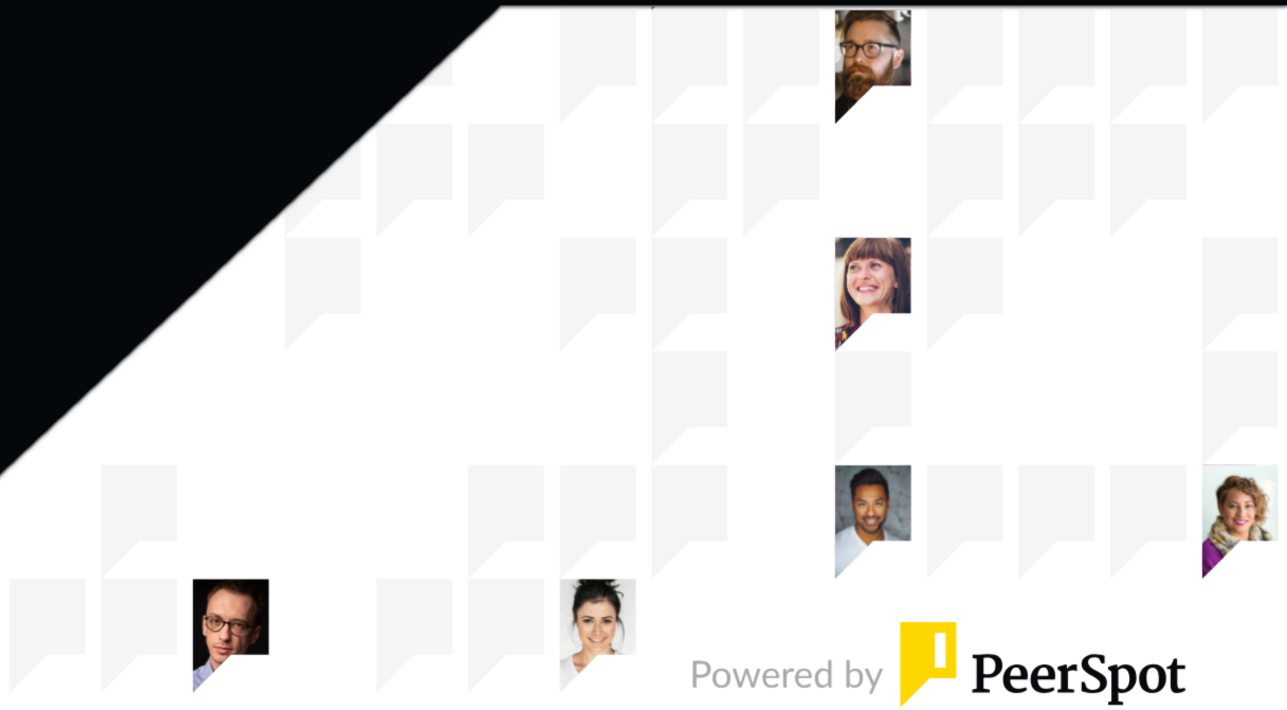
aws marketplace

Abnormal Security

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents

Product Recap

Abnormal Security

Abnormal Security Recap

Abnormal Security is a cloud-based email security platform designed to protect organizations from advanced targeted attacks, such as phishing and business email compromise (BEC), and account takeovers. Their approach is centered on using artificial intelligence (AI) and behavioral data science to detect anomalies in email activity.

Abnormal Security is specializes in protecting email communications, detecting and preventing threats, filtering out spam and phishing emails, and blocking malicious attachments. Users rely on Abnormal Security to enhance their email security, identify and stop sophisticated attacks, safeguard sensitive information, and improve overall cybersecurity measures.

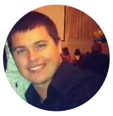
Abnormal Security targets sophisticated attacks that traditional email security measures might miss. Their system analyzes various data points to build an understanding of email behavior within your organization. This includes emails themselves, sender and recipient information, and even business context. By understanding these patterns, they can identify anomalies that might indicate a malicious attempt. Their solution is designed for the cloud, offering quick deployment and minimal configuration. This eliminates the need for complex setup processes often associated with security software.

Abnormal Security customers appreciate the ease of use in setting up and managing the platform, along with its ability to accurately filter out suspicious emails and prevent potential cyber threats. Abnormal Security has been praised for streamlining processes, boosting productivity, improving communication within teams, providing valuable analytics for informed decision-making, and driving success in various projects. Experience the robust security measures and benefits of Abnormal Security to safeguard your sensitive information and maintain a secure email environment.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “It protects us from being business email compromised, which is invaluable for maintaining our security.”



ChrisBrown5

Manager, Information Technology Technical Services at a wholesaler/distributor with 5,001-10,000 employees

✓ “I have never encountered any stability issues with Abnormal.”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

✓ “Ease of use is undoubtedly one of the most valuable features of Abnormal Security.”

Christopher Chambers.

Vice President of Information Security at Comfort Systems USA Inc

✓ “The features that appeal to me most are the combination of auto-remediation and Detection 360.”

Robert Crowther

IT Manager at a media company with 501-1,000 employees

✓ “Initial auto-remediation allows us to auto-remediate before the email lands in the end user's inbox for a split second.”

Verified user

Sr. Director Information Security at a energy/utilities company with 5,001-10,000 employees

✓ “I like Abnormal's threat protection with auto-remediation, but I also love its abuse mailbox feature, which automatically responds to the end user. That feature has a super-valuable security component and helps improve the user experience.”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

✓ “One of the things that I love about them is that the setup and installation are super easy. All you do is give them access to your Microsoft 365 tenant, and through APIs, they are able to do their work. They are doing all this through APIs, so you do not have to install the software and take a month to get it all set up to even see the value of the solution. You could be up and running in less than an hour.”

User:761099

VP of Engineering at a hospitality company with 1,001-5,000 employees

What users had to say about valuable features:

“What I like about Abnormal Security is that it notifies me if any of my partners or suppliers are experiencing a security breach by analyzing their database and identifying potential cyber threats..”

Jasmin Surani

Senior Cybersecurity Engineer (Security Operations & Engineering) at a manufacturing company with 10,001+ employees

Read full review

"The features that appeal to me most are the combination of auto-remediation and Detection 360. The latter allows us to submit emails that seem to have been missed by the system. Within a few hours, a human expert reviews the submission and determines if it represents a missed attack. If so, they explain why it went undetected and then automatically remediate the issue. Additionally, the submitted email is used to train the AI, improving its ability to detect similar threats in the future.."

Robert Crowther

IT Manager at a media company with 501-1,000 employees

Read full review

"Ease of use is undoubtedly one of the most valuable features of Abnormal Security. Its intuitive interface requires minimal training for our IT staff to extract significant value. It was practically plug-and-play, with minimal configuration needed on our end. The product itself has limited configuration options, as it leverages pre-built back-end tooling and algorithms to work its magic. This streamlined design makes it ridiculously easy to use and set up. Moreover, the Abnormal team provides phenomenal support whenever we encounter any issues, far exceeding the support we receive from many of our other tech vendors.."

Christopher Chambers.

Vice President of Information Security at Comfort Systems USA Inc

Read full review

“Abnormal Security is valuable because it features an automated scoring tool that doesn't require much intervention from our team. It enhances threat detection capabilities by making the process automated and is easy to scale to our entire environment.

Additionally, it protects us from being business email compromised, which is invaluable for maintaining our security..”

ChrisBrown5

Manager, Information Technology Technical Services at a wholesaler/distributor with 5,001-10,000 employees

Read full review

“I like Abnormal's threat protection with auto-remediation, but I also love its abuse mailbox feature, which automatically responds to the end user. That feature has a super-valuable security component and helps improve the user experience.

I also like the dashboard. It's easy to get information. For example, when my director asked for numbers, finding all these graphs on the dashboard was great.

We have an API setup with our automation software, so Abnormal gets alerts about spam and malicious threats. This sends alerts to our SOC, notifying them to take a closer look. From an API perspective, integration with our security automation software is extremely important to help draw attention to those sorts of things.

We've got some of those integrations set up, so it can get help from those feeds from an account takeover perspective. Abnormal can monitor many different inputs to draw attention to when an account might be compromised. We have started implementing those integrations to give Abnormal more signals to alert us about possible account takeover. We don't have it set up yet to monitor things going on in Slack or Zoom to be able to tell us when a conversation might be malicious..”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“The most valuable aspect of the solution is the ability to pull out threats from mailboxes quickly instead of going through Microsoft's content query.

Their ability to take things out of the mailbox and catch things much faster than users is excellent.

It is extremely efficient and quick, giving us visibility into internal spam attacks due to its API-based architecture.

The solution is great for detecting the full spectrum of email attacks.

It's important to have normal architect threats in cloud collaboration applications. My ecosystem is my ecosystem. If we are accepting just from outside of the business, and they are coming in through methods such as Slack, Teams, or Zoom, then they're absolutely a concern.

The AI and ML broaden the types of email attacks it can stop. It learns employee behavior. So far, it has helped us to reduce the number of attacks that get through. While it doesn't completely remove threats, it does bring threats down to a manageable level for small companies or small security teams.

It reduces the amount of time spent on managing threats. It also gives us a little bit more flexibility in some instances. It'll mark something as a threat, or it'll start to monitor things naturally. And then some of the integrations such as the CrowdStrike Integration, put these users on a watchlist. That way, if something strange does happen, extra scrutiny is done on those individuals to ensure that there are no account compromises or anything like that.

Abnormal helped us to reduce the cost of redundant, secure email gateway solutions. We went from Mimecast as a secure email gateway, which was a cost per year, to Microsoft's secure email gateway, which is baked into our existing Office 365, and so that was a cost savings immediately. We've saved probably about $50,000. I spent about $180,000 total for the services and tools that we had. However, then saved $50,000 for the secure email gateway, and then on top of that, I have a much, much better product that catches a lot more - which is limiting my exposure at the user level..”

N Wallace

Director of Infosec at a real estate/law firm with 1,001-5,000 employees

Read full review

Other Solutions Considered

“Our company chose Abnormal Security over other options because it is an advanced tool, especially in comparison to other products. It outperforms competitors like Proofpoint in detecting fraudulent, spam, and malicious emails. The use of machine learning sets Abnormal Security apart, making it more effective in identifying various types of harmful emails..”

Jasmin Surani

Senior Cybersecurity Engineer (Security Operations & Engineering) at a manufacturing company with 10,001+ employees

Read full review

“In the past, we utilized Mailroute for our email security. We simply configured our MX records to point to their servers. These servers would then collect and analyze our incoming emails for any threats. Only after deeming them safe would Mailroute forward the emails to our chosen provider, such as Microsoft or another service. We relied on Mailroute during the time we hosted our email on Exchange, before migrating to Microsoft 365. After a long-standing relationship of 15 years, we ultimately decided to switch to a different security solution..”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

“While evaluating solutions back then, Abnormal Security stood out with its advanced AI capabilities in the email security space. While a few other players existed, none matched their level of sophistication. Today, there are new contenders like Avanan. We did consider Proofpoint, impressed by their AI initiatives and user-centric approach. However, similar to Mimecast, they seemed adept at catching signature-based threats but struggled with advanced business email compromise attempts. During our Abnormal Security proof-of-concept, the detections lit up like a Christmas tree, highlighting their effectiveness against these sophisticated attacks..”

Christopher Chambers.
Vice President of Information Security at Comfort Systems USA Inc

Read full review

“Previously, we relied on Mimecast for email security, but we found their product underperforming and their account team unhelpful. The support staff lacked expertise, leaving us vulnerable to phishing attempts and impersonations. We would receive phishing emails from scammers claiming to be the CEO of the company requesting gift cards, and some employees unfortunately fell victim. The need for robust email security, encompassing both phishing and malicious link protection, prompted us to switch to Abnormal Security.

Mimecast is so much of a problem that I have blocked its domain in Abnormal Security from emailing me..”

Robert Crowther
IT Manager at a media company with 501-1,000 employees

Read full review

“They had been using Proofpoint Track, which was expensive. They were trying to save money because Abnormal has much of that same functionality. Also, I think it's a good idea to have two different vendors. Each has different threat intel that they can base their catches on. We can save money and get that defense in-depth because there were things the main email gateway was missing.

It only takes one malicious email that one user interacts with incorrectly to cause company-wide problems, so it's critical to have this area locked down as much as possible. At the last place I worked, we had the same kind of setup where we had an email gateway and a separate second layer. What I like about Abnormal is that it does a great job of automatically detecting and remediating threats. .”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“Last year, we explored alternative solutions. We evaluated Proofpoint, Barracuda, and Mimecast. All three offered API integration with our Microsoft 365 environment, enabling them to detect these types of threats. We piloted Barracuda but found it cost-prohibitive. While Proofpoint was appealing, we weren't impressed, and Mimecast proved overly complex to set up. Consequently, we stuck with our existing provider for another year.

Abnormal Security entered the picture later. We evaluated them and conducted a pilot program. Impressively, within a day of initiating the pilot, they identified a compromised account. Normally, they wouldn't reveal such findings until the pilot's conclusion. However, the urgency warranted immediate notification. They discovered that someone was accessing a low-level account from a location outside the user's usual login area in New York. This incident, coupled with Abnormal Security's overall capabilities, convinced us to switch providers..”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

ROI

Real user quotes about their ROI:

“I can't speak to a direct ROI. However, we did have staff time returned to us, and we have been able to focus on other initiatives around email. It has been a net positive, however, I don't have any specific statistics related to ROI..”

Verified user

Associate CIO & Enterprise CISO at a educational organization with 10,001+ employees

Read full review

“I can't put numbers to it, but our current environment needs to trim the budget as much as possible, and Abnormal has proven itself to offer such good value that no one has even mentioned not renewing it. It's considered an invaluable piece of our security fabric here, so it's such a good return on investment that even cost-cutters aren't looking to cut its cost.

It's cheaper than Proofpoint Track, the product Abnormal replaced. It saved us tens of thousands of dollars plus the cost of paying people to manually run down all of these malicious emails. .”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

Use Case

“Our use case was to pull malicious emails that were getting through our secure email gateway and making it to our inboxes. We were trying to shrink that footprint from a typical 85% to less than 5%..”

N Wallace

Director of Infosec at a real estate/law firm with 1,001-5,000 employees

Read full review

“The primary need for the product, what drove us to that product, was a need for greater email security. We had been experiencing a series of executive impersonation attacks that our current email gateway was not able to pick up. People were pretending to be an executive at our organization and trying to get people to buy gift cards or send them the codes or complete an action or something along those lines for them. We did a proof of concept with Abnormal, and it did a really good job of preventing those attacks from happening..”

Verified user

Associate CIO & Enterprise CISO at a educational organization with 10,001+ employees

Read full review

“We use Abnormal Security to protect us against phishing.

We implemented Abnormal Security to reduce the number of phishing attacks that reach users, internal customers, and other users in our organization. This automated AI-driven technology replaces the need for multiple resources to review, identify, and block malicious emails..”

Verified user

Sr. Director Information Security at a energy/utilities company with 5,001-10,000 employees

Read full review

“We use Abnormal Security for our email protection in addition to Microsoft 365. Previously, we relied on another provider for many years to scan emails for malicious content, viruses, and spam. However, with the increasing sophistication of email attacks, our old provider simply couldn't keep up. Their system involved rerouting our emails to them for scanning before delivery to Microsoft 365. This approach proved ineffective, particularly for attacks like CEO impersonation emails or simple text messages requesting personal information. These attacks didn't contain any traditional malicious attachments.

Abnormal Security serves several key functions for us. Primarily, it excels at detecting malicious content. Additionally, it effectively isolates spam, preventing it from cluttering our inboxes. For legitimate but unwanted emails, such as newsletters, it creates a dedicated "Promotions" folder, keeping our inboxes organized. These are the main reasons we appreciate Abnormal Security..”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

“We have a separate Proofpoint email gateway, so Abnormal is what we consider to be defense in depth. It catches malicious emails that our primary email gateway misses, so we're depending on Abnormal to detect them for us. It also gives us trickier stuff, like zero-day threats.

We also use Abnormal for our abuse mailbox. Our users have a "report phishing" button in Outlook. If they get any suspicious email that they think is malicious or spammy, they can click that button and report it to Abnormal. The Abnormal abuse mailbox automatically analyzes it and responds to the user as to whether it is safe spam or malicious. If it is safe, it sends a copy of the email back to the user so they don't have to look for it in their deleted items.

We have close to 24,000 users. Not all of those are users because a large percentage of those work mainly in Salesforce, but many mailboxes. It's also three different Microsoft tenants because we acquired or merged with other companies throughout the years. .”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“Our main goal is to use Abnormal Security as an additional shield against the increasingly advanced email threats targeting our organization. During our implementation, we've discovered additional benefits. Firstly, it dramatically reduces the time needed for investigations, giving our IT team more efficient access to search and discovery tools than our current system provides. Secondly, it empowers both our threat-hunting and incident response teams, especially frontline responders. This allows them to access crucial data points directly, without always needing to wait for escalations.

The biggest challenge we faced was sophisticated business email compromise attacks. These targeted our customers or vendors, with attackers gaining access to their legitimate email systems and impersonating users to send emails to our enterprise. Our existing security tools were ineffective at detecting this traffic, as it originated from legitimate mail servers and mailboxes of people we regularly communicate with. Traditional security analysis didn't have enough telemetry to detect the anomalies. We needed a solution to differentiate between genuine interactions with our customers and vendors and those disguised as them by attackers who had hijacked their mailboxes. This was the primary use case for Abnormal Security, and it's proven highly effective in addressing this challenge..”

Christopher Chambers.
Vice President of Information Security at Comfort Systems USA Inc

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.

“Abnormal Security is the easiest solution I have ever deployed. Integrating Abnormal Security via the API is simple. I would be comfortable allowing a junior member of my team to deploy the solution.

The deployment took one minute to complete and required one person..”

Robert Crowther

IT Manager at a media company with 501-1,000 employees

Read full review

“I was involved in the initial deployment. It took more time to have introductions on the call than it did to actually do the API integration. The process was very straightforward. The first ten minutes would have been introduction and conversation, and the last four minutes would have been flow integration.

I mostly handled the setup myself.

There is no maintenance needed on my end. .”

N Wallace

Director of Infosec at a real estate/law firm with 1,001-5,000 employees

Read full review

"I wasn't here when Abnormal was deployed, but I've been told that it was quick and easy. According to the story I heard, they were planning to renew Track before they realized how much it cost. Abnormal was easy enough to integrate with low configuration requirements that they could get it done within a couple of weeks, which is almost unheard of for tools here.

After deployment, the solution doesn't require much maintenance so far, but it will as they add more integrations. That is something I will be spending more time and energy on. Periodically, I need to add something to the safe list, but I don't spend as much time as I did on Proofpoint because Abnormal doesn't have as many false positives. ."

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“The initial deployment was very easy. All I had to do was access the Abnormal service through the provided URL. It then requested my global administrator credentials for our Microsoft 365 environment, which I granted. This initial step simply integrated Abnormal with our 365 environment. After that, we configured the settings to determine what kind of alerts we wanted to receive. There were a few things that potentially needed to be done beforehand, such as setting up IT login access and establishing a process for handling the "abuse" mailbox and account takeovers. For account takeovers, we could choose to have Abnormal automatically remediate and lock out the user, or we could have it send an email notification to IT for manual intervention. All these configurations were done through simple checkboxes, which we reviewed with an Abnormal technician during our initial call. By following these steps, we were up and running within an hour.

It was super easy to integrate Abnormal via the API..”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

“It was easy to integrate Abnormal Security via API. It was a lot harder to get through things like contracts and business associate agreements. The actual part of turning the tech on took less than a day.

We monitored everything in a proof of concept. We monitored the results for about a month before we turned it on and active; however, that was just a toggle. The actual part of hooking it up to our systems took a day.

We had security and mail administrators involved in the deployment. We had four people involved; however, it wasn't a massive thing. It was more just to make sure that everyone's voice was included.

Not much maintenance is needed. We don't have to spend a lot of time on the tool to get value out of it. We use it for reporting. We use it to investigate incidents, et cetera, however, there's no hands-on maintenance due to the way that it's deployed. There's no patching or updating VMs or anything like that. That's all handled by the vendor..”

Verified user

Read full review

Associate CIO & Enterprise CISO at a educational organization with 10,001+ employees

“We've implemented Abnormal Security for our main enterprise and a few of our acquired companies that already had cloud email systems. The process is incredibly user-friendly. Authorization involves only two clicks once their support team sends the necessary links for adding them to our enterprise tenants. It's a breeze to set up and eliminates the substantial configuration work required by traditional SEGs, which surprised us greatly. We're glad to be free from policy creation, allowlist, and blocklist maintenance, and even bypass configurations for SPF headers. The tool's elegance lies in its automated backend processes, eliminating the need for manual allowlist/blocklist adjustments, as the technology intelligently manages these aspects.

Integrating Abnormal Security through their API was incredibly straightforward. It took only two clicks! We've even combined it with one of our existing security platforms, and that too was just a single click within each platform thanks to the well-designed API. Honestly, it's one of the simplest security product deployments I've ever experienced in our company.

Only one IT team member, possessing the necessary permissions, could deploy the change..”

Christopher Chambers.

Vice President of Information Security at Comfort Systems USA Inc

Read full review

Customer Service and Support

“I regularly communicate with technical support. It's extremely quick. They are very accurate and thorough. They listen to my concerns, and they repeat them back to me as they understand them. They usually have some type of answer. They understand when I'm looking for something, and I'm not getting what I want..”

N Wallace

Director of Infosec at a real estate/law firm with 1,001-5,000 employees

Read full review

“Technical support is excellent.

I've never had a vendor engaged like this. They're really passionate about improving the product, and whenever we've had an issue, we've got great support. I've never had to escalate anything. They've been great..”

Verified user

Associate CIO & Enterprise CISO at a educational organization with 10,001+ employees

Read full review

“The technical support speed has been fantastic. They're very responsive. I usually get a same-day response on any tickets I submit. The representatives are knowledgeable and helpful, and they always jump right on any issues I bring to their attention. Overall, I haven't experienced any long wait times for support, although thankfully, nothing major has required fixing..”

William Schellhaas

Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

“Abnormal's technical support is incredibly responsive when we encounter issues. We first used them shortly after our initial deployment when we hit a snag with an email we thought should have been blocked. It was just a single email, and they resolved the issue within five minutes. They promptly stopped another attack just a few minutes later. Their response times are truly impressive, and they avoid unnecessary back-and-forth communication. Unlike many tech support teams who spend long periods gathering information before handing things off to another technician for a callback, Abnormal takes ownership and resolves issues swiftly. We always feel heard and valued when we contact them. They get it right, and they get it done quickly..”

Christopher Chambers.

Vice President of Information Security at Comfort Systems USA Inc

Read full review

“I rate Abnormal support nine out of 10. Their support has gotten better. When I started, it seemed like there were a few hiccups, but it has markedly improved in recent months. I had found a support person that I absolutely loved. She was awesome. And she got promoted, and I was like, "I know you deserve this promotion because you are great." It's the support that got me even more excited about the product.

They're so good at following up on unusual cases and strange things that we were seeing in our environment that other customers weren't even noticing. She did a fantastic job with communication and following up with the back-end support. Since she moved on, it sometimes takes a little longer to get back to me when I open a support case. For the most part, they're still highly responsive and do a good job with communication..”

Verified user

Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“Their technical support is incredibly fast and provides detailed responses, which is rare in my experience. Often, support representatives try to close tickets quickly and move on, which is understandable. However, I appreciate receiving thorough explanations, especially for complex issues like Detection 360.

For example, with Detection 360, they might say: "The most recent attack has been contained, and we've implemented a new feature to detect similar messages in the future. Business attacks occurred due to a gap in sender and recipient frequency analysis. To address this, we'll be incorporating a new general model."

This kind of information is valuable because it explains the problem and the solution. Similarly, if we have questions about phishing campaigns, they provide clear answers. For example, if we wanted to run a phishing campaign, Abnormal Security would already know it was a campaign based on our settings and would allow us to continue, which is unlike Mimecast and the other solutions I am aware of that would require digging deep through the settings and do test after test..”

Robert Crowther

IT Manager at a media company with 501-1,000 employees

Read full review

Other Advice

“I would strongly recommend using Abnormal Security. I would rate the product as a nine out of ten. While it excels in functionality and effectively filters out bad emails, it is not a perfect ten due to identified bugs in the console and integration issues with other tools. Overall, it is a highly effective security solution..”

Jasmin Surani
Senior Cybersecurity Engineer (Security Operations & Engineering) at a manufacturing company with 10,001+ employees

Read full review

“I rate Abnormal Security 10 out of 10. If someone had doubts about Abnormal's maturity, I would reassure them that it has been rock solid in my experience. They are continuing to build more into the product all the time, and if it's missing a specific feature, then it will probably happen because it's not a static product.

While some products take a long time to build, Abnormal keeps things moving. They seem to have an excellent sprint cycle, with a solid focus on constant improvement. It would depend on what specifically they are looking for. To me, it acts like a mature product compared to other systems like this that I've used in the past..”

Verified user
Cyber Security Engineer at a hospitality company with 10,001+ employees

Read full review

“I'm a customer.

I'd rate the solution nine out of ten overall.

I would advise others to get experience with Abnormal. Do the demo. The proof is in the pudding. It's one of the very few products that works exactly as it's designed to work. The quality of the output is right there. The service speaks for itself.

Talk to their staff and their team and look at their metrics. Then, turn on Abnormal and see what it catches. Do a side-by-side comparison..”

N Wallace
Director of Infosec at a real estate/law firm with 1,001-5,000 employees

Read full review

“I would rate Abnormal Security nine out of ten.

Minimal maintenance is required.

While some may have concerns about Abnormal Security's relative newness, I'm curious what specific aspects of its youth are causing apprehension. The product is demonstrably performing well for our needs, and I'd encourage those with reservations to consider trying it firsthand. If not, I'm happy to move on from the discussion unless they're open to a hands-on evaluation. I'm always transparent about my experience with Mimecast and other solutions we explored before choosing Abnormal Security. Ultimately, as long as a product delivers results, its age shouldn't be the primary factor in our decision-making.

It's worth checking the Abnormal app store for potential integrations with other platforms your organization already uses, such as Teams, Slack, Zoom, Microsoft 365, Okta, or CrowdStrike. During the proof-of-concept, if Abnormal Security identifies existing integrations with these tools, it can further enhance its functionality..”

Robert Crowther
IT Manager at a media company with 501-1,000 employees

Read full review

“I would rate Abnormal Security ten out of ten.

The previous solution had significant limitations. It functioned like a basic antivirus program from the 1990s. It would simply scan a file and determine if it was malicious or not. It lacked any context about the file or the sender. Abnormal Security takes a completely different approach. By integrating with our Microsoft 365 environment through an API, Abnormal Security understands our organization and communication patterns. It can identify important individuals and prioritize emails from them. This helps to prevent fraud attempts where someone might impersonate a VIP by using a spoofed email address. Abnormal Security goes beyond just checking attachments for malware. It analyzes various aspects of emails, including the sender's domain age, the language used, and other key factors. These elements are then factored into an algorithm that determines whether an email is malicious or legitimate. In contrast, the previous solution only focused on attachments. It didn't analyze the email content, sender identity, or any other contextual information. This made it vulnerable to phishing attacks and other email-borne threats.

This system is maintenance-free after deployment. It functions independently, even if I don't actively monitor it. Once deployed in our environment, it automatically adds new users to the portal and scans them. There's no need for further manual adjustments. While I only receive weekly reports outlining the number of attacks, actions taken, and breakdowns in graphs and percentages including most at-risk users, impersonation attempts, etc., the system itself operates autonomously.

There's very little setup involved with Abnormal. The installation and configuration process is virtually seamless. However, there's one key thing to keep in mind: make sure your email environment is clean before onboarding. This means having an accurate user count and keeping your mailboxes free of unnecessary data. Abnormal charges per user mailbox, so it's important to avoid migrating junk or accounts of terminated employees. These will inflate your bill unnecessarily. Beyond that, there's not much preparation needed for new users. Abnormal is a great product! One potential snag to consider is Abnormal's ticketing system integration. As of now, it doesn't directly integrate with Microsoft ticketing systems although they claim future compatibility. This might be an issue if your mailboxes automatically route emails to a ticketing system. Messages routed this way wouldn't be analyzed by Abnormal, potentially missing threats..”

William Schellhaas
Senior Director of IT at Crunch Fitness West Florida and Atlanta (CR Fitness)

Read full review

“I would rate Abnormal Security a ten out of ten.

It is not that important that Abnormal Security can detect threats in cloud collaboration applications because we are a Microsoft team shop so we are not using a lot of the other collaboration tools. So exploring new frontiers isn't a high priority for us right now. While I'm curious to see what innovations emerge in that space, it's not something we're actively looking to deploy at this time.

While Abnormal Security offers strong capabilities, it hasn't eliminated the need for our existing secure email gateway solution entirely. Our situation is unique due to our merger and acquisition activity. We initially hoped Abnormal could replace our SEG and reduce costs. In terms of features and performance, it outperforms our current solution for specific tasks. However, we couldn't fully switch because our existing SEG provides crucial protection for both on-premise and cloud-based emails. In our acquisition scenario, Abnormal wouldn't immediately protect acquired companies using non-cloud email systems. The migration process would be lengthy, delaying security coverage. Conversely, our current SEG allows us to quickly add protection by simply repointing DNS records, offering immediate security for acquired companies within an hour. Therefore, while Abnormal is a compelling alternative, it doesn't address our specific on-premise email needs due to their current product offerings. If not for this factor, we would readily consider migrating entirely to Abnormal Security.

Although Abnormal Security has delivered cost savings in managing account takeover incidents, the key driver behind its implementation wasn't cost reduction. We didn't have a separate solution focused solely on account takeover before, so Abnormal filled a critical gap in our security posture.

While the platform itself requires no active maintenance, it's still essential to provide some basic care. This involves regularly reviewing audit logs and threat dashboards to ensure their continued functionality. The key difference compared to other platforms lies in the lack of constant updates. Unlike systems plagued by frequent firmware updates, signature refreshes, and hash revisions, this one quietly hums in the background, needing only oversight to confirm its smooth operation.

Our initial internal debate about Abnormal Security's maturity stemmed from the specific problem we wanted to solve by adopting their platform. Our threat actors are highly sophisticated and constantly evolving their tactics, outpacing traditional security solutions. While classic methods are excellent for known threats with established patterns (think signatures based on 20 years of historical data), they struggle to keep up with rapidly changing attackers. This is where AI-powered solutions like Abnormal shine. The significant advancements in AI have only recently matured enough to meaningfully impact security, and companies like Abnormal, focused on cutting-edge solutions, can't boast long-standing track records because the technology itself is barely five years old. So, for those facing novel, bleeding-edge threats, partnering with a provider like Abnormal, operating in the same bleeding-edge space as the attackers, becomes crucial. Our initial hesitation about Abnormal seems rather silly in retrospect, especially considering we only planned to use it as an initial augmentation to our existing defenses. My advice for anyone with similar doubts is to, clearly define what they need to protect and they will realize that tackling cutting-edge problems requires solutions that meet their opponents on their bleeding-edge turf..”

Christopher Chambers.
Vice President of Information Security at Comfort Systems USA Inc

Read full review

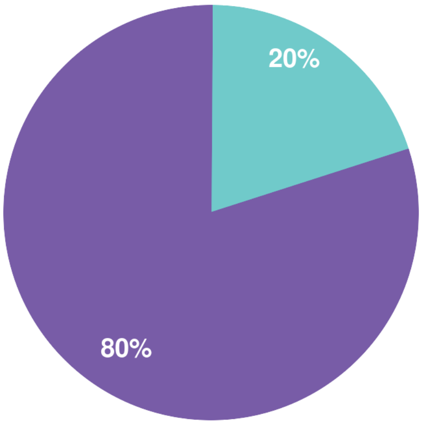
Top Industries

by visitors reading reviews

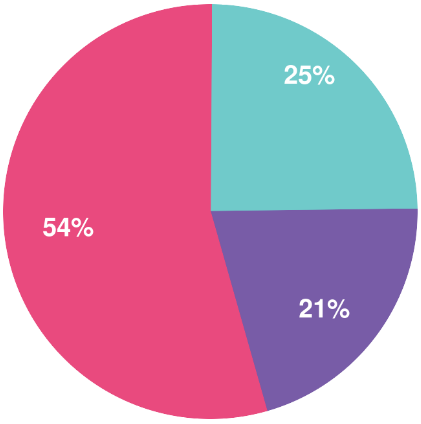
Computer Software Company	15%
Financial Services Firm	9%
Manufacturing Company	7%
Government	7%

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