the AI revolution

How It's Transforming SaaS and Cybersecurity

TRAVA

Artificial intelligence (AI) is unarguably one of the most disruptive technologies of the 21st century. It has taken every industry and sector by storm, and SaaS and cybersecurity are certainly no exception. From faster threat detection and improved response times to task automation and quicker code generation, the benefits of AI across these two realms abound.

Despite all its shiny perks, AI still poses glaring risks to those who overestimate its capabilities. There's the potential for bias, misuse, data privacy violations, and more. While some of these flaws are negligible, others are potentially crippling, requiring SaaS and cybersecurity leaders to employ requisite policies, training, and everything in between fast.

In this guide, based on a webinar by Rob Beeler (CTO, Trava), Jim Goldman (CEO, Trava), Rahman McGinnis (Engineering Manager, Engineered Innovation Group), and Jake Miller (CEO, Engineered Innovation Group), we explore how AI is impacting SaaS and cybersecurity in their entirety. Read on to learn more about the good, the bad, and the yet-to-be-known side of the novel, ground-breaking technology that is artificial intelligence.

The Current AI Landscape

Let's take a trip down memory lane, shall we? Machine learning, which is one of the most powerful subsets of AI, has been around for quite some time now - at least a decade to be exact. Despite the emergence of new AI tools in recent years, it's still widely used by big companies, corporations, and even giants like Google and Facebook.

To many people, the difference between AI and machine learning may not be so apparent. Yet today's fast-changing AI landscape requires this knowledge. Not only are we trying to combat real humans, but now we're combating machines pretending to be humans in many different ways.

The transition from machine learning to newer AI tools like ChatGPT is inevitable at this point. These tools are much more advanced and capable than machine learning, offering many possibilities and use cases. However, making a smooth transition into this new world of AI isn't exactly a piece of cake.

"I think once we've moved from machine learning, which I think a lot of people feel is more structured and tangible, into this world of AI, things start to get a little more fuzzy and even fluffy." — Jake Miller

Which is why it's crucial to first understand what these new-age AI tools bring to the table.

What AI is bringing to the table

FASTER THREAT DETECTION

If you want to keep your company's sensitive data out of the reach of malicious actors, then you inevitably need to respond to cyber attacks swiftly and efficiently. Using human staff to monitor vast amounts of data and respond to potential threats in real-time is a time-consuming process. Modern-day AI can achieve this quickly and thoroughly, sifting through high amounts of information and identifying threats in an otherwise seemingly routine and ordinary activity.

"That's really where something like artificial intelligence can really shine once it learns, and it learns what normal looks like and therefore this is not normal." — Jim Goldman

Although tools for log management and threat detection have been available before, they aren't as powerful as today's AI. They struggle to filter and consolidate large amounts of information efficiently.

"As skill increases, it becomes a task that's just kind of beyond one person, that becomes beyond a group of people or a team. So being able to just have all that filtered down in a way that is reasonable, it's crazy, it's intense." — Ramon McGinnis

SIMULATED ATTACKS

For instance, generative AI like ChatGPT can create realistic phishing emails and other attacks that can be used to train employees and AI-enabled security systems to recognize and avoid such attacks. This can help prevent successful attacks and improve overall security posture.

Generative AI can also move us from a defensive posture, where we react to threats, to a proactive stance, where we predict threats that are not yet happening. We can respond to the predictions to avoid the threats they present, significantly reducing and even eliminating the risk of a breach.

MINIMIZES DUPLICATE TASKS

AI can seamlessly handle the monotonous and repetitive security tasks that can cause cybersecurity personnel to drag their feet. It detects and prevents basic security threats regularly and performs thorough analysis to pinpoint potential security loopholes. With AI, your organization can ensure its network security best practices are consistently implemented without the risk of human error or boredom.

How AI affects company policies, including cybersecurity

Any new disruptive technology is bound to affect an organization's core policies. That's especially the case if the organization is eyeing that technology to augment and fine-tune its processes. Due to the rise of AI, your organization will need to readjust existing policies or create new ones, particularly those focused on cybersecurity.

In this section, we'll explore how AI affects key company policies.

SECURITY AWARENESS AND TRAINING POLICY

Chances are, your organization already has a security awareness and training policy in place. While that's a good thing, the advent of AI means that you might need to give it a revamp.

"So as a company is thinking about do we deal with this, they need to be looking at their training tools and making sure they're educating people, just because they could inadvertently take steps that hurt the company." — Rob Beeler

Workers know that they aren't supposed to share sensitive company data externally. They know topics like social media safety, password management, and mobile device security like the back of their hand. However, new AI technology poses an entirely different hurdle, one that requires a fresh round of training to navigate.

RISK MANAGEMENT POLICY

Walking into new AI territory without a policy that addresses any and all imaginable risks is detrimental from a cybersecurity standpoint.

At its core, risk management is an equation of risk versus reward. Think of it as a sliding scale. How much benefit do you think you can get out versus how much risk it takes to get that benefit out.

“It's going to be different for every entity. And so I really see it evolving into a policy." — Jim Goldman

Here’s an action step:

- Brainstorm ways that your company or organization could use AI or ChatGPT in a beneficial manner. Armed with that knowledge, you'll then determine where to draw the line; where the risk clearly outweighs the reward.

Depending on your unique use cases, you could potentially have a gray area. At the end of it all, you should have a risk management policy that is as in-depth as it is sensible.

VENDOR MANAGEMENT POLICY

It's absolutely crucial to keep a close eye on your vendors. The last thing you want is for them to accidentally share or expose customer data when using modern AI.

"When working with third party vendors, it’s important to understand where their models are hosted. Are they being transparent? Do you actually know what's going to happen to that data when it goes into that model? Do they have their own compliance and regulatory frameworks that they comply with or are certified in?" — Jake Miller

At a high level, the purpose of a vendor management policy is to identify which vendors put your company at risk and then define controls to minimize risk. It starts with due diligence and assessing whether a third-party vendor should have access to sensitive data.
at addresses any and all imaginable risks is detrimental from a cybersecurity standpoint.

AI and cybersecurity: challenges & concerns

It's important to remember that AI is not a silver bullet for cybersecurity. It requires significant resources and expertise to train and maintain AI models. Additionally, there are ethical, privacy, and compliance concerns around the use of AI in cybersecurity.

PRIVACY AND COMPLIANCE

The issue of data privacy is often the first concern that comes to mind.

In most companies, people are freely using AI tools and feeding confidential or private data into those tools to solve a problem. While that's a step in the right direction, they might inadvertently expose that data to outsiders. That's because most of these tools actually have learning algorithms, which means they keep track of every single thing they're fed on.

"A lot of people don't understand what's happening with the new AI technology, so they don't understand. Maybe, hey, I'm putting this data in and it's going out and I could be exposing myself." — Rob Beeler

ETHICS

There are also concerns about the potential misuse of AI for offensive or evil purposes. As of today, no US organization or governmental agency has the mandate to address this issue.

"That may have to be something that's just legislated because when you think about all these models that are being chained together, one person's responsible for their model, but what happens when you have 10 models working together, all created by different people, then working together to create a different result. There's no oversight in that." — Jake Miller

The good, the bad, and the unknown

New sophisticated AI tools have entered the market, hackers have grown in wit and in number, and organizations are now utilizing SaaS applications like never before. This section explores the good, the bad, and the unknown side of the union between AI, SaaS, and cybersecurity.

THE GOOD

AI Code Generation

As a SaaS company, AI tools like ChatGPT and GPT 4 can make code generation a whole lot easier. All you have to do is train the tool on a large dataset of programs, languages and code examples. It learns the structure and syntax of different programming languages, enabling it to generate code that is syntactically and semantically correct.

Using AI for code generation can save time and effort for programmers. The generated code may not always be optimal, however, and may require human intervention and refinement.

New Product Features

AI can generate ideas for new product features by training it on a dataset of product features and descriptions. Once you've trained the model, you can use it to generate feature ideas that could be added to the product.

Using AI for finding new product features can help companies and product teams to come up with innovative ideas.

Automation

The critical advantage that AI brings in SaaS is its ability to automate many repetitive organizational tasks, freeing employees to focus on more critical ones.
For example, an AI-powered chatbot can deal with customers' queries 24/7, which reduces the workload on your customer support team. Moreover, AI in SaaS helps positively impact the user experience by giving quick and informative answers.

"I actually think we're going to see a boom in opportunities with SaaS companies, with generative AI. You're already seeing a lot of new products and new companies pop up using the technology." — Rob Beeler

THE BAD

Algorithms Can Easily Become Biased

At the end of the day, AI's intelligence is determined by the data it receives. The bigger the data set, the more "intelligent" the tool will be. Thus, a lack of information can easily create bias. Plus, let's not overlook the fact that data can easily be manipulated.

Bias can also creep in when algorithms train using unrepresentative data or the reliance on flawed information that reflects historical inequalities. If left unchecked, biased algorithms can lead to decisions that can have a collective, different impact on certain groups of people even without the programmer's intention to discriminate.

For instance, a decision made by an AI system based on biased inputs could lead to false positives and block legitimate users from accessing company systems, resulting in lost productivity, or worse, frustrated customers.

Possible Solutions

How can we ensure that AI systems are fair and unbiased? One potential solution is to take time to understand how these models work, down to the minutest details.

"Understanding what data you're putting in and is it clean? Is it prepared? And testing the outputs of those models. I think at a high level, those are the things we need to do." — Jake Miller

Beyond that, ensure the data being used by your AI models is diverse as well. Data diversity greatly reduces the chances of discriminating against certain groups or individuals.

Another potentially great remedy for the AI bias problem is strict human oversight. However, for this to work, oversight has to be done from the onset and throughout the process. An AI-based system can only be as good as what you put in it from the start and how closely you monitor it from then on out.

"To me, it kind of comes down to two really simple things. Diversity of incoming data, diversity of the data that's being used by the models, and really strict oversight all the way through the process. I think it's one of those things where we're just getting out what we're putting in." — Ramon McGinnis

Potential for Misuse or Abuse

If you thought the good guys are the only ones that benefit from AI, you thought wrong. The bad guys are benefiting as well, sometimes even more than the good guys. This brings up a dilemma or debate of some sort: good versus evil.

Fax machines underwent a similar dilemma back in the day. When they first came out and they were put into offices, everybody thought the technology was great. If you walked by the fax machine and there was a fax on there, you'd just pick it up and read it, and then you'd deliver it to whoever it was meant for.

Chances are, there could have been some very private or confidential information on there. It's like the fax technology just jumped ahead of the thoughts about how to use it in an ethical manner. That's pretty much the same thing we're facing right now with ChatGPT and its ilk.

"This is not the first time we've had to face this. In fact, it's almost like a continuous cycle of new technology being introduced and it catches people off-guard. People come up with all sorts of ideas about how to use it. And then comes the debate about good versus evil, ethical versus unethical." — Jim Goldman

Specifically, cybercriminals may use AI to:

- Create precise and undetectable attacks, such as phishing attacks, at an increased speed.
- Reverse engineer AI systems to gain access to sensitive data sets that were used to train them.
- Scope and identify vulnerable applications, networks, and devices to scale their social engineering attacks.
- Create deepfake social media content with the aim of propagating disinformation and attracting users to click phishing links and go down rabbit holes that will end up compromising their individual security.
- Alter input into AI networks that set off incorrect or unexpected results. For example, an attacker can use concealed malicious code to benign applications, programming codes to "go off" at a specific time, even months after altering the code. This allows them to maximize the impacts of their attacks by infiltrating an application when it is most vulnerable.

Possible Solutions

The good versus bad debate surrounding AI ultimately comes down to personal opinion. It's a relative topic, meaning no one is ethically right or wrong.

"Whenever you get a topic like that, it's not easy to say this is the way it's going to be unless you're a government entity like the European Union, et cetera, that has the power to just put out regulations about how it's going to be." — Jim Goldman

That said, there's no shortage of ways you can utilize to fend off bad actors who are solely focused on weaponizing AI.

As a SaaS company, one potential solution is to filter down the input you're giving to AI solutions. This particularly applies to code review. Make sure your code is meticulous, fluff-free, and doesn't include any unnecessary or excess data.

"When it comes down to usage for safety, we just want to make sure that we're delivering what we need, to get what we get from it, and nothing more. We really want to filter down the information we're delivering to these things." — Ramon McGinnis

Another possible solution is to integrate AI into security systems. AI can be highly effective in network monitoring and analytics, establishing a baseline of normal behavior and flagging discrepancies in things like server access and data traffic immediately. Detecting intrusions early gives you the best chance of limiting the damage they can do.

While it may be initially best to have AI flag abnormalities and alert IT departments so they can investigate, it may be given the authority to nullify threats itself and block intrusions in real-time. After all, it thrives on learning and modeling human behavior.

THE UNKNOWN

Impact of AI Tools on the Usage of Cyber Insurance Coverage

The short answer is...we have to wait and see. At Trava, we're doing some research right now, reaching out across the industry to try to get a read on how cyber insurance companies will react to ChatGPT.

"In other words, if you have evidence of using it for nefarious purposes, does that somehow nullify their need to pay off a claim for a cyber incident, that type of thing? Or they could just simply exclude all claims being paid if the evidence points at the fact that it was a ChatGPT generated attack." — Jim Goldman

Tools that Businesses Should Be Leveraging When It Comes to AI

There are many tools out there, all with unique capabilities and functionalities. To ensure you don't select the wrong tool, know the exact problem you're trying to solve beforehand. What is the use case?

"It really comes down to what you are doing over the course of your day and what's going to make your day easier." — Ramon McGinnis

Above all else, remain authentic. Whether it's ChatGPT or Copilot, use these tools only as inspiration, not as a plagiarism tool.

"Make sure you're doing something that isn't plagiarized, something that isn't generic, something that's still you. Some you just want to use some of those tools, don't let them be just the thing that gives you answers." — Ramon McGinnis

What the future of AI looks like

The future of AI in relation to cybersecurity is anything but blurry. It promises tremendous growth and advancements, punctuated by next-level tools and wittier professionals.

ADVANCES IN PREDICTIVE AI TECHNOLOGY

It may come as a surprise, but predictive AI can generate advanced types of cybersecurity solutions. These self-supervised AI systems can apply their analysis even in rapidly-changing situations. Their self-learning capabilities also enable them to create new conclusions while learning from new observations all on their own.

"I was reading about tools to secure Kubernetes, or tools to secure your cloud environment, things to help you come up with your security policies or help you with those. So I think we're going to see more predictive technology and it will just be integrated into our tools." — Rob Beeler

NEW, MORE COMPREHENSIVE REGULATIONS

There's a need for more comprehensive privacy regulations that aren't limited to a particular jurisdiction. We will see checks and balances come into place from both the technology industry itself and from governmental and regulatory agencies.

"Governmental and quasi-governmental agencies are getting involved. The EU that gave us GDPR, they're not looking at this, they're actively working on producing regulations that would complement GDPR." — Jim Goldman

In the United States, right now at least, we're taking a state-by-state approach to protecting private information. California and CCPA are leading examples, but many other states are looking into that. New regulations will bring a much-needed reprieve across the board.\

The bottom line: AI is here to stay

There's no doubt that AI plays an increasingly pivotal role in SaaS and cybersecurity. It's the engine that keeps these two sectors moving, the glue that holds them together. The companies that will truly thrive in this new age of AI are those that are willing to move with the times, continually innovate using new-age tools and cutting-edge knowledge, train all relevant stakeholders, and give their policies a complete reshuffle.

That's the price of excellence in AI, and every SaaS company or security-forward organization must pay it. The consequences of doing the opposite are dire, from incredibly sophisticated threats to subpar products that leave customers in limbo.

TRAVA

Trava was founded by Jim Goldman and Rob Beeler to protect businesses and insurance agencies from the potential damage of cyber threats. By integrating risk assessment, risk mitigation, and cyber insurance renewal preparation into one, convenient, comprehensive cyber risk management platform, Trava enables business owners and IT professionals to operate secure, productive businesses without fear of interruption or loss caused by cyber incidents.

Talk to Trava