CYBERSECURITY TRENDS 2023

AI TIME JOURNAL

Table of Contents

Engage With Our Upcoming Ebooks!

Upcoming Ebooks

Cloud Computing Trends 2023

Digital Marketing Trends 2023

Software Development Trends 2023

AI in Healthcare Trends 2023

AI in Insurance Trends 2023

Get Involved

Thought Leaders:	Contribute Your Insights
Sponsors:	Become a Sponsor
Media Partners:	Become a Media Partner

Cybersecurity Trends 2023

These trends reflect the evolving nature of cybersecurity in response to emerging threats and technological advancements, emphasizing the importance of staying informed and proactive in the face of growing cyber risks.

Cybersecurity in 2023 is marked by several critical trends:

AI and ML Integration: AI and machine learning play vital roles in cybersecurity, both for defense and offense, but ethical and regulatory challenges must be addressed.

IoT and Cybercrime Risks: The Internet of Things (IoT) increases cybercrime risks, with AI and ML used to enhance security, especially in areas like face recognition and language processing.

Diverse Cyber Threats: Various threats, including cloud jacking, ransomware, automotive hacking, malware, and mobile attacks, emphasize the need for robust cybersecurity measures.

Multi-Factor Authentication (MFA): MFA is essential to bolster security against cyberattacks.

Zero Trust Security: The adoption of the zero trust model, where trust verification is required for all network components, is growing as organizations move away from traditional perimeter defenses.

Supply Chain Security: There's a rising focus on scrutinizing suppliers' cybersecurity practices to enhance supply chain security.

Employee Cybersecurity Awareness: Training programs and education efforts are increasing to boost employee cybersecurity awareness and prevent data breaches.

Mobile Device Vulnerability: With the proliferation of smartphones, securing mobile devices for both personal and business use is a significant concern.

Tech Giants' Responsibility: Tech companies are expected to take action to protect customers from cyber threats and fraudulent transactions.

Ransomware Escalation: Ransomware threats are increasing in sophistication and frequency, posing a growing risk to organizations.

Data Protection Emphasis: Data protection and privacy regulations like GDPR and CCPA emphasize the critical importance of safeguarding personal data, and driving compliance efforts.

Cybersecurity Talent Shortage: The shortage of cybersecurity professionals is expected to worsen, highlighting the need for skilled experts in the field.

Automated IAM: Identity and Access Management (IAM) is becoming more automated with the integration of AI and ML, streamlining user access management.

Cloud Security Priority: As more businesses migrate to the cloud, ensuring cloud security becomes a top priority, with a focus on multi-cloud security and shared responsibility models.

Overall, cybersecurity in 2023 involves addressing new challenges, embracing AI and ML, and adopting innovative approaches like zero trust security to protect against evolving cyber threats.

Cybersecurity Trends 2023 According to 30+ Experts

In this comprehensive eBook, we have gathered the wisdom and insights of over 30 cybersecurity experts and thought leaders, providing a detailed outlook on the cybersecurity landscape for the year 2023.

Their combined expertise sheds light on the significant transformations that are underway in the realm of cybersecurity, encompassing AI and ML integration, the evolving IoT and cybercrime risks, a multitude of cyber threats, the growing importance of Multi-Factor Authentication (MFA), and the rising prominence of the Zero Trust model.

As we delve into their perspectives, we uncover the critical cybersecurity trends that are reshaping the way we defend our digital domains, emphasizing the need for a proactive and holistic approach to safeguarding our digital assets.

Kārlis Pots

Tech PR Specialist at Dynatech

1. Ransomware assaults have increased in frequency and sophistication over the past few years. As they can result in huge financial losses and disrupt business operations, these attacks can be incredibly upsetting.

2. Data protection and privacy regulations like the GDPR and CCPA, have highlighted the significance of protecting personal data. With the development of technology and the growing usage of personal data, cybersecurity privacy issues are likely to persist as a significant problem. Many people are still concerned about how businesses acquire and utilize their data.

3. The shortage of cybersecurity professionals. There is a current scarcity of cybersecurity experts, and this gap is anticipated to grow over the next few years.

4. Identity and access management (IAM) will remain a crucial component of cybersecurity as businesses strive to strike a balance between security and employee accessibility. The use of machine learning (ML) and artificial intelligence (AI) algorithms to automate and streamline various IAM operations is one of the most recent IAM trends to keep an eye on.

Protecting sensitive data and systems will depend on enterprises staying informed and proactive in identifying and avoiding security breaches

Ron Sharon

Owner and Ron Sharon LLC

Ransomware is malware that encrypts a victim's data and demands a ransom payment to restore access. Ransomware attacks are becoming increasingly sophisticated and significantly threaten businesses and individuals.

Social engineering attacks are a cyberattack that relies on human interaction to trick the victim into giving up their personal information or clicking on a malicious link. These attacks are becoming increasingly sophisticated and significantly threaten businesses and individuals.

Cybersecurity regulations. Organizations should brace for tighter cybersecurity regulations, influencing data and security management.

AI and Machine Learning. Prepare for more sophisticated AI-driven cyber-attacks as AI and machine learning become integral in cybersecurity solutions.

The Zero Trust model will transition from an optional security measure to an essential one.

Quantum Computing looms on the horizon, presenting both challenges and solutions, making the development of quantum-resistant algorithms crucial.

Ayman Nazish

CEO at SocialSharings

1. Zero Trust Architecture (ZTA): In 2023, we're seeing a shift towards the Zero Trust approach. This means trusting nothing and verifying everything, even inside your network. It helps prevent insider threats and external attacks by constantly verifying users and devices.

2. AI-Powered Security: Artificial Intelligence is being increasingly used to detect and respond to cyber threats in real time. It can analyze massive amounts of data to identify patterns and anomalies, making it a crucial tool for cybersecurity.

3. Ransomware Resilience: With the rise of ransomware attacks, organizations are focusing on becoming more resilient. This includes robust backup and recovery plans, employee training, and better threat intelligence.

4. Cloud Security: As more businesses move to the cloud, securing cloud environments is a top priority. Multi-cloud security solutions and a shared responsibility model are becoming essential.

5. IoT Security: With the proliferation of IoT devices, ensuring their security is vital. More attention is being given to securing these devices to prevent them from being exploited in attacks.

Farhan Siraj

CEO of OSHA Outreach Courses

Organizations can leverage generative AI to create highly realistic and immersive training scenarios like simulated cyberattacks or phishing campaigns for their employees. Such simulations can provide a valuable hands-on experience to workers in a controlled environment, allowing them to respond to threats in real time.

Beyond that, generative AI can create other forms of content like multiple-choice questions and case studies that can help employees better understand online threats. It can also personalize this training material based on the employees' learning patterns to make cybersecurity training more engaging. For instance, if an employee struggles to understand phishing attacks but excels in dealing with malware threats, it can customize the training material to work on the employee's weaknesses.

Daniel Sjöström

Sales Engineer at Maven Wireless

With the recent implementation of the EU's NIS-2 regulation and the growing number of security threats, it's more crucial than ever to ensure our buildings are not only secure but also equipped with fast and reliable networks, particularly as we transition to 5G. As we move into an era where nearly 80% of data consumption occurs within buildings, the advent of 5G technology is poised to revolutionize the daily operations of various types of commercial properties, including hospitals, stadiums, venues, and skyscrapers.

As we integrate more connected devices and systems into our buildings, the security implications become increasingly complex. It's crucial to address these concerns to maintain the integrity of both the physical and digital environments within these smart buildings.

I believe this is a topic that would greatly interest your readers and would like to propose an interview or article where we can share our expertise and insights on this critical subject.

Jason Toy

General Manager at 88stacks

Since cybersecurity is evolving quickly, 2023 will see several trends. AI-driven threat detection and response will rise. As fraudsters become more adept, AI and machine learning will help organizations detect and thwart cyberattacks in real-time.

The zero-trust architecture will gain in 2023. This approach challenges perimeter-based security by assuming all users, devices, and networks are insecure. Multi-factor authentication and strict access controls protect sensitive data and systems.

The IoT will also provide cybersecurity challenges. IoT ecosystem security is important as connected devices increase. Safeguarding IoT devices requires strong authentication, encryption, and vulnerability patching.

Finally, companies will prioritize quantum-resistant encryption. Traditional encryption may become vulnerable as quantum computing improves. To protect sensitive data, quantum-resistant encryption must be designed and applied. In 2023, cybersecurity will protect digital assets and privacy by leveraging current technology, and comprehensive security procedures, and staying ahead of growing threats.

Joshua Spencer

Founder of FortaTech Security

Firstly, I have seen an increasing focus on Artificial Intelligence (AI) and Machine Learning (ML) to enhance threat detection and response. These technologies are becoming integral in identifying anomalies and patterns in vast datasets, helping organizations stay ahead of evolving threats.

Secondly, I think that the concept of "Zero Trust" security will continue to grow. I have witnessed a shift towards continuous verification and validation of users and devices, regardless of their location within the network. Zero Trust ensures a higher level of security by assuming that no one, even those inside the network, can be trusted without proper authentication and authorization, making it a critical approach in the ever-evolving cybersecurity landscape.

Bobby Cornwell

Vice President Strategic Partner Enablement & integration at SonicWall

The first half of 2023 saw overall intrusion attempts up, led by the highest year on record for global cryptojacking volume recorded by SonicWall, as threat actors shifted away from traditional ransomware attacks in favor of a stealthier means of malicious activities. Our data suggests increased law enforcement activity, heavy sanctions and victims' refusal to pay ransom demands have altered criminal conduct, and threat actors are targeting other means of revenue.

Additionally, the seemingly endless digital assault on enterprises, governments, and global citizens is intensifying, and the threat landscape continues to expand. Threat actors are relentless, and our data indicates they are more opportunistic than ever, targeting schools, state and local governments, and retail organizations at unprecedented rates.

Our intelligence suggests that bad actors are pivoting to lower-cost, less risky attack methods with potentially high returns, like cryptojacking. It also explains the reason we're seeing higher levels of cybercrime in regions like Latin America and Asia.

Oleg Shumar

FounderCEO & GetTrusted.io

FAI-powered attacks represent a formidable threat. While AI holds immense potential for enhancing security measures, in my opinion, the malicious use of AI to craft highly sophisticated and targeted phishing emails is particularly concerning.

Cloud security must also take center stage, and it's my belief that organizations moving to cloud environments need to complement the robust security features offered by cloud providers with strong access controls, data encryption, and continuous monitoring to safeguard their assets effectively.

Regarding remote work, which has become the norm post-pandemic, I've seen firsthand that cybercriminals are actively exploiting security gaps in remote access solutions, hijacking threads, and targeting vulnerable endpoints. I think that companies must proactively address these threats to secure their remote workforce effectively.

Chris Hale

President at Technology Response Team LLC

There is a massive increase in phishing attacks, with much better phishing techniques driven by access to AI.
An increase in hacker tradecraft. For example, there was a big attack on MGM casinos.

The bad actor used MGM's helpdesk as a vector to bypass existing cybersecurity measures.

Jason Stockinger

Director, Global Information Security, Royal Caribbean Group

Language Learning Models, and Generative AI have been buzz-worthy topics in 2023. The ability of these models to generate output and replace tasks such as editing, generation of policy, and response to queries is truly awe-inspiring.

On the other hand, the ability to control what these models output and 'create' based on sensitive data input is scary. The lack of regulation in this space will encourage litigation (especially in litigious countries like the US) as these models interact with humans. The SEC just released cyber regulation that for publicly traded companies could have additional impact. It requires companies to really define what materiality is when an incident occurs and to communicate to investors (and The Street) within 4 days.

The leading technology creates cyber issues, and the lagging regulation creates an ever-widening gap for the CISO to educate humans and control AI. This will continue to create sleepless nights for our cyber defenders and frustration for consumers who will continue to have their privacy hacked by bad actors by no fault of their own.

Gregory Hoffer

CEO at Coviant Software

What I hope to see emerge as a cybersecurity trend is a reexamination of how core business services and applications are deployed, configured, and operated. The cl0p attacks on managed file transfer software products like MOVEit and GoAnywhere illustrate the vital role mature technologies play in data management and movement, and how prioritizing convenience over security can have devastating effects.

Many organizations take for granted that software solutions they purchase and deploy are secure by design, only to learn this isn't the case. 2023 demonstrated the frailty of many important back-office systems that had been hiding in the shadows. As a result, 2024 will see a much-needed refocus on properly ensuring (rather than assuming) security.

Vendors will embrace their responsibility to be secure by design, using integral AI and automation to enhance security and usability--and then get to work discovering and evaluating how the software, services, and devices they are using affect their security posture. That is a monumental but necessary task, but there are good, AI-driven tools that can help get the job done. 2024 will see more and better tools and increased usage.

Blair Cohen

President and Founder of AuthenticID

We'll begin to witness how the federal oversight of AI regulation will shift the main focus toward ethical concerns as they relate to cybersecurity and the evolving regulatory landscape.

As cyberattacks and data breaches continue to make headlines, government bodies and regulators around the world are becoming more vigilant when it comes to cybersecurity. They recognize the value AI can play in protecting individuals' data, but understanding how to encourage its development while also mitigating its risks is the challenge.

As policymakers gain more insights and expertise about generative AI, key concerns will revolve around its ethical considerations surrounding bias, security, and privacy. This will involve protecting sensitive data used by AI models and safeguarding against potential misuse. Unfortunately, bad actors also recognize the value of AI, and the difficulty of enforcing these regulations on those who refuse to comply will remain a challenge. However, we will begin to see businesses embracing continuous AI innovation to stay ahead of bad actors, and leveraging it as a core component of their cybersecurity practices to maintain that competitive edge.

Tom Ricoy

Chief Resource Officer at Cigent Technology, Inc.

In 2023, the fight against cyber criminals continues to be an arms race of malware vs. anti-malware. AI has become a powerful weapon for both sides. We are seeing “smart malware” that is more efficient, adaptive, autonomous, and better at evading detection. Like with traditional arms races, the counter is to fight fire with fire. In this case, the defender’s tool sets have started to incorporate AI for better analytics, reduced false positives, and greater operational efficiency.

Cigent, for example, has applied smart technology to its Secure SSD+ drives to automate data protection against ransomware and data theft. One of the core weapons is a smart microprocessor embedded in the data storage itself. This uses AI to analyze read/write patterns to the drive. These analytics provide an efficient and highly effective counter to ransomware by catching it in the act and preventing it from doing damage.

Alan Bavosa

VP of Security Products

Mobile apps are now the dominant way consumers interact with brands, making them an increasing target for attackers seeking personal data, financial information, and more.

Automation and AI have become instrumental tools for cybercriminals, allowing them to scale their operations and execute attacks with unprecedented efficiency and speed. To protect apps, brands and mobile users, manual coding of cyber security is no longer possible to keep up. App makers need to respond in kind to counter the escalating threat of cybercrime on mobile. The implementation of automated, AI-assisted no-code techniques is imperative for dev and cyber teams to keep up.

No-code techniques, empowered by artificial intelligence enable a dynamic defense, capable of adapting to evolving attack strategies. By automating the implementation of mobile app protection, coupled with real-time threat detection and automated response, mobile developers and brands can stay ahead of what's next in mobile app defense.

Christen Costa

CEO at Gadget Review

While I'm not an advocate for AI in all areas of business (for example, I think generative AI for content is a bit ethically questionable), I am an advocate for its use in IT and cybersecurity. This is an area of business that has probably utilized AI the longest, but even just in recent months, the ways in which it is implemented have significantly expanded.

From machine learning to cybersecurity, to software analysis and so much more, AI is doing a lot of both the menial IT tasks and the more complicated ones. With cybersecurity, it has many functions that operate around the clock, like assessing network vulnerabilities.

Businesses can significantly improve their data protection and network security with the use of AI, which in turn helps reduce the likelihood of successful cyberattacks or data breaches – which can be the end of a business.

Mark Stamford

CEO at OccamSec Cyber

Get ready to see generative AI applied everywhere in 2024-- with the inevitable crash, before settling into actual useful applications. Right now it's being applied to everything anyone can think of... creating a lot of noise and a lot of overspending before an inevitable clawback.

The technology has benefits, but the application is not universal and will take some time to become so. AI will likely constrict, and open source will improve its capabilities, so eventually anyone will be able to mine it for their specific benefit.

Attackers will be front and center. Generative AI will produce better phishes, malware, and bugs, and analyze environments for exposures. On the defender side, we'll see integrated products that don't slice a problem ever thinner, but start to reconstruct it in a way that allows organizations to effectively defend themselves.

Obviously, providers will continue putting money into infosec, but their bottom line will always be a determining factor. And of course, government regulation will be discussed, and we'll see attempts made.

Zach Varnell

Cybersecurity Consultant at Asteros

We're seeing a notable shift in the capabilities of adversaries, significantly amplified by the adoption of Large Language Models (LLMs). Historically, precise, surgical cyberattacks were the domain of those with deep expertise. But now, LLMs are leveling the playing field. These models serve as force multipliers, allowing individuals with even limited experience to launch highly targeted attacks with the kind of efficacy that was once the hallmark of seasoned experts.

LLMs are reshaping various sectors, enabling average individuals to make impactful strides in their respective fields, and hackers are certainly capitalizing on this trend. As they harness the power of these models, the challenge for cybersecurity professionals grows exponentially.

In response to this threat landscape, it's crucial for professionals to be at their absolute best. It's not just about understanding these tools, but proactively leveraging them. Establishing comprehensive vulnerability management programs, bolstered by rigorous penetration testing, has become essential. In this age of rapid technological progression, preemptively addressing threats is the cornerstone of maintaining a secure environment.

Prabhsharan Singh

Software Engineer at ClinicSpots

Cybersecurity is another rapidly evolving field with several emerging trends forecasted for 2023.

Firstly, Automated Cyber Threat Intelligence is expected to surge. As cyber threats become more sophisticated, the need for automated threat intelligence - capable of predicting and preventing attacks - will become paramount.

Secondly, Secure Access Service Edge (SASE) will likely become a standard, integrating networking and network security services into a single cloud-based service. This will enhance security for remote workers, a crucial consideration given the rise of hybrid work models. Thirdly, Privacy-Enhancing Computation is anticipated to gain traction.

This trend focuses on processing and analyzing data in a manner that preserves privacy, a direct response to the increasing emphasis on data protection and privacy laws.

Henri Hubert

Founder of AI Engineer Hub

In 2023, AI is pivotal in cybersecurity. Its real-time analysis intercepts threats early, and machine learning detects anomalies. AI tools, like chatbots, enhance cybersecurity awareness.

Yet, challenges arise. AI's sophistication can be misused, biases may cause false positives, and data poisoning attacks loom. Quantum computing, while promising, might challenge current encryption. However, it also introduces quantum-encrypted communication, offering robust security. Ethical considerations and continuous learning models ensure AI's adaptability against evolving threats.

Deepak Bala

CTO at Rocketlane

Automation is a key trend in 2023. Enterprise buyers seek businesses that comply with leading security standards such as SOC2 Type 2, GDPR, and ISO 27001. Automation of cybersecurity helps with the real-time compliance of these standards. By continually monitoring critical infrastructure using automation, companies can mitigate threats as they happen.

The best companies can remain on the right side of security in seconds rather than days. For example, hackers are constantly scanning for servers that are not password-protected. You are doomed if your company cannot secure them faster than the hackers can find them.

Aimei Wei

CTO & Founder of Stellar Cyber

A key trend in 2023: the threat of a recession, coupled with a talent shortage, means companies are looking to consolidate security tools.

The challenge is, which ones?

Secure Access Service Edge (SASE) and Extended Detection and Response (XDR) bring the best of new ideas while keeping the best of your existing tools.

The old way of thinking about security was logs. That is slow, and why you hear about so many ransomware attacks happening 6 months after the hacker gained access.

AI + SASE + XDR ensures you see the forest. This arms you with a threat detection and response framework that is purpose-built for modern attacks.

AI-driven algorithms can analyze vast datasets in real time, identifying anomalous behavior patterns and potential threats more accurately and swiftly. This empowers organizations to proactively defend against cyberattacks. AI can sift through vast amounts of data to identify emerging attack vectors and vulnerabilities, enabling organizations to fortify their defenses.

AI + SASE + XDR (access plus better visibility and compute to scrub massive amounts of data quickly) is the new equation for today and tomorrow."

Juliana Spofford

General Counsel and Chief Privacy Officer at Aidentified

Organizations of all sizes and across all industries are (or should be) prioritizing internal cybersecurity programs to implement proper security controls to protect personal, customer, and other confidential data sets within their systems. Governance, Risk & Compliance ("GRC") tools such as SOC 2 compliance software platforms (e.g., Vanta, Drata) are being used at a higher rate to help organizations enable customized security operations solutions and to assist them in achieving audited security attestations such as SOC 2 (System and Organization Controls 2).

These platforms assist with implementing and monitoring internal security programs with appropriate policies, security training, monitoring of devices, testing software vulnerabilities, vendor management, and more.

Generative AI usage policies are being adopted by organizations as more employees are using easily accessible generative AI tools, such as ChatGPT, often without an employer's knowledge. Sharing data with a generative AI tool increases the risk of company and customer intellectual property and private information being compromised, putting an organization's systems and data at risk.

Vladislav Bilay

DevOps at Aquiva Labs

1) Rising emphasis on securing the Internet of Things (IoT) devices and networks. As the number of connected devices continues to proliferate, ensuring their security becomes paramount.

2) Growing prominence of artificial intelligence (AI) and machine learning (ML) in cybersecurity. AI and ML technologies are being utilized to enhance threat detection, automate security operations, and improve incident response.

3) Increasing focus on proactive and preventive measures rather than reactive approaches.

Gopi Sirineni

President & CEO at Axiado

Innovations that promise to catch cyberhackers before they can attack are starting to enter the market, and a new breed of AI-driven hardware security processors are predicted to safeguard servers and networks through preemptive threat detection, robust root of trust (RoT) protection, and always-on monitoring, operating in secure isolation from the main CPUs and other processors.

For an industry that has sought for years to achieve the highest level of trust, AI combined with hardware may have delivered the most promising achievement yet. And it's doing so as the world adapts to 5G, the next-generation cellular wireless network that will drive more connectivity and necessitate greater security. We're already seeing the advantages of AI-based hardware for business leaders in the areas of customer relationship management, internet and data research, and digital personal assistants, just to name a few. These advantages in efficiency and performance are translating to improvements in cybersecurity measures in 2023 that will make businesses in our digital age more secure than ever.

Harman Singh

Managing Consultant | Director at Cyphere Ltd

1. Increased focus on cloud security: As more organizations adopt cloud services, securing cloud environments becomes paramount. Implementing robust access controls, encryption, and continuous monitoring will be crucial in safeguarding data stored in the cloud.

2. Emphasis on zero trust architecture: Traditional perimeter-based security is no longer sufficient. Zero trust architecture, which assumes that every user and device is a potential threat, will gain prominence. This approach requires continuous verification of user identities and device health before granting access to resources.

3. Rise of artificial intelligence (AI) in cybersecurity: AI-powered tools are becoming indispensable in detecting and responding to cyber threats. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies, enabling proactive threat detection and faster incident response.

4. Focus on securing the Internet of Things (IoT): With the proliferation of connected devices, securing the IoT ecosystem will be critical. Implementing strong authentication protocols, encryption, and regular updates to address vulnerabilities will help mitigate risks associated with IoT devices.

5. Growing importance of employee awareness: Cybersecurity is a shared responsibility. Organizations will invest more in training employees to recognize and respond to phishing attacks, social engineering attempts, and other common security threats.

To stay ahead, organizations should prioritize these trends and invest in robust cybersecurity measures, including regular risk assessments, implementing multi-factor authentication, and establishing incident response plans. Remember, proactive and layered security measures are key to mitigating cyber risks effectively. Stay vigilant, stay informed, and adapt to the evolving threat landscape.

Shri Ganeshram

CEO / Founder at Awning

1. AI and Machine Learning for Threat Detection: Artificial Intelligence is not just for Netflix recommendations anymore, huh? We're seeing the use of advanced machine learning algorithms to predict and identify cyber threats before they happen. We've moved from a reactive stance to a more proactive one. At Awning, we use AI to scan for vulnerabilities and it's incredibly effective. It's like hiring a digital Sherlock Holmes that works 24/7.

2. Zero Trust Architectures: The trust but verify mantra is kind of outdated now. Businesses are adopting a 'never trust, always verify' model. This means even if someone is inside your network, their activities still undergo scrutiny. It’s like those heist movies where even the members of the team keep tabs on each other to make sure no one goes rogue.

3. Supply Chain Attacks: This one's a bit scary. The hackers go for less secure elements in a supply chain to compromise the entire network. It’s sort of like if you're building a fortress, but the guy delivering your bricks is shady. If the bricks are compromised, so is your fortress.

Cybersecurity strategies are increasingly focusing on securing every node of the supply chain.

4. Cybersecurity Mesh: Traditional perimeters are fading fast, especially with remote work becoming ubiquitous. Cybersecurity mesh allows for defining a security perimeter around the identity of a person or thing. So instead of a single fence around your property, imagine an individual bubble around each family member and even the dog.

5. Blockchain for Security: Blockchain isn't just for cryptocurrency enthusiasts. Its applications in securing transactions and verifying identity are gaining traction. In essence, blockchain makes tampering very, very difficult.

6. Rise of Cyber Insurance: Much like you'd insure your car or property, businesses are now opting for cyber insurance to mitigate financial losses due to cyberattacks. It’s basically acknowledging that while you can have airbags and good brakes, you still need insurance for your vehicle.

7. Focus on the Human Factor: And let's not forget us, the humans. Increasingly, cybersecurity strategies are focusing on employee training because the most sophisticated software can't stop someone from clicking on a phishing link if they don’t know what to look out for.

Rahul Vij

Managing Director at WebSpero Solutions

One of the most significant trends will be the increased use of artificial intelligence and machine learning to detect and respond to cyber threats.

These technologies will enable us to analyze vast amounts of data in real time, identify patterns and anomalies, and respond quickly to potential threats.

Another trend we can expect to see is the growing importance of cloud security. With more and more businesses moving their operations to the cloud, it's essential to have robust security measures in place to protect sensitive data.

Finally, we can expect to see a continued focus on employee training and education. As cyber threats become more sophisticated, it's essential that every member of an organization understands how to identify potential threats and take appropriate action to prevent them.

Andrew Chen

Chief Product Officer at CommentSold

When it comes to protecting your business from cyberattacks, mobile devices will be a significant focal point in 2023 and beyond. If left unprotected, your phone can have direct access to sensitive files and documents accessible through your business email. Emails are also primary targets for viruses that spread harmful bugs that weaken the security of your devices, making you more prone to cyberattacks.

Businesses will look to prevent this by using a strengthened and cutting-edge operating system. Some specific security measures will be implemented to strengthen OS including firewall configurations, anti-virus checks, access controls, software updates, and updated frameworks. These measures are all easy to set up and as convenient as downloading protection software directly from an app, a downloaded file, or your phone's settings, so you can expect businesses to equip their devices with powerful operating systems for the foreseeable future.

Vincent Zhu

CEO and Founder of ShineACS Locks

By 2023, I believe that proactive security measures, such as micro-segmentation and artificial intelligence (AI), will become much more commonplace. As attackers continue to grow in sophistication, organizations must be equally as prepared to detect and respond to threats quickly.

I also anticipate that multi-factor authentication will be widely implemented to validate and secure user access.

Ranee Zhang

VP of Growth @ Airgram Inc

By 2023, I expect to see an increased use of cloud-based security solutions that can help organizations systemically improve their overall security posture.

Additionally, I anticipate that data security and privacy solutions will become more sophisticated to ensure the secure handling and storage of customer data.

Finally, I anticipate that endpoint and identity security will be at the forefront of many organizations' security strategies.

Rob May

Founder & MD ramsac

A clear and obvious cybersecurity trend from my perspective is the use of both artificial intelligence (AI) and managed learning (ML) which are increasingly pivotal in shaping cybersecurity strategies for both offense and defense.

On the defensive side, these technologies are employed for more sophisticated anomaly detection, automated incident response, and phishing detection. AI-enhanced Security Information and Event Management (SIEM) systems and User and Entity Behaviour Analytics (UEBA) are also emerging to refine threat identification and management.

From an offensive perspective, AI algorithms are capable of automating hacking attempts, crafting more effective social engineering attacks, and creating adaptive malware. There's also the concern of data poisoning to compromise ML models and the use of deepfakes for disinformation or impersonation.

However, the integration of AI and ML brings about ethical, legal, and technical challenges. Automated offensive capabilities could lead to misuse and unintended consequences, while the regulatory landscape is yet to catch up with these technological advances.

In essence, while AI and ML offer promising enhancements in cybersecurity, they also introduce new forms of risks and complexities, maintaining a dynamic tension between cybersecurity defense and offense.

Steve Feiner

Co-Founder & CEO at ABF Group

Cybersecurity is crucial in protecting networks and devices from threats, as cybercriminals evolve their attack methods and techniques based on technological advancements and the sophistication of security defenses.

The Internet of Things (IoT) has increased cybercrime risks with physical objects connecting to the Internet and data exchange. Artificial intelligence (AI) and machine learning have improved cybersecurity in face recognition, natural language processing, and automated security systems.

Cloud jacking involves illegally accessing a company's cloud infrastructure for profit or to launch attacks. Ransomware targets computer systems, encrypting files and demanding a ransom. Automotive hacking involves automated software in modern cars, requiring stringent cybersecurity precautions for self-driving vehicles and other complex systems.

Malware, or sophisticated software, infiltrates networks to steal data. Mobile phones replace traditional banking and shopping experiences, increasing malware attacks in e-commerce, banking, and online booking. Multi-factor authentication (MFA) is a security mechanism that requires multiple forms of authentication to access an account, enhancing protection against cyberattacks.

Gagan Deep Singh

Founder - Blocktech Brew

1. Attack against cloud services
2. Growing IT Skills Gap
3. Rise in IOT services
4. Integration of AI & machine learning
5. Zero trust cyber security
6. Multi-factor authentication
7. Organisational behaviour
8. International state-sponsored warfare
9. Increasing threat of deep fakes

Shanal Aggarwal

CCO at TechAhead

As the Chief Commercial Officer of TechAhead, I forecast significant cybersecurity developments for 2023. AI and machine learning will be increasingly integrated into security systems to proactively detect and battle risks in the information technology sector. The adoption of Zero Trust frameworks, which prioritize trust verification for all network parts will gain traction. Collaboration between corporations and government agencies will increase, leading to improved cybersecurity rules.

At TechAhead, we are devoted to disrupting traditional outsourcing by aligning with these trends, assuring the long-term prosperity and security of our customers and the digital ecosystem.

Vikas Kaushik

CEO at TechAhead

As CEO of TechAhead, a pioneer in IT, I've seen technology revolutionize our industry. Our operations depend on cybersecurity in today's fast-changing digital world, where innovation drives success. With over 24 years of expertise, I know how important cybersecurity leadership is. TechAhead's digital transformation solutions are driven by quality and client-centricity, including cyber protections.

IT cybersecurity is changing dramatically in 2023. As an industry thought leader, I stress the need to be current on trends and innovations. AI Time Journal's Cybersecurity Trends 2023 Ebook is a wonderful resource with professional perspectives like mine. We deploy cutting-edge tools, threat intelligence, and proactive techniques to secure our digital assets. This ebook provides a thorough examination of the evolving threat landscape to help industry leaders like us make decisions. In an age when technology drives growth, and cybersecurity leadership is strategic.

Cybersecurity is part of our digital development at TechAhead, not just a precaution. The insights in this ebook help us match our strategy with the newest trends and give secure and innovative solutions to our worldwide clients. We are shaping the future of IT by keeping resilient and proactive in the face of evolving cyber threats.

Youssef EL ACHAB

IT Consultant at EFS

In 2023, cybersecurity is poised to witness several noteworthy trends. One significant development is the increased emphasis on zero-trust security models. Organizations are shifting away from traditional perimeter-based defenses and adopting a never-trust, always-verify approach.

This means scrutinizing all network traffic, regardless of its source, and
verifying user identities and device integrity continuously. Google's BeyondCorp is a prime example of this approach, where access is granted based on device and user credentials, not network location.

Another trend is the rise of AI-driven threat detection and response. Machine learning algorithms are being employed to analyze vast amounts of data in real time, identifying anomalous patterns indicative of cyberattacks. Dark Trace's use of AI to autonomously respond to threats and Cisco's integration of AI into their cybersecurity solutions demonstrate this shift.

Furthermore, supply chain security is gaining prominence. With high-profile
incidents like the SolarWinds breach, organizations are increasingly scrutinizing their suppliers' cybersecurity practices. Collaborative efforts like the Charter of Trust by Siemens and its partners underscore the importance of ensuring security across the entire supply chain.

In summary, 2023 will see a focus on zero-trust models, AI-powered threat defense, and supply chain security as cybersecurity continues to evolve in response to an ever-changing threat landscape.

Matthew Ramirez

Entrepreneur and Investor at Reach Capital

I think the trend of cybersecurity threats becoming more frequent and severe will continue. Cyberattacks are becoming more sophisticated and widespread, which often results in massive data loss and damage to organizations. Cybercriminals are taking advantage of the growing complexity of today's IT infrastructures, increasing digital dependence, and people's lack of cybersecurity awareness.

I believe there will be a trend of higher employee cybersecurity awareness, which will help prevent data breaches. Employees are often the weakest link in cybersecurity defenses. They often don't take their cybersecurity responsibilities seriously and expose the company to cyberattacks. But this trend might change it.

A shift in employee cybersecurity culture will occur, which will be achieved through various training programs and education about the importance of cybersecurity for the company and themselves.

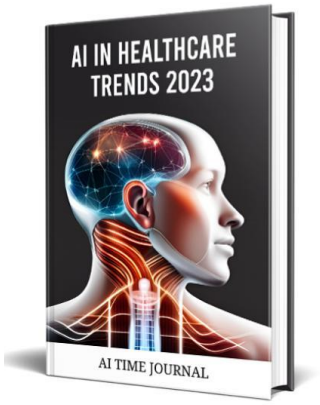
Isla Sibanda

Cybersecurity Specialist, Privacy Australia

As of last year, we had over 6.5 billion people using smartphones across the world. With such an exponential increase in the consumption of mobile devices, the avenues for hackers to attack have also increased. People use their smartphones for personal and business communication, shopping, banking, etc., leaving a lot of their private information vulnerable.

Even the applications that we download on our mobiles can place us at risk for malicious attacks to infiltrate our devices. Tech giants are expected to work more diligently towards protecting their customers from fraudulent transactions in the coming months.

Engage With Our Upcoming Ebooks!



Upcoming Ebooks

Cloud Computing Trends 2023

Digital Marketing Trends 2023

Software Development Trends 2023

AI in Healthcare Trends 2023

AI in Insurance Trends 2023

Get Involved

Thought Leaders:	Contribute Your Insights
Sponsors:	Become a Sponsor
Media Partners:	Become a Media Partner