC teams get all alerts related to that entity in one place. For organizations moving towards cloud environments, Sweet Security provides a reliable solution to protect cloud resources and supports major cloud platforms including AWS, Azure, and Kubernetes environments.

"Before implementing Sweet Security, we did not have a solution specifically for cloud resources. We had a SIEM integrated Microsoft Azure and Defender. After incorporating Sweet Security, we observed a significantly higher number of alerts and more reliable alerts with greater visibility into what was happening at the cloud level in the runtime dynamic timeframe. We were able to get in-depth details about cloud resource sharing, uploads, and downloads, and our SOC team utilized it across a broad range of applications.

"Sweet Security reduced most of the false positive alerts that we were getting through our SIEM. It provided more real-time interaction data, allowing us to identify threats more effectively. The alert logics available in the platform are very helpful for conducting in-depth investigations.."

Prajwal Chougale
SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"Sweet Security is deployed in my organization in a straightforward manner for multiple users across our partners and customers. While some experienced a few challenges, including a couple of bug log connections, the process was mostly easy and quick to implement. Generally, across variant sizes of teams, the setup was effective and took a couple of days depending on the approach from the security teams.."

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

"I wouldn't say the deployment of Sweet Security is too complex. There was some bug in the Sweet Security UI at first that didn't allow me to fully connect the sensor to AWS logs or something. However, apart from that, once they resolved this issue, the installation itself is not very difficult. It's straightforward. It took days to get Sweet Security implemented.."

Filippos Malandrakis

Infrastructure & Dev Ops Lead at Babylon Labs

Read full review

"The deployment was pretty easy. It's just a daemon set being installed on the Kubernetes level, which the team handled easily. The deployment itself can take minutes. We wanted to be sure that we did it correctly, so we deployed it in phases, which took a bit more than a few weeks.."

Verified user

Read full review

Director of Security Operations at a tech vendor with 501-1,000 employees

Customer Service and Support

"Whenever we faced any issue during the integration phase, we received very good direction to resolve the issues. The customer support is very helpful and knowledgeable. They have documentation that is very well organized and presented in a simple way.."

Prajwal Chougale
SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

"The technical support is exceptional. Sweet Security is amazing in that part. They are there immediately, providing us with the best technical people, solving any issue we had. Although we didn't have many issues, the few we had were resolved quickly, so I'm very satisfied.."

Verified user
Director of Security Operations at a tech vendor with 501-1,000 employees

Read full review

"I would rate the vendor support an eight, as we have a very close relationship, allowing me to contact my account manager at Sweet Security anytime, and she gets the right people involved during our weekly meetings and ad hoc meetings, making the support very good.."

Elior Duanis

Cloud and compute team leader at a manufacturing company with 1,001-5,000 employees

Read full review

"Sweet Security excels in customer support, as they provide on-hand, prompt, hands-on assistance. Their customer service and CSM team address issues, and users get a line to a specialist who are the right experts and are involved in technical support. They are quick to resolve any issues that are encountered. This is why, even if the price is a bit higher, users get ROI from the price they pay because of the constant user help provided by customer service and support.

"I would rate customer support a nine out of ten because they maintain a competitive price, offer trial periods, provide follow-up, are very responsive, and are effectively hands-on in assisting and offering prompt service and support.."

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

Other Advice

"The Sweet Security solution requires maintenance from our end, and we would prefer it to require less maintenance if possible.

I would recommend Sweet Security to other users based on all my previous responses, and because they succeeded in getting the biggest results during my POC.

On a scale of one to ten, I rate Sweet Security a nine.."

Reviewer302234
Works at a tech services company with 201-500 employees

Read full review

"If an organization is considering Sweet Security, I would give three key pieces of advice to them. Sweet Security is not just another static scanner; it is a runtime reachability analysis to reset patching SLAs. I would tell them about how it impacts our organization's focus strictly on vulnerabilities that are loaded into memory and reachable by it, automatically filtering out dormant code. They can immediately eliminate up to 90% of vulnerability noise and restore developer trust and accelerate patch cycles, also having a tension-less job for the end customers. I would rate this solution an 8 out of 10.."

NavnathSolanke
senior executive at a tech vendor with 10,001+ employees

Read full review

"When it comes to user experience, more time is needed to understand the tool,

and then everything will fall into place. While integrating with some other SIEM or SOAR solutions such as Netskope, we encountered problems and had to repeatedly reach out to the support team, which was somewhat cumbersome. Licensing and cost have been handled by the higher organization, so we do not get involved with those aspects. My review rating for this solution is nine.."

Prajwal Chougale
SOC L2 Analyst at a tech services company with 51-200 employees

Read full review

“I assess the effectiveness of the machine learning algorithms in reducing threat response time as pretty good. At first, when we started with Sweet Security, the first month or so was pretty noisy with lots of different alerts being raised, but that's understandable. However, as time passed, we don't see any false positives, which is amazing.

The machine learning works extremely well. We use the customizable dashboards and they are excellent in allowing us to create one dashboard for the CISO view. The CISO view is mainly for the CISO and the directors who are operating on the cloud, infrastructure and application security. They want to see things from a high-level, cross-company-wide perspective.

We have that dashboard, but we also created a dedicated dashboard per specific analyst team. We still don't really use the reporting tools much, unfortunately. This is our next step. The next step for us would be to connect the reporting mechanism with our internally developed system that knows how to take off those reports and then do whatever we need with them.

The threat detection capabilities influence our decision-making processes. Whenever we need to make a decision about what should be fixed first or what we should focus on, the team will first go to the threat detection page and learn about the system or the environment that we need to take a decision for.

On a day-to-day basis, around 10 users are logging into the platform. Overall, there might be around 30 or 40 people. The solution requires maintenance, but it is minimal. Once in a while, when Sweet Security releases a new agent, we need to conduct the installation ourselves, as we chose not to allow them to reinstall it remotely.

Overall rating: 10/10..”

Verified user
Director of Security Operations at a tech vendor with 501-1,000 employees

Read full review

“I am using the eBPF sensor in Sweet Security. The usage of the eBPF-based sensor has been pretty low. I was concerned about this initially because these sensors typically are pretty resource-intensive. However, this specific one is below one gigabyte of RAM and has very low CPU usage. The RAM consumption is around three hundred megabytes and the CPU usage is around three percent of one core. It's super low.

I haven't tried the LLM-based reply scanning feature in Sweet Security yet. I recently received a message that they are also doing LLM reply scanning now, but I haven't tested this one yet.

It hasn't really saved me time, I would say. It actually creates more work because it makes me aware of things that I was not aware of before. I would probably receive a different answer from a company that had another tool before and now has Sweet Security, but for me, I didn't have any tool before, so Sweet Security creates more work now. However, it's good to have.

Babylon is a pretty small company, so the number I'll give for Sweet Security usage is up to ten users. That's a small number.

I am a global company with Sweet Security and operate remotely.

I have integrated Sweet Security with AWS and have integrated it with my own on-premises infrastructure as well. I have tried a few more integrations. I requested an integration with PagerDuty and an integration with GitHub audit logs, which they both don't have. They haven't implemented this and it's been almost half a year now. So they have some things, but they could have more.

I would definitely recommend Sweet Security to companies like mine, to small companies, small to medium-sized companies, or startups that need somewhere to start, need to get a lot of things from a single tool, don't want to pay a lot of money, and want to build the initial security. My overall review rating for Sweet Security is seven out of ten..”

Filippos Malandrakis
Infrastructure & Dev Ops Lead at Babylon Labs

Read full review

“I would describe the effectiveness of Sweet Security's Layer-7 network traffic inspection in understanding application requests and responses as very important. Sweet Security monitors real-time API and service-to-service traffic in production while building context around normal versus abnormal application behavior. What Layer 7 detects in Sweet Security is essential because many modern attacks do not break infrastructure; they abuse applications. Traditional CNAPP tools often just look at misconfigurations and CVEs, whereas Sweet Security adds depth by focusing on runtime behavior. Sweet Security's Layer 7 capability means real-time visibility into API and application behavior to detect attacks that bypass infrastructure-level defenses.

“I would assess the integration of LLMs in Sweet Security's vulnerability management as beneficial because they can summarize complex runtime security events in plain English. This gives faster alert triage and investigation and reduces alert noise. CNAPP tools can normally generate many alerts, but LLMs filter duplicates, group related issues, and prioritize real threats. This is why we are experiencing better time efficiency because we are prioritizing real threats and taking away alert fatigue. LLMs help interpret API and application layer behavior, which is useful for understanding normal API flows and authentication abuse, providing strong Layer 7 contextual analysis. Additionally, LLMs enable executive-ready reporting by converting technical incidents into summaries, impact analysis, and business risk explanations, making it much easier to communicate with leadership. The LLM integration with Sweet Security improves detection, reduces noise, and turns complex runtime cloud security data into clear, actionable intelligence.

“My advice to others looking into Sweet Security is to examine whatever cloud-native platform they have, run a free trial, and attempt a proof of value or proof of concept. Learn about it, use it, and compare it to what you currently have. Although it may not be as well-known as Wiz, Palo Alto, or Tenable CNAPP, Sweet Security definitely stands the test of time and is a great product. Everything I have mentioned is truly excellent. Sweet Security represents the next generation of CNAPP that differentiates through a runtime-first approach and focuses on detecting and responding to real attacks in environments. For me, that provides correlating signals across cloud, app, and identity. What stands out against

traditional tools is that we are shifting right in our approach. If you want to be proactive rather than reactive, Sweet Security is a strong CNAPP enterprise vendor that any organization should consider.

“As a shifting-right technology in the production environment responding to real-time threats with Layer 7 integration and LLMs to help contextualize risk and show where breaches will occur rather than providing a long list of vulnerabilities, Sweet Security offers competitive pricing and great customer service. I would highly recommend that people research Sweet Security, trial it, and definitely compare it to their current CNAPP platform. I would rate this review an eight out of ten overall..”

Verified user
Partner Account Manager at a wholesaler/distributor with 51-200 employees

Read full review

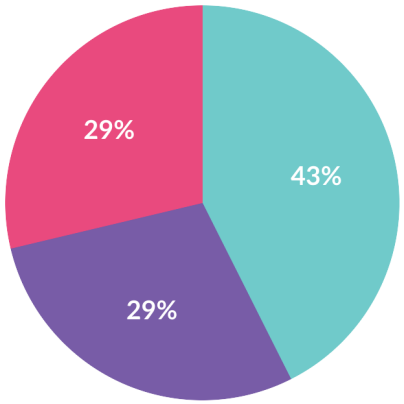
Top Industries

by visitors reading reviews

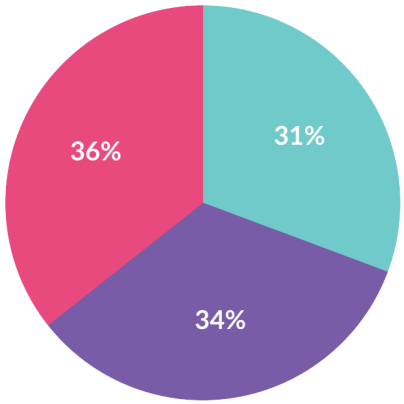
Financial Services Firm	11%
Outsourcing Company	9%
Healthcare Company	8%
Wellness & Fitness Company	8%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944