aws marketplace

Sublime Security

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 5

Valuable Features . . . . . 6 - 9

Other Solutions Considered . . . . . 10 - 11

ROI 12

Use Case . . . . . 13 - 14

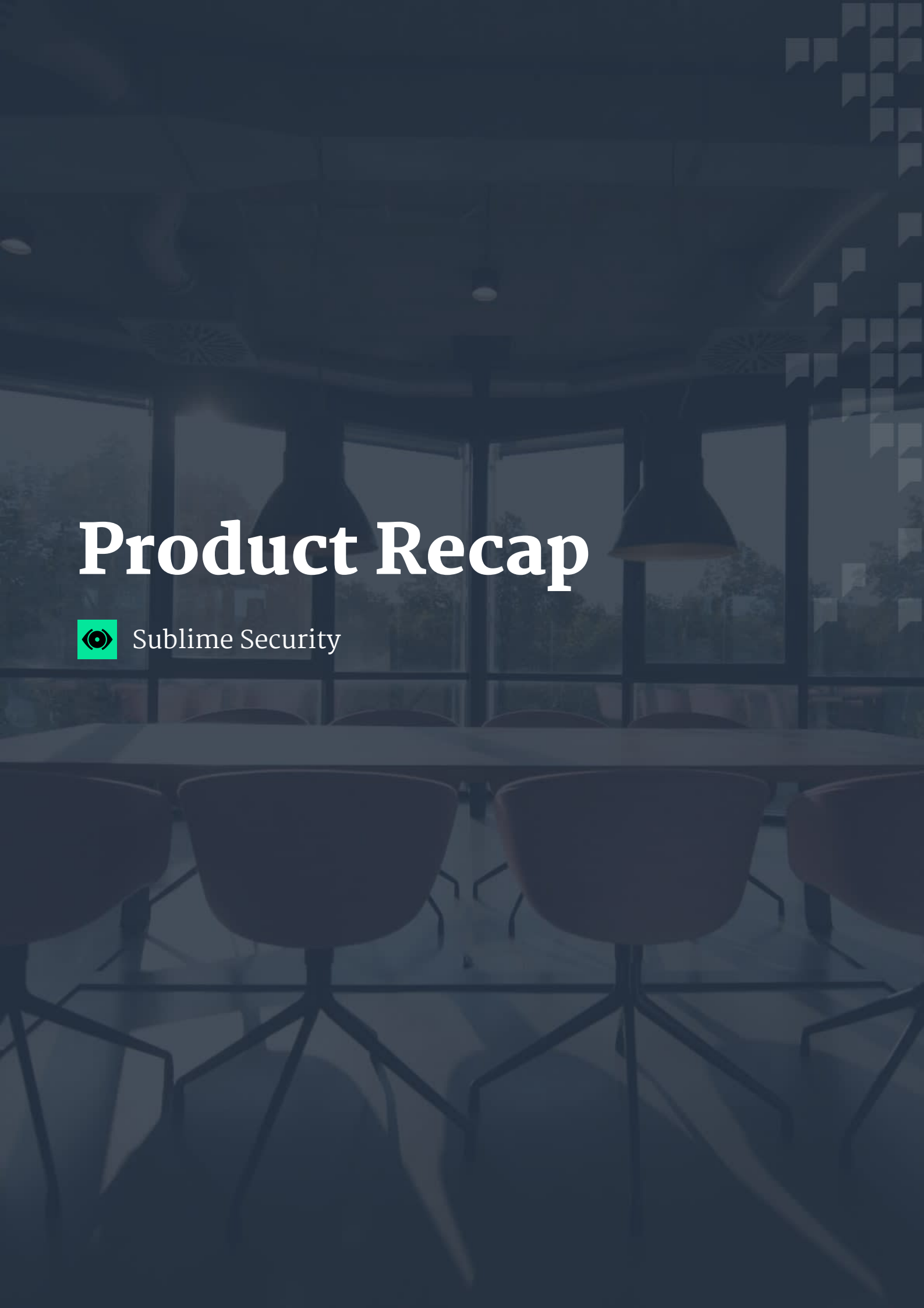
Setup 15

Customer Service and Support 16

Other Advice . . . . . 17 - 19

Trends . . . . . 20 - 21

About PeerSpot . . . . . 22 - 23



Product Recap

Sublime Security

Sublime Security Recap

Sublime's agentic platform stops more email attacks with less work. Our AI agents work like a digital SOC team in your environment, triaging and blocking advanced threats while adapting protections at adversary speed. It provides full transparency and automation by default, with control on demand for advanced teams, eliminating vendor bottlenecks or one-size-fits-all limits.

Core Outcomes (The What):

- Stop More Attacks with Fewer False Positives - block sophisticated threats (BEC, novel phishing, QR-based phishing) and reduce the false positives that waste time and disrupt workflows. Our tailored protections deliver a demonstrably higher catch rate, validated by the world's most demanding security teams.

- Automate the Abuse Mailbox - Our Autonomous Security Analyst (ASA) automates triage, investigation, and remediation of user-reported email, cutting MTTR from hours to seconds and freeing your SOC team to focus on the threats that matter most.

- Adapt Defenses Automatically. - When a missed attack is identified, we can create new coverage in hours. Our Autonomous Detection Engineer (ADÉ) generates, backtests, and deploys org-specific coverage, eliminating vendor ticket limbo.

Differentiators (The How):

- A Team of Agents using AI, Not Just a Black Box - Sublime deploys a team of specialized agents - like an analyst and a detection engineer - that use AI to protect, triage, and adapt your defenses. Unlike an opaque, monolithic AI, our agentic approach provides full transparency into every action, with visible decision history, message lineage, and backtests.

- Org-Specific Protection, Not One-Size-Fits-All - Our Distributed Detection Model (DDM) is the foundation of our platform. It runs per-environment coverage that adapts to the unique attacks you face, allowing us to safely deploy protections that would be noisy in global models - something centralized systems simply can't support. This means higher day-one efficacy and fewer false positives.

- Autonomous by Default, Control on Demand - By stopping more attacks and reducing false positives, Sublime delivers a superior autonomous experience that requires less work. For advanced teams, the platform is fully extensible, allowing you to author your own detections and hunt for threats with a level of precision that one-size-fits-all solutions can't.

Innovative organizations including Spotify, Snowflake, Brex, Elastic, Compass, Anduril, SentinelOne, and others rely on Sublime to secure the business and keep teams focused on strategic defense.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"Overall, the auditability and the ability to evaluate the information in Sublime through various mechanisms made me very comfortable with setting these capabilities to auto-remediation."

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

"Sublime Security helps save my business time and money by reducing 40% of the manual work and increasing IO operations."

Abhijit Mishra

Data Engineer at LG Soft India

"This is why it provides absolute value; it adds a smarter layer that catches anything missed by Microsoft 365 or Google Workspace protection, as attackers can breach those systems easily using flexible detection logic that security teams can quickly customize."

Verified user

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

"Sublime Security is easy to implement; it is simply an integration with the API, and then I can see what is happening after the message arrives in my inbox."

Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

"I like its ability to detect and block."

LARK IT

Head of IT at a manufacturing company with 51-200 employees

What users had to say about valuable features:

"Sublime Security has improved my organization and helped my business because of the optimizations and all the optimization techniques I use, including enabling long-term memory (LTM) and selective context sections and file folder context. Using commands such as right-clicking on folder files and adding them to the clip slot context has been beneficial.

Sublime Security helps save my business time and money by reducing 40% of the manual work and increasing IO operations.."

Abhijit Mishra

Data Engineer at LG Soft India

Read full review

"The best features of Sublime Security that I appreciate the most are advanced phishing detection, as the zero-day phishing attack detection is very powerful, along with deep email analysis and the examination of headers and language patterns.

"Sublime Security has helped my organization by making the visibility of emails much clearer with real-time response after the email arrives in the inbox. It is easy to integrate, I can use it with Microsoft Defender for Endpoint, and the customization is very good.."

Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

Read full review

"What I appreciate most about Sublime Security is the amount of detail that's provided. I've used Microsoft Defender and, in the past, Proofpoint for similar purposes. Both offer valuable insights, but what stands out about Sublime Security is how accessible the detailed analyses are for the messages that have been evaluated. The tools clearly explain why a specific verdict was assigned to a message. This level of detail is essential for analysts and anyone conducting evaluations, as it helps them understand the specific circumstances of their environment. What may be clearly malicious in one organization could be viewed as legitimate or benign in another. The information provided about flagged emails and the subsequent evaluations offers a comprehensive breakdown of how a particular conclusion was reached, which has been incredibly beneficial.."

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

Read full review

"The standout features of Sublime Security revolve around its ability to catch advanced threats that bypass native defenses. Specifically, it excels at blocking malware attachments and stopping Business Email Compromise (BEC), such as CEO fraud and invoice scams.

A major advantage is its fast time-to-value because it isn't a rip-and-replace solution. Instead, it acts as a 'smarter layer' that enhances existing protections like Microsoft 365 or Google Workspace. While native security catches the obvious junk, Sublime uses flexible, customizable detection logic to catch the highly sophisticated attacks that easily slip through standard filters.

Finally, the platform gives you deep visibility and fast search capabilities across all email activity. Without a tool like this, investigations take far too long, and teams lack visibility into what actually breached the inbox. Sublime solves this by offering rapid detection, automated response actions, and the ability to quickly remove malicious emails in bulk.."

Verified user

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

Read full review

Other Solutions Considered

"When I compare it to Microsoft Defender in terms of security effectiveness, I would prefer Sublime Security because it is a separate solution from the main stack, which makes it more proactive in identifying and stopping malicious emails.."

LARK IT
Head of IT at a manufacturing company with 51-200 employees

Read full review

"When I compare Sublime Security with other solutions or vendors, I think it is best for context-aware chat and long-term memory, as well as official GitHub integration and high-privacy local code completion. I have not tried another solution to compare.."

Abhijit Mishra
Data Engineer at LG Soft India

Read full review

"I compare Sublime Security with other vendors and I think it has more features than other vendors. I think Sublime Security is the only one in the market that integrates with the API so easily, offering visibility for all emails, all detections, and all responses, covering everything that happened in my email.."

Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

Read full review

ROI

Real user quotes about their ROI:

"Sublime Security has proven to be a significant advantage for us. We transitioned from relying on a third-party service provided by Cofense for handling user-reported phishing emails to managing everything in-house. This means that our previous relationship with Cofense has ended, and we have fully replaced their services with Sublime, which automates many remediation actions.

Importantly, we didn't need to hire any additional staff; we were able to absorb this responsibility using our existing team. As we activated more functionalities of the tool, our team learned to manage the process effectively. Now, we handle everything internally, utilizing both the tool and our team's processes.."

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

Read full review

Use Case

"The basic functionality provided by Microsoft Defender and its email protections was insufficient for our needs. While it effectively handled common spam and phishing attempts, we required a solution that could address more sophisticated attacks. After researching the market, we discovered Sublime Security. Our organization expressed considerable interest in tools that utilize LLM and AI agent technologies. After conducting a thorough review, we selected Sublime Security, and we have been using it in our environment ever since.."

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

Read full review

"Our main use case is two-fold. Primarily, as a channel partner, our core focus is channel enablement. We actively pitch, demonstrate, and distribute Sublime Security to our partner network, who then deploy it for end-user organizations. Secondarily, we 'drink our own champagne' by running it internally to protect our own business communications.

When we position it to our partners, we frame it as an advanced email security platform. It goes far beyond traditional junk filtering by actively hunting the sophisticated threats that bypass native defenses—specifically Business Email Compromise (BEC), CEO fraud, invoice scams, fake login pages, and malware attachments.."

Verified user

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

Read full review

"Sublime Security is used because one of my clients uses FortiMail for email security, and sometimes malicious emails pass through FortiMail. I was looking on the market for a third-party automation to analyze the emails after they arrive in my inbox. Sublime Security is easy to implement; it is simply an integration with the API, and then I can see what is happening after the message arrives in my inbox. I have two lines of defense with this approach: FortiMail before the message comes to my inbox, and Sublime Security after the message gets inside my inbox.."

Ibrahim Hassan Barakat
Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

Read full review

"I use Sublime Security dictionary for synonyms and the assistant for code comments, documentation, and writing tasks.

The best features of Sublime Security that I appreciate the most are the hover mode, the configurable settings, and the UTF-8 support.

My thoughts on the AI agents, the autonomous security analyst, and the detection engineer in Sublime Security are that it is a semi-autonomous assistant that I can use to perform coding tasks beyond simple auto-complete. Context-aware chat, snippet management, and autonomous tasks are also available. In a window, LLM conversion that understands the full concept of the open files and project repository is also present.."

Abhijit Mishra
Data Engineer at LG Soft India

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.

"The deployment is not complex, but it is also not easy; I would say it is at a medium level. Sublime Security has materials available on the internet where I can find documentation for the product.."

Ibrahim Hassan Barakat

Read full review

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

"It's very simple. You just need to gain API-level access to a Microsoft 365 tenant or a Google Workspace account. As long as someone can provide an API key with the necessary permissions, that's all it takes. The entire process of setting it up is straightforward and easy to implement.

It could take about a week to get the right approvals because of the large organization, but the actual technical implementation takes 30 minutes.

Maintenance is taken care of by Sublime. They do auto updates and addition of new rules and all of that. It's completely hosted by them. It's a full SaaS model.."

Verified user

Read full review

Manager Security Operations Center at a educational organization with 10,001+ employees

Customer Service and Support

"I rate technical support from one to ten, though I have not needed them, so I cannot provide a reliable rating based on personal experience. However, some of my colleagues say they respond very quickly.."

Ibrahim Hassan Barakat

Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

Read full review

"We have a Teams channel that we use regularly with them. They provide updates on new capabilities being enabled, as well as information that allows us to open cases if we have questions. If there's an issue in the platform that they want us to investigate further, this communication channel allows for free-flowing dialogue.

I haven't been disappointed so far; their response is very fast. If there's something more complex, they can connect you with the appropriate engineering resources for a more in-depth conversation. We have our own internal AI review panel, and we were able to get in touch with the person who constructed the LLM and its agentic aspects relatively quickly to address our questions. They offer a wide range of expertise to their customer base on relatively short notice. Overall, they have been highly responsive and very helpful. ."

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

Read full review

Other Advice

"My thoughts on pricing for Sublime Security are that it is affordable and not cost-prohibitive.

I believe over 1,000 users across various institutions use Sublime Security, with thousands of people using it overall, though I do not have complete numbers.."

Abhijit Mishra
Data Engineer at LG Soft India

Read full review

"On a scale of one to ten, I rate Sublime Security a nine out of ten because I believe there are a couple of negatives regarding scalability for catering to enterprise and small to medium enterprises. Additionally, the product requires a learning phase, and it is not readily usable right away.

" Sublime Security merits this rating because of a couple of changes that need to be addressed. If it catered to both small and enterprise businesses on a pricing scale, it would receive a ten, but it is not far away.."

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

Read full review

"We have not yet fully enabled ADÉ, but I am working on getting it activated because we have confidence in the rest of the toolset and its available functions. Currently, it is undergoing evaluation and remains in public beta. For any

components that we activate, particularly those based on AI, we have an internal review board. This board focuses on determining whether a large language model (LLM) or AI component will be used to facilitate model learning in other environments or if it will be restricted solely to our tenant. We want to ensure that our internal organizational messages are not used to train external models. This review process will be conducted on a function-by-function basis, even for tools we've previously assessed. Although we haven't completed this review for the component yet, it is on our agenda. I would like to have it turned on before the end of the calendar year. We are moving forward with this, but it must pass our internal review first. If the review results are positive, we will aim to enable it before the end of December.

I would rate Sublime Security a nine out of ten.."

Verified user
Manager Security Operations Center at a educational organization with 10,001+ employees

Read full review

"My thoughts on the AI Agents for detection are that I am currently trying to review all of its engines. I have put all the engines in the default mode or learning mode to understand how they interact with the messages.

"Regarding the AI, I do not use it, but I have opened the ODL, the detection engine, and while I am not using it, I am trying to understand what can be added to the email security.

"I think Sublime Security currently blocks approximately seventeen to eighteen percent of malicious emails. There are no issues with the email system as FortiMail blocks much before Sublime Security does.

"In my company, three specialists work with Sublime Security.

"My clients are medium-sized businesses and medium enterprises.

"So far, the solution does not require maintenance.

"I give this review an overall rating of seven point five out of ten. I recommend Sublime Security to others looking to implement this product.."

Ibrahim Hassan Barakat
Senior Network Security Engineer at EMAK For Computer Manufacturing (ECM)

Read full review

Top Industries

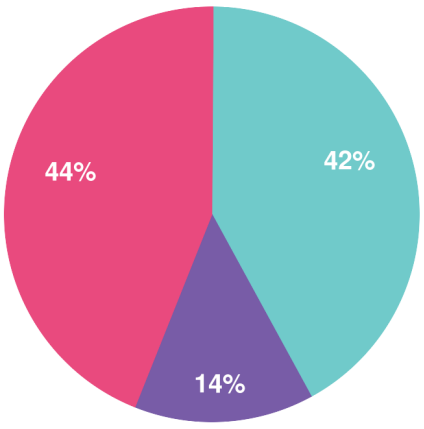
by visitors reading reviews

Financial Services Firm	10%
Computer Software Company	9%
Marketing Services Firm	7%
Outsourcing Company	7%

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 software running on AWS and other platforms. 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