



TRAVA



Carbide



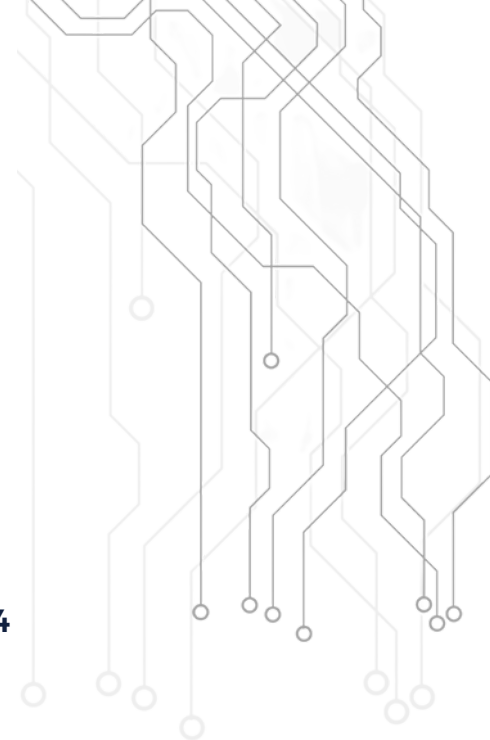
**engineered
innovation
group**

A GLOBAL ESCALATION

RANSOMWARE THREATS, TRENDS, AND SOLUTIONS FOR 2024

Threats, extortion, cyber-terrorism. If this sounds like something out of a movie, think again: a ransomware attack could become your reality. Ransomware is quickly evolving and growing, with the potential to strike any business, nonprofit, or governmental agency. Fortunately, there are ways to protect yourself when you understand the threat.

We've brought together insights from cybersecurity leaders and industry research to help you understand the state of ransomware today and how to protect your business in today's climate.



CONTENTS

3	The Evolution of Ransomware: Trends and Threats in 2024
6	The Business Impact of Ransomware Attacks
12	How to Protect Against the Threat of Ransomware
13	How to Respond to a Ransomware Attack
15	Ransomware and Software-as-a-Service (SaaS)
16	Key Takeaways



THE EVOLUTION OF RANSOMWARE: TRENDS AND THREATS IN 2024

Ransomware is a type of cybercrime where attackers send malware to encrypt a company's data, locking them out, and demand a ransom payment for the decryption key. Despite dating back to the 1980s, the ransomware landscape has significantly changed from a few years ago.

More attacks, multiple attack factors, bigger ransoms, and AI technology are several developments that make ransomware a significant threat to businesses. These top five trends showcase how ransomware could affect you in 2024.

66% of companies hit with a ransomware attack recovered their data within a week if they used backups, Sophos₁.

MALWARE THREATS SURGED 110% IN Q3 2023
reaching 127.5 million emails, KnowBe4₁₁

RANSOMWARE DEPLOYMENT TIME IN 2021
3.85 days, down from 60+ days in 2019, IBM₂

41%
of infection attempts
originate with phishing, IBM₂

\$1.54M
Average ransom
request in 2023, Sophos₁

Rising Attacks and Ransom Demands

The scale of ransomware attacks and ransom amounts are both rising sharply. A report by MalwareBytes₃ found the number of ransomware attacks in the US grew 75% between the second half of 2022 and the first half of 2023. The average ransomware request reported by companies in 2023 was \$1.54 million, nearly double the 2022 average of \$812,000₁. Ransomware requests can reach into the tens of millions of dollars.

Phishing continues to be the most popular delivery method, with emails spiking 173% in Q3 2023 over Q2. August 2023 smashed records with over 207 million phishing emails sent impersonating brands like Facebook, Microsoft, and Bank of America₁₁.

Systematized Attacks from Organized Crime

If you picture ransomware attackers as twenty-year-olds in hoodies working out of a basement, you might be surprised by today's cyber-criminal profile.

"The biggest evolution that I see in ransomware attacks is actually the evolution of sophistication and organization in ransomware. We're talking about organized cartels," explained Darren Gallup, Founder and CEO of Carbide. There are now companies that offer 'ransomware as a service (RaaS)' where affiliates can pay a ransomware cartel to conduct attacks with just a credit card.

Many ransomware attacks originate from outside the country, leaving little to no law enforcement recourse. While a major motivator is financial, there can be a darker element. "You could call it cyber warfare. You could call it cyberterrorism. There will always be the financial gains from it, but there's also an element of disruption or terror," said Jim Goldman, CEO of Trava.

"The gross margin on cyber-criminal activity is high and the risk of getting caught is low, so it's very quickly become the premiere organized criminal activity as we stand here in 2023. Every single one of us, at a business level and a personal level, need to be realistic about the fact that we are targets for those organizations."

Darren Gallup, Founder and CEO,  Carbide

Sophisticated Delivery Methods

There's no one delivery method for a ransomware attack, but many ways one can originate. Popular entry points for an attack include:

- Email
- Mobile phones
- Web servers
- SaaS platforms
- Web applications
- VPN technology

While many of these are not new, what is new is the use of artificial intelligence to infiltrate servers and systems. These work by vastly improving phishing attempts that can trick the weakest link in your cybersecurity chain: your people.

"There is almost always a human element to ransomware attacks," said Gallup. "Social engineering is becoming really sophisticated and, in fact, a lot of the evolution around AI has been quickly embraced by these ransomware attacks."

Take, for example, a phishing attempt. Traditional cybersecurity training teaches that you can easily spot a phishing email by grammatical errors, non-native English, and a message simply not sounding like the sender. Today, a criminal can upload a recording of you talking or a batch of your emails or LinkedIn messages to an LLM-powered AI tool in a matter of minutes. After being trained, the tool can imitate your writing style or even produce live audio that sounds like you—making it much harder to spot.

Systematized Attacks from Organized Crime

If you picture ransomware attackers as twenty-year-olds in hoodies working out of a basement, you might be surprised by today's cyber-criminal profile.

"The biggest evolution that I see in ransomware attacks is actually the evolution of sophistication and organization in ransomware. We're talking about organized cartels," explained Darren Gallup, Founder and CEO of Carbide. There are now companies that offer 'ransomware as a service (RaaS)' where affiliates can pay a ransomware cartel to conduct attacks with just a credit card.

Many ransomware attacks originate from outside the country, leaving little to no law enforcement recourse. While a major motivator is financial, there can be a darker element. "You could call it cyber warfare. You could call it cyberterrorism. There will always be the financial gains from it, but there's also an element of disruption or terror," said Jim Goldman, CEO of Trava.

"The gross margin on cyber-criminal activity is high and the risk of getting caught is low, so it's very quickly become the premiere organized criminal activity as we stand here in 2023. Every single one of us, at a business level and a personal level, need to be realistic about the fact that we are targets for those organizations."

Darren Gallup, Founder and CEO,  Carbide

Sophisticated Delivery Methods

There's no one delivery method for a ransomware attack, but many ways one can originate. Popular entry points for an attack include:

- Email
- Mobile phones
- Web servers
- SaaS platforms
- Web applications
- VPN technology

While many of these are not new, what is new is the use of artificial intelligence to infiltrate servers and systems. These work by vastly improving phishing attempts that can trick the weakest link in your cybersecurity chain: your people.

"There is almost always a human element to ransomware attacks," said Gallup. "Social engineering is becoming really sophisticated and, in fact, a lot of the evolution around AI has been quickly embraced by these ransomware attacks."

Take, for example, a phishing attempt. Traditional cybersecurity training teaches that you can easily spot a phishing email by grammatical errors, non-native English, and a message simply not sounding like the sender. Today, a criminal can upload a recording of you talking or a batch of your emails or LinkedIn messages to an LLM-powered AI tool in a matter of minutes. After being trained, the tool can imitate your writing style or even produce live audio that sounds like you—making it much harder to spot.

No Recovery Guarantee

While the choice of whether or not to pay a ransom is a unique calculus for each organization, it's important to understand that paying a ransom doesn't provide any guarantee of recovery. You may or may not receive a decryption key, which may or may not work to access all of your data. Some organizations receive additional ransom requests after paying, called double extortion, demanding additional payment to keep your data from being leaked to the dark web.

"Remember they had your data for a period of time, so there's nothing necessarily to keep them from extorting you later on," said Goldman. "So, even if you just paid \$15 million to decrypt your data, they could ask for another \$15 million or \$15 million a year not to expose the data they still have."

Zero-Day Vulnerability



While some ransomware attacks come from vulnerabilities a company hasn't detected, many others come from known security issues that a company simply hasn't had time to patch yet. This phenomenon is called zero-day vulnerability, the concept that every day you fail to close a security gap means a potential ransomware attack.

"Keeping everything up to date is super critical today. We've seen cases where there are vulnerabilities in phones or computer operating systems that get identified, but maybe organizations take weeks or even months before all their machines are patched," said Gallup.

Cyber-criminals today have access to web crawler tools which can continually scan sites and networks for vulnerabilities to exploit, making it much easier for criminals to find potential victims at scale. Known criminal groups and affiliates launch dozens of attacks in a month using RaaS platforms like LockBit₅ and CLOP₆— and that number is growing.

"Ransomware is becoming more sophisticated, and it's getting faster. Attacks that used to take 10 days to set up are now easily done within 48 hours."

Katie Kaupke, DevSecOps Manager,  engineered innovation group

THE BUSINESS IMPACT OF RANSOMWARE ATTACKS

The business impact largely depends on the type of business you have and what protections you have in place. All companies that experience ransomware attacks stand to lose revenue and customer trust.

Companies may need to temporarily shut off their systems or pause business during an attack. In the better case, you'll miss out on a few days of revenue and customer frustration due to the business interruption. In the worst case, a ransomware attack can endanger lives at places like hospitals or put your customers at risk of fraud if their personal details are sold.

84% of private-sector businesses lost revenue due to a ransomware attack, Sophos₁

47% OF BUSINESSES RECOVER IN UNDER A WEEK
29% take between 1 week and 1 month to recover, and
24% take between 1 and 6 months to recover, Sophos₁

15%
of businesses have no cyber
insurance policy, Sophos₁

\$1.82M
Average recovery cost
(excluding ransom), Sophos₁

Hospitals and medical practices have become popular targets for ransomware because of the personal data they house. Healthcare companies face the additional risk of lawsuits due to data loss that violates HIPAA.

Industries reporting that they lost a lot of revenue due to an attack include education, business and professional services, media, and construction and property management₁. Schools and state and local governments are popular targets because of their relative lack of IT resources.

Cybersecurity: The Key to Smart Growth

On the other side, smart ransomware protection can fuel growth by legitimizing your business in the eyes of potential clients. Strong cybersecurity practices place businesses in a better position to secure insurance policies and business loans and land enterprise accounts.

Investing in cybersecurity measures and insurance can not only prevent catastrophic losses, but propel your growth.

HOW TO PROTECT AGAINST THE THREAT OF RANSOMWARE

While the ransomware outlook may seem dire in 2024, there are many steps you can take to protect yourself. Think about your cybersecurity defense in terms of layers. The more layers you have to protect yourself, the smaller your chance of a successful attack.

Protecting against ransomware starts with people, but since humans are fallible, you need other defenses. Next, ensure your communications platforms such as email platforms are secure with state-of-the-art malware and anomaly detection.

Finally, invest in backups, cybersecurity monitoring software, and cyber insurance to complete your circle of protection. Let's dive into how to protect yourself one step at a time.



Invest in Employee Training

As we've covered, humans are the main entry point that attackers use to try and gain access to your systems. "We're seeing a huge rise in that sophistication of multi-stage trust social engineering," explained Gallup. "At that point, phishing can be used to get somebody to do something whether it's click on a link, go to a website, receive an email, or receive an attachment."

To combat this, build an employee training program to build awareness of and knowledge around ransomware attacks. Follow these three best practices to build an effective cybersecurity employee training program.

BUILD A CULTURE OF AWARENESS AND ACCOUNTABILITY

First and foremost, build a culture of awareness around ransomware and phishing attacks in your organization. Talk about it at quarterly or annual meetings, encourage managers to lead on this topic, and provide lunch and learns or webinars around the topic.

"If people don't realize how important this is, it won't matter how good the security awareness training program is because they won't take it to heart and they're going to blow it off."

Jim Goldman, CEO of  TRAVA

Outside of making cybersecurity a recurring talking point, build accountability into your training program. Require employees to complete training and send a notice to managers for a reminder when one isn't done. You can also create incentives like a prize drawing or free food.

REINFORCE SECURITY PROTOCOLS YEAR-ROUND

Since cybersecurity is an ever-present, changing threat, don't limit yourself to one or two hours once a year. Instead, engage employees at least once a month. Companies with larger IT departments can build their own training, but small businesses can license a training curriculum like, don't limit yourself to one or two hours once a year. Instead, engage employees at least once a month.

Companies with larger IT departments can build their own training, but small businesses can license a training curriculum like [InfoSec](#).

"Probably the least effective security awareness training method is the way traditionally it was done, which was an annual training. What we do at Trava is more effective and that's doing 15 minutes a month. So, on the first day of each month, we send a notice and link to the monthly training. It only takes 15 minutes, it's engaging, and it's always on a different topic."



MAKE YOUR CURRICULUM ENGAGING AND INTERACTIVE

Research shows that employees engage better with content that is short, visual, and interactive. Rather than an hour-long recording talk or webinar, create training content that employees can complete on their own time, wherever they are.

Aim to make your content engaging and even entertaining, like a funny video. You can even offer multiple formats so your team can choose whichever one suits their learning style best. Use tools like quizzes to gamify and engage participants and measure how much they're retaining the information.

Follow Cybersecurity Best Practices

Many of the IT best practices you've heard about for years are still effective at preventing ransomware attacks. While ransomware has evolved, following these practices as a baseline will continue to set you up for success. These practices include:

- Install antivirus software on all devices with regular scans.
- Implement multi-factor authentication (MFA) for your logins to prevent threat actors from accessing user credentials.
- Practice good password management, such as requiring strong passwords changed frequently.

Use end-to-end data encryption, especially when you have a distributed workforce. 97% of organizations that had data encrypted recovered their data¹.

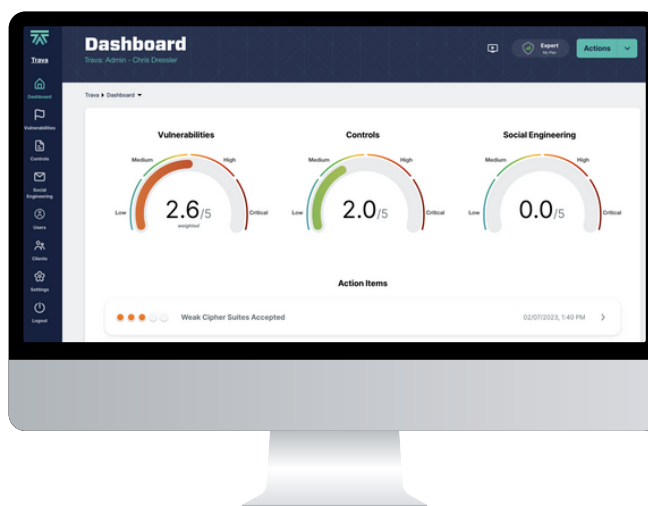
Create an Incident Response Plan

Heading into 2024, it's realistic to assume that you will have a ransomware attack sooner rather than later. With this view, you can prepare your company for the steps you'll take when one does happen. An incident response plan, also called a recovery plan, should include documentation for your backup procedures, action steps, and crisis communications in a ransomware situation.

Katie Kaupke, DevSecOps Manager at The Engineered Innovation Group, Kaupke explains how an incident response plan comes into play in the stressful moment when a ransom note is received.: “When you get into a ransomware situation, you need to access your backup and you need to get your system back up. It can become a panic situation, and things can go wrong when you're trying to work with a tight recovery time. So, the clearer your steps are and the more that you have practiced them and made sure that it's going to work, the more you'll relieve some of that stress.”

Just like you would practice a fire drill, review and practice your incident response plan once a year to make sure your team knows the procedures and your documentation stays up to date.

Monitor for Threats



Since your business faces zero-day vulnerability where any security weakness can turn into a ransomware attack, you need to monitor threats in real time. Monitoring software like [Trava](#) equips your business with a dashboard that gives you visibility into security gaps and early detection of a potential ransomware attack.

“In today's age, like, you should be scanning your environment constantly. The tools exist to do it. Because if you're not, the criminals are. And when they find that vulnerability, they're going to come looking for a way to execute upon it before you get around to your next monthly or whatever sort of iteration of scan you're doing,” said Gallup.

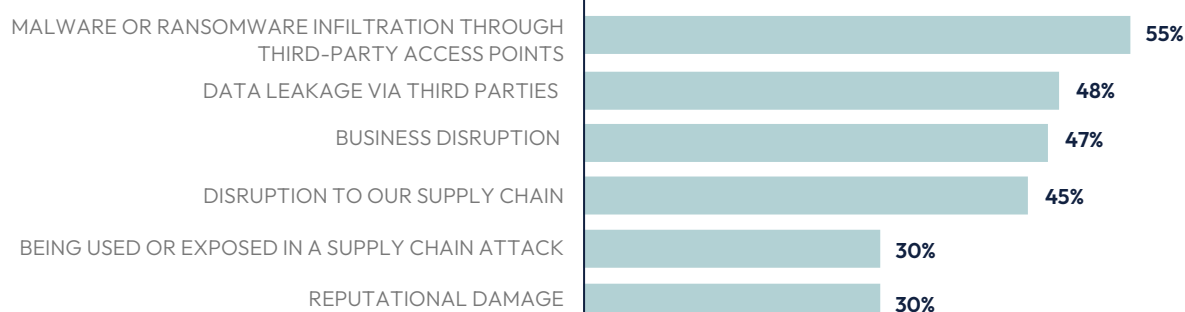
While preventing attacks, monitoring software also gives you peace of mind with [compliance](#) to SOC 2 or ISO 27001 or a security credential you can take to your insurer or customers.

Monitor and Minimize Access

Another vulnerability for ransomware attacks is third-party access. Most businesses contract with dozens, if not hundreds of vendors. Granting access to these parties who may not share your security protocols can be a risk factor.

In our research on third-party access with Cyber Risk Alliance⁷, we found that 60% of companies experienced a cybersecurity event in the past two years due to a third-party partner with access privileges. 45% of these companies reported losses of over \$100,000, with several paying more than \$1 million.

Impacts of Potential Third-Party Breach



Q: Thinking about the impacts to your organization of a potential third-party breach in the next 12 months, which of the following would you say your organization is most concerned about? Please select up to 3.

Another area where companies can protect themselves is by paying attention to and limiting employee access.

“It’s very easy to fall into a trap where you’re moving fast and engineers may have blanket access to a ton of infrastructure, much of which they don’t need to be using,” explained Kaupke. “You want to make sure that those access controls are least privileged. Make sure that people actually need the access that they’re using or that they’ve been granted.”

Use Backups

Of course, every company knows they should have backups. But how your backups are structured can make the difference between recovery and data loss.

“Make sure that your backups are not stored on the same network as the rest of your system or application,” advised Kaupke. “If your application is compromised by an attack like this and they gained access to your network, if your backups are on the same network, your backups are no longer useful.”

45% of companies hit with a ransomware attack recovered their data within a week if they used backups, Sophos¹.

Secure a Cyber Insurance Policy

Like other liabilities in your business, having insurance can give you peace of mind and a financial safeguard if an attack occurs.



There are two types of cyber insurance: a standalone policy or one that's wrapped under other insurance categories. Both types give you key protection. Before going out to request a quote, it's important to understand how underwriters will assess your risk factors.

Unlike most other kinds of insurance, cyber insurance companies can't rely on actuarial tables or historical data. Because of the reality of zero-day vulnerability, the security protections that you have in place today could be irrelevant in a matter of days. Cyber insurance companies need to assess your real-time security risk profile to underwrite a policy, and they need external validation to make an assessment.

"What we do at Trava is to give validated, verified data about a company's cyber risk posture," explains Goldman. "We objectively scan the customer's environment, and say what percent of the machines have MFA enabled or identify people with administrative privileges who don't have it enabled, for instance. We're able to give customized reports to the insurance company with quantitative application data versus qualitative."

Because companies need to have strong cybersecurity practices to qualify for a policy, insured companies are much more likely to recover quickly, recoup their financial losses, and recover their data in a ransomware attack.

97% of ransomware victims with cyber insurance were able to recover their data from a ransomware attack, Sophos₁

HOW TO RESPOND TO A RANSOMWARE ATTACK

Most companies realize they're under a ransomware attack when they reach a lockout screen while trying to log into their system. A ransom note will soon follow, often by email or as a link, with the demand and payment instructions. Most ransomware attacks demand cryptocurrency for payment.

If this happens, don't panic. Switch into action mode to understand the situation, what you can control, and what the next best step is for your business.

FOLLOW YOUR INCIDENT RESPONSE PLAN

If you've taken the steps recommended, you'll have a backup and recovery plan to follow to prevent data loss and recover your data. Keep a cool head and stick to your plan. While each situation is unique and you can't account for every possibility in advance, you should clear steps to gather information and make decisions quickly.

CONSULT WITH LEGAL COUNSEL

When deciding who from leadership should be included in ransomware decisions—often your entire C-suite and IT leadership— don't forget to include your legal counsel.

“Having legal involved is an absolute must. You may be conducting an act that is illegal on other levels, so the decision of whether or not you pay the ransomware is a very complicated one.”

Darren Gallup, CEO and Founder,  Carbide

“There are potential legal concerns with paying a ransom. This is especially true when you're talking about large organizations and wiring large amounts of funds,” explained Gallup. “You could be effectively wiring funds to a known terrorist organization or a known criminal group depending on where you are, where your business resides, and where an individual resides.”

TO PAY OR NOT TO PAY?

In 2023, around 46% of companies decided to pay a ransom¹ to attempt to retrieve their data. As we've covered, not all of those companies recover their data or find their troubles are over. Additional demands and harassment can continue after a ransom is paid.

Most companies that decide to pay a ransom do so because it will be a short-term solution to a difficult situation. But unlike other unexpected expenses, paying ransomware isn't a simple financial transaction. Legal implications, double extortion, and recovery failure can compound financial losses with months-long recovery efforts.

The best financial decision you can make is to proactively invest in cybersecurity before an attack occurs—to minimize liability and losses down the road.

RANSOMWARE AND SOFTWARE-AS-A-SERVICE (SAAS)

According to BetterCloud⁸, companies use an average of 130 SaaS applications—a number that's grown 5x since 2017. Whether you're a SaaS provider or a SaaS customer, it's important to know about the potential for cyber-attacks originating from a SaaS platform. Cyber-attacks originating from software platforms have grown by 300%⁹ and can be a new delivery method for ransomware attacks.

One infamous example is SolarWinds, an IT management firm with software used by 30,000 clients across industries and governmental agencies. In late 2020, the firm disclosed to regulators that it had been hacked by a Russian group known as Nobelium. Not only were its records compromised, but hackers accessed the data of thousands of its customers through undetected malicious code sent out in a security update. Once the hack was finally discovered, customers learned they had been vulnerable for up to nine months.

ARE YOU SECURITY SAVVY? YOUR SAAS BUYERS ARE.

Research from Gartner shows that security is the number-one factor that B2B software buyers look for in a SaaS platform, even more than features and ease of use¹⁰.

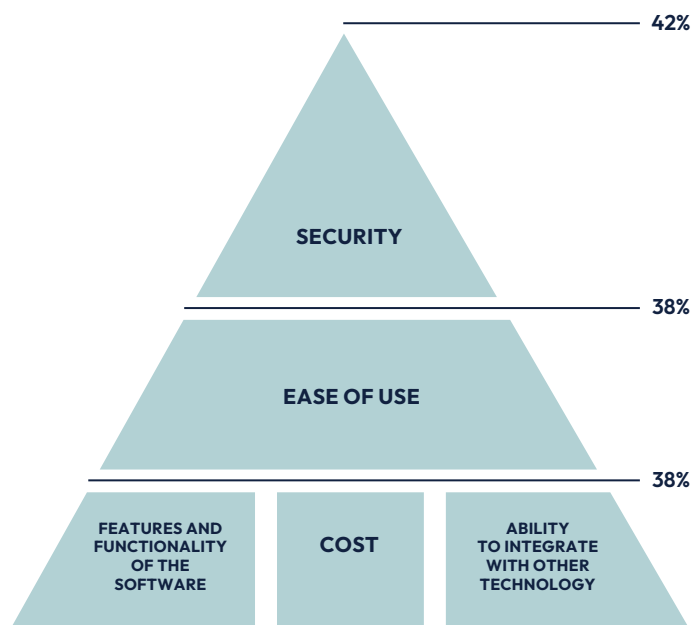
Showcasing your data protection and cybersecurity strength builds trust with potential buyers and differentiates you from your competition. Demonstrating top-of-the-line security credentials can help you land clients in key industries like healthcare and government.

Security Is A Top Priority for Software Buyers

TOP FIVE FACTORS BUYERS LOOK FOR IN NEW SOFTWARE

WHEN EVALUATING SOFTWARE OPTIONS, MOST BUYERS (42%) PRIORITIZE SECURITY - EVEN ABOVE PRODUCT FEATURES AND FUNCTIONALITY TO ENSURE THEIR DATA IS KEPT SAFE AND SECURE AND COMPLIES WITH PRIVACY REGULATIONS.

OTHER FACTORS SOFTWARE BUYERS SEEK INCLUDE EASE OF USE, PRODUCT FEATURES AND FUNCTIONALITY, COST (INCLUDING LICENSING FEE AS WELL AS VARIABLE COSTS SUCH AS MAINTENANCE) AND INTEGRATION CAPABILITIES.



Q. Select the top five most important factors when your company is searching for new software (max 5 responses allowed); Note: Percentages may not equal 100% as respondents were asked to select multiple options.

HOW TO BUILD SAAS PLATFORMS WITH A SECURITY-FIRST APPROACH

Many SaaS startups already have a foot forward in cybersecurity, building their tech stacks with cloud-based infrastructure instead of legacy platforms.

However, SaaS companies can suffer from speed over substance, especially when it comes to security. “If you're building a product, don't wait until the end to realize that you need to pay attention to your networking,” advised Kaupke. “Build in antivirus software and other preventative measures from the start, because it's easier to do this earlier.”

Kaupke also recommends scripting out your security infrastructure as much as possible using a tool like Terraform. “There are multiple tools and, there are a few different ways to do this, but having it that scripted is going to all feed back into having those backup and recovery procedures. It's also going to make it easier to find and correct issues and to make sure that they're corrected if you ever do need to make changes down the line.”

HOW TO SHOP FOR SECURITY-CONSCIOUS SAAS PLATFORMS



70% of businesses planned to spend more on software in 2023
Gartner

If you're searching for new software providers (or assessing current ones), consider security requirements proportionate to your business needs. As you research SaaS solutions, research your audience and what their needs are. If you expect to house ePHI data (medical data protected by HIPAA), look for vendors who can support compliance. Do you have an international client base? If so, you'll want vendors that can support GDPR or an ISO security certification.

Even without those special needs, make sure your SaaS vendors have solid security practices in place and a well-functioning business. Balancing security with cost and other factors is tricky, especially for small businesses and startups, but prioritizing security gives you stability as you grow.

KEY TAKEAWAYS

No business or nonprofit wants to deal with a ransomware attack. However, these attacks are quickly becoming a reality for many companies. Fortunately, with a realistic outlook and a prevention-first approach, you can safeguard your data and your business.

“Prevention and preparedness should always be first, even for a small business. Enable multi-factor authentication everywhere, have a good security awareness training program that people take seriously, and build an incident response plan that you test at least annually.”

Jim Goldman, CEO,  TRAVA

- Ransomware attacks are on the rise, with larger ransoms and potentially catastrophic business impacts. Phishing attempts are getting better and harder to spot, fuelled by AI.
- People are the weakest link where cyber-criminals can gain access—but can be your greatest strength to stop ransomware attacks before they strike.
- To prevent a ransomware attack, build awareness into your culture and make cybersecurity training a year-round priority.
- Zero-day vulnerability means you can't delay security patches. Invest in round-the-clock monitoring tools to spot vulnerabilities and attacks.
- Deciding whether or not to pay a ransom is a difficult decision each organization must make. Just remember, there are no guarantees of data recovery even if you pay.
- SaaS is a growing delivery method for ransomware attacks, and buyers are placing a high value on data security.
- You can minimize the damage of a ransomware attack with cybersecurity best practices, an incident response plan, vulnerability monitoring tools, and cyber insurance.

Ready to safeguard your future?

Contact Trava today.

Trava's not just a tool; we're your dedicated team of compliance experts, ready to walk with you through every step of the process.

www.travasecurity.com 

connect with trava



About Trava:

Trava was founded in 2020 with a vision to protect small and midsize businesses (SMBs) from the potential damage of cyber threats. Trava leverages powerful scanning technology, industry expertise, and an intuitive platform to protect businesses and their customers from cyber threats, prepare them for compliance, while integrating risk assessment and risk mitigation into a comprehensive and user-friendly solution.

travasecurity.com 



About The Engineered Innovation Group (EIG):

EIG designs, builds and engineers innovative B2B SaaS products for entrepreneurs, enterprises and educational institutions. Our mission is to help companies create products and build their software organizations from insights to impact. We specialize in making the complex simple.

engineeredinnovationgroup.com 



About Carbide:

Carbide makes enterprise-class security and privacy accessible to fast-growing companies. Unlike “checkbox”-style compliance solutions, our information security and privacy management platform is based on universal best practices to enable customers to create, promote, and prove their commitment to security no matter which security framework or privacy regulation they wish to comply with. By making it easy to embed security and privacy into the DNA of your organization, Carbide can help sharpen your competitive edge and accelerate your company’s growth trajectory.

carbidesecure.com 

ADDITIONAL CYBERSECURITY RESOURCES

Want to learn more? Go deeper with these additional resources from Trava:

- Dive into the SolarWinds case study with [Third-Party Risk: A Turbulent Outlook](#), a research report by Trava and Cyber Risk Alliance
- Get tips from Trava's blog posts like [Social Engineering 101: Phishing](#)
- Listen to cybersecurity insights with Trava podcast [The Tea on Cybersecurity](#)
- Take a [free Cyber Risk Assessment](#) to learn your cyber risk score

Research Index

1. The State of Ransomware 2023, Sophos
https://assets.sophos.com/X24WTUEQ/at/h48bjq7fqnp3n5thwxtg4q/sophos-the-state-of-ransomware-2023-infographic-1200-1200px_2x.png
2. IBM Security X-Force Threat Intelligence Index 2023, IBM
<https://www.ibm.com/reports/threat-intelligence>
3. 2023 State of Ransomware, Malwarebytes for Business
https://go.malwarebytes.com/rs/805-USG-300/images/CORP_USA_SOR_Pillar_Asset_07262023.pdf
4. Ransomware as a Service, Crowdstrike <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
5. Understanding Ransomware threat actors: Lockbit, CISA <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>
6. #StopRansomware: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, CISA <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>
7. Third-Party Risk: A Turbulent Outlook, Trava and Cyber Risk Alliance
<https://travasecurity.com/learn-with-trava/resources/third-party-risk-a-turbulent-outlook>
8. State of SaaS Ops 2023, BetterCloud
<https://www.bettercloud.com/resources/stateofsaasops23/>
9. AO Labs Notes an Over 300% Increase in SaaS Attacks, AppOmni
https://appomni.com/blog_post/aolabs-notes-increase-saas-attacks-misconfigurations/
10. 2023 Global Software Buying Trends, Gartner <https://www.gartner.com/en/digital-markets/insights/2023-global-software-buying-trends>
11. Phishing Attacks Surge By 173% In Q3, 2023; Malware Threats Soar By 110%, KnowBe4
<https://blog.knowbe4.com/phishing-threats-surge>