Bluewave

Ntirety™

UNLOCKING THE FUTURE:

INSIGHTS ON CYBERSECURITY AND CLOUD IN 2024

AUTHORED BY EMIL SAYEGH, CEO AND PRESIDENT, NTIRETY

TABLE OF CONTENTS

INTRODUCTION

Welcome to *Unlocking the Future: Insights on Cybersecurity and Cloud in 2024*, a forward-looking exploration of the evolving realms of cybersecurity and cloud computing. In this eBook, we delve into the transformative developments of 2023, laying the groundwork for what we anticipate will be key trends, challenges, and opportunities in the upcoming year. Our journey traverses diverse landscapes—from emerging technologies and geopolitical shifts to regulatory landscapes and security challenges—offering insights and predictions vital for businesses, IT professionals, and policymakers alike.

As the digital world becomes increasingly complex and interconnected, understanding these trends is crucial for staying ahead of the curve. We'll explore how advancements in AI, quantum computing, and cloud technologies are reshaping the cybersecurity landscape. We'll also discuss the impact of political turmoil on cyber espionage and data protection, the evolving nature of regulatory compliance, and the critical role cloud-native security solutions play in modern business strategies.

Our aim is to provide a comprehensive overview of anticipated shifts in the cybersecurity and cloud domains, to equip you with the knowledge and strategies to navigate these changes successfully. Whether you're a seasoned IT professional, a business leader, or simply someone interested in the future of technology, this eBook is designed to offer valuable insights and actionable takeaways for a secure and innovative 2024.

Emil Sayegh, CEO, Ntirety

Emil Sayegh

REFLECTING ON 2023: LESSONS IN CYBERSECURITY

2023 marked a transformative journey for the increasingly-intertwined cybersecurity, IT, and cloud industries. Global cyberattacks spiked by over 40%, and emerging security and cloud technologies responded to address the risks. The cybersecurity landscape shifted as a result, with an increased focus on zero trust, AI, and cloud technologies. The year was also marked by increased investments in cybersecurity and new legislation to combat associated challenges.

EMERGING TECH

2023 brought transformations in emerging technologies, with some ramping up and others fading out. The metaverse fell short, failing to maintain its momentum due to economic downturns and a lack of forethinking about security implications. Focus instead surged to AI, bringing new use cases and cybersecurity concerns to the forefront. In a similar vein, breakthroughs in encryption unleashed potential for quantum computing, while simultaneously unveiling concerns about the vulnerability of existing cryptographic methods.

POLITICAL SHIFTS

The past year has witnessed significant geopolitical turmoil, profoundly impacting the cybersecurity landscape. This upheaval led to an intensification of cyber espionage, state-sponsored cyberattacks, sophisticated disinformation campaigns, and increasingly aggressive ransomware attacks. These developments underscore the deeply interconnected nature of our globalized world, highlighting how geopolitical events can have far-reaching effects on cybersecurity practices and policies.

For those interested in delving deeper into cyber espionage, our companion eBook, Unmasking the Shadows: A Guide to Notorious Hacker Groups and Strategies for Defense, offers an extensive exploration.

It provides in-depth analysis of the key players in cyber espionage, the evolution of state-sponsored cyber activities, and effective strategies to defend against these growing threats. This additional resource is designed to give you a more comprehensive understanding of how global politics intertwine with the realm of cybersecurity.

REGULATION AND COMPLIANCE

In 2023 the United States government unveiled a new plan to mitigate cybersecurity risks and boost investments, with an emphasis on public-private sector collaboration. The plan encompassed enhancing cyber incident reporting, updating response plans, tackling ransomware, and prioritizing software transparency. The Securities and Exchange Commission also revamped its rules on cyber risk management, governance, and incident disclosure, to address the growing centrality of cybersecurity in corporate compliance.

SECURITY CHALLENGES

Cyberattacks increasingly targeted data-intensive content such as streaming services, and in response companies prioritized robust security measures. Amid rising cyber threats and constrained budgets, the significance of automation and partnerships with cybersecurity service providers intensified. Perhaps one of the most significant challenges was in the financial sector, as crypto faced unprecedented turmoil, crashes, and high-profile attacks, surfacing the vulnerabilities existing within the crypto landscape.

See how an insurance company addressed increasing security challenges last year through their partnership with Ntirety.

READ CASE STUDY

LOOKING FORWARD TO 2024

All these instances underscored the importance of robust cybersecurity frameworks across industries, businesses, and technologies at large. As cybersecurity took center stage it was joined by cloud technologies, and the two became increasingly intertwined and interdependent. Reliance on cloud services surged, amplifying both the opportunities and risks for digital security. All in all, 2023 reinforced the need for a harmonized cybersecurity strategy that addresses the evolving landscape of cloud-based threats. As the world continues to move to the cloud, the intricate dance between safeguarding data and leveraging cloud efficiencies reinforces the imperative of an integrated and holistic cybersecurity approach.

ANTICIPATING CHALLENGES AND OPPORTUNITIES:

CYBERSECURITY AND CLOUD IN 2024

2023 was a momentous year, marked by remarkable progress and significant challenges in the worlds of cybersecurity and cloud. As we set our sights on 2024, the cybersecurity landscape is on the cusp of substantial transformations characterized by mounting complexity, evolving threats, and an increasing necessity for sophisticated and integrated security solutions. The dynamic realm of cloud computing is also on the brink of remarkable transformation, as organizations and service providers brace themselves for an era characterized by innovation, challenges, and opportunities.

We are positioned at the crossroads of unprecedented technological advancements and escalating cybersecurity challenges, and we must gear up for the journey ahead.

Here, we present overarching predictions for 2024 as they relate to **IT** and **technology**, **cybersecurity**, **AI**, and the **cloud**. These predictions reflect key trends set to mold the industry, and signal a new chapter in this ever-evolving landscape.

PREDICTIONS ON CYBERSECURITY THREATS

A variety of cybersecurity threats are on our radar for the upcoming year. Below are predictions on the attack vectors and threats we expect to intensify.

01 RISE IN RANSOMWARE

Ransomware attacks are expected to continue their upward trajectory in 2024, as cybercriminals target not only corporations but critical infrastructure and municipal services. The potential for disruption and financial loss remains significant.

02 AI-POWERED ATTACKS

Artificial intelligence (AI) and machine learning (ML) will play an increasingly prominent role in cyberattacks in 2024. Expect cybercriminals to leverage AI and ML to automate and enhance their capabilities through more sophisticated and adaptable attacks.

03 ELECTRIC VEHICLE HACKS

Most modern vehicles rely on numerous chips, computers, and remote connectivity. Because of this connectedness vulnerabilities are prevalent, and a catastrophic attack affecting fleets of electric vehicles, charging stations, or connected apps is a conceivable threat.

04 QUANTUM COMPUTING THREATS

Advancements in quantum computing will reshape the cybersecurity landscape in 2024. The immense computational power of quantum computers could break existing encryption algorithms, necessitating the development of new encryption and security measures.

05 SUPPLY CHAIN ATTACKS

Supply chain attacks will persist this year, as threat actors continue to compromise software and hardware providers in order to infiltrate their downstream targets. These attacks may have geopolitical roots and hold far-reaching consequences.

06 IOT VULNERABILITIES

The expanding Internet of Things (IoT) landscape will introduce new vulnerabilities in 2024, as connected devices continue to become integrated into our daily lives and critical infrastructure. Many IoT devices still lack adequate security measures, making them attractive targets for bad actors.

07 BIOMETRIC AUTHENTICATION CHALLENGES

Biometric authentication methods, such as fingerprint and facial recognition, are becoming increasingly prevalent. With their widespread adoption, attempts to bypass or compromise these systems are also expected to rise in the coming year.

PREDICTIONS ON TECHNOLOGIES

As we move into 2024, emerging and advancing technologies will continue to evolve at a rapid rate, bringing with them both great opportunities and difficult challenges.

01 ASCENDANCE OF SERVERLESS COMPUTING

The adoption of serverless computing will continue its upward trajectory in 2024. As serverless platforms and applications mature, businesses are poised to leverage them for building and deploying agile, cloud-native applications. Alongside this adoption, specialized serverless security tools and practices will emerge to safeguard against vulnerabilities.

02 INTEGRATION OF EDGE COMPUTING

The seamless integration of edge computing with cloud services will become a reality in 2024. This integration promises real-time data processing at the edge, which reduces latency for IoT applications and other latency-sensitive workloads. By offering these solutions, cloud providers will extend their reach to the edge of networks and unlock new use cases.

03 AI AS A CYBERSECURITY TOOL

The rapid advancement of AI will continue, and the same tools that equip attackers with new capabilities will also serve increasingly useful in cyber defenses. AI is poised to take on new heights as a tool in the fight against cybercrime.

04 DATA VELOCITY AND HYBRID INFRASTRUCTURES

The increasing velocity of data accumulation and movement across hybrid and multicloud infrastructures will pose significant security challenges in the year ahead.

05 RISE OF CONTAINER ORCHESTRATION

Container orchestration platforms, and notably Kubernetes, will maintain their growth and relevance in 2024. Critical to modern cloud-native architectures, these tools simplify the deployment and management of containerized applications and will render cloud development more efficient and scalable.

PREDICTIONS ON SECURITY SOLUTIONS

In response to evolving cyber threats, risks, and vulnerabilities, security solutions will evolve in 2024 to meet the conditions that arise.

01 STRICTER DATA PRIVACY REGULATIONS

Governments worldwide will continue implementing more stringent data privacy regulations in 2024, placing greater responsibility on organizations to secure customer and user data. Non-compliance will result in fines and reputational damage, not to mention financial losses. Regulations will no longer be confined to borders, and decisions in the EU will have far-reaching impacts.

02 EVOLVING REGULATORY COMPLIANCE

The regulatory landscape surrounding data privacy and security will continue to evolve - and become more intricate - in 2024. Cloud providers will enhance compliance services to assist organizations in navigating this complexity, and help them adhere to global data privacy regulations and mitigate risks.

03 CLOUD-NATIVE SECURITY SOLUTIONS

Innovative, cloud-native startups will increasingly offer simplified, software-driven security solutions tailored for the cloud. As organizations adopt these cloud-native applications and microservices, the industry will respond with security tools designed to address the unique challenges of cloud-native architectures and protect applications throughout their lifecycles.

04 AI-DRIVEN CLOUD RESOURCE OPTIMIZATION

AI and machine learning are poised to play an increasingly significant role in optimizing cloud resource management. AI-driven cloud management will transition from novelty to norm, and empower organizations to reduce costs, enhance performance, and streamline cloud operations. Machine learning algorithms will provide value by dynamically optimizing resource allocation, identifying cost-saving opportunities, and automating routine management tasks.

05 QUANTUM-SAFE CLOUD SECURITY MEASURES

Advancements in quantum computing are beginning to present a threat to existing encryption methods. In response, in 2024 cloud providers will introduce quantum-safe encryption and security measures to shield data from emerging quantum threats. Businesses will gain access to quantum-resistant cryptographic solutions, and fortify sensitive information in the cloud.

06 INCREASED ZERO TRUST ADOPTION

Zero Trust principles emphasize the verification of every user and device, regardless of location. Adoption of this security model is expected to expand in 2024, as organizations recognize the need to enhance network security and protect sensitive data in the era of remote work and distributed computing.

07 DEVSECOPS AS A NECESSITY

DevSecOps (development, security, and operations) practices will prove critical for the secure development and deployment of software, due to the growing diversity of APIs and applications creating a larger attack surface. Infrastructure, governance, and platform cohesiveness will be critical to success in these areas.

PREDICTIONS ON CLOUD EVOLUTION

Cloud computing is set for a significant shift this year, with many evolutions in the cloud and implementations on the horizon.

01 HYBRID AND MULTI-CLOUD EVOLUTION

The era of one-size-fits-all cloud solutions is giving way to a more tailored and dynamic approach. Hybrid and multi-cloud environments combining public and private cloud are set to redefine the paradigm and become the new normal. The approach will provide unparalleled flexibility, empower businesses to select the optimal cloud resources for specific workloads, ensure redundancy, and embrace vendor-agnostic solutions. Along with this shift will come novel challenges for IT departments, and tools will be needed to streamline complexities that arise from multi-cloud.

02 CLOUD SUSTAINABILITY INITIATIVES

Environmental considerations take center stage in 2024 as cloud providers invest in green technologies and advocate sustainable practices. Focused on reducing carbon footprints, cloud providers will implement eco-friendly data storage solutions and innovate to make data centers more energy-efficient in alignment with the values of socially-responsible organizations.

03 SKILLS GAP IN CLOUD EXPERTISE

The rapid migration to cloud services has accentuated a persistent skills gap, which will become prominent in 2024. The demand for system administrators, database administrators, AI experts, and software engineers well-versed in cloud computing is expected to intensify as cloud adoption accelerates and becomes more multifaceted.

TIPS & TAKEAWAYS:
LESSONS FOR 2024

From these predictions, we can glean a variety of cybersecurity tips and takeaways. These lessons will be essential as organizations of all sizes adapt to new technologies, shifts in the IT landscape, the adoption of cloud computing, and resulting effects on cybersecurity.

01 IMPLEMENT ROBUST SECURITY

Implementing strong cybersecurity measures can help protect against cyberattacks and vulnerabilities, including the ransomware, supply chain attacks, and IoT threats mentioned above. To reduce the chance of disruption and financial loss, organizations should prioritize robust backup solutions, employee training, and vulnerability assessments. Protections should also be put into place for new and emerging threats such as serverless computing, quantum computing, and biometric authentication. Organizations must adopt a proactive approach to detecting and mitigating potential cybersecurity threats, and implement comprehensive, full-stack security, with multiple layers.

02 EMBRACE THE CLOUD

The cloud revolution has fundamentally reshaped the trajectory of business operations, innovation, and technology. As the cloud computing landscape becomes more multifaceted and the trend towards multi-cloud environments continues, organizations must remain agile and adaptable. Embracing the cloud in a thoughtful manner will allow organizations to fully harness its power while effectively managing associated risks and complexities.

See how Ntirety provided strong cybersecurity for a communications company.

READ CASE STUDY

03 USE CAUTION WITH AI

A diligent and cautious approach is needed to apply AI effectively in cybersecurity and across industries. As always with AI, it's essential to balance unleashing the opportunities with maintaining an honest and careful handle on the risks. Cybersecurity professionals should also harness the power of AI to stay one step ahead of hackers who are doing the same.

04 STAY AHEAD OF REGULATIONS

Organizations must stay abreast of new and evolving regulatory compliance. Companies should invest in robust data protection mechanisms including encryption, access controls, and privacy-aware data management practices. Organizations may increasingly seek the support of outside providers when meeting these new regulatory demands.

See how Ntirety modernized a global non-profit's cloud-based identity and access management system.

READ CASE STUDY

Ntirety™

A PIVOTAL YEAR AHEAD

2024 promises to be a dynamic and transformative year for cybersecurity and cloud computing alike. As organizations navigate shifts in technologies, workflows, and security threats, it will be essential to remain agile, innovative, and adaptable. Staying informed about emerging threats and leveraging the latest security technologies is crucial. While there are many challenges ahead, there are also myriad opportunities for a successful path forward. We look forward to collectively working together towards a safer, more productive digital future.

THE IMPORTANCE OF PARTNERSHIP

In today's complex digital ecosystem where cybersecurity and cloud infrastructure are intertwined, Ntirety emerges as a pivotal ally. Their comprehensive range of services spans Data Management (essential for AI applications), Managed Private and Public Cloud Infrastructures, Managed Security Services, and Managed Compliance.

Ntirety's offerings are meticulously crafted to streamline and unify various facets of IT management, providing a singular point of accountability. This holistic approach integrates seamlessly into your business operations, ensuring a robust and proactive defense against cyber threats while maintaining compliance with evolving regulations. The breadth of Ntirety's services is particularly beneficial for mid-market clients, offering a tailored and scalable solution that addresses specific needs.

By partnering with Ntirety, organizations gain not only a shield against emerging cybersecurity risks, but an avenue for optimizing IT infrastructure in alignment with strategic objectives. We invite you to explore a partnership or request a demo to discover how Ntirety's comprehensive services can empower your organization to navigate the complexities of today's digital landscape with confidence and efficiency.

If you are interested in learning how Ntirety can help your IT organization with managed services around cloud infrastructure, security, compliance, or data administration, visit us at Ntirety.com.

CONTACT NTIRETY

ABOUT THE AUTHOR

Emil Sayegh is a renowned figure in the IT security industry, currently leading Ntirety as President and CEO. Under his stewardship, Ntirety has emerged as a trailblazer in both cloud and compliant security solutions, setting benchmarks for excellence and innovation in the field. Emil's deep expertise and visionary leadership have been instrumental in steering the company's growth and success since 2016.

Prior to his tenure at Ntirety, Emil held several key leadership roles including Chairman of the Board, CEO, and President at Codero Hosting. His extensive career also includes pivotal contributions to the expansion of cloud computing and hosting businesses at both HP and Rackspace, where his strategic initiatives left a lasting impact.

Beyond his executive roles, Emil is a respected thought leader and influencer in IT security. He regularly imparts his knowledge and perspectives in his Forbes columns and through his podcast, *The Cyber Hour*. His achievements include holding nine patents, showcasing his innovative spirit and technical acumen. Emil is also a sought-after international speaker and author, sharing his expertise on global stages and through various publications.

ABOUT NTIRETY

Ntirety is a leader in comprehensive managed services, partnering with organizations to modernize and secure today's complex IT environment. Ntirety's solutions span cloud infrastructure, cybersecurity, data, and compliance, connecting mission-critical data across highly secure, available, and resilient environments. For over 25 years, Ntirety has empowered organizations to reduce risk, increase agility, and optimize IT spend by combining full-stack technical expertise with practical, strategic guidance and a commitment to achieving desired business outcomes. Learn how Ntirety sets the standard for IT modernization at Ntirety.com.

Visit our Website at Ntirety.com

RELATED READING

1. Reflecting On The Evolution Of Cybersecurity In 2023, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/12/12/reflecting-on-the-evolution-of-cybersecurity-in-2023

2. AI In The Boardroom: The Inevitable Evolution Of Decision-Making, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/08/17/ai-in-the-boardroom-the-inevitable-evolution-of-decision-making/

3. The Art of CyberWar: Understanding Your Enemy, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/02/14/the-art-of-cyberwar-understanding-your-enemy

4. Balancing Transparency And Practicality Amidst CISA Call For Enhanced Cyber Incident Reporting, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/11/22/balancing-transparency-and-practicality-amidst-cisa-call-for-enhanced-cyber-incident-reporting

5. Why Companies Are Struggling With Cybersecurity: Big Players In Bad Situations, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/09/19/why-companies-are-struggling-with-cybersecurity-big-players-in-bad-situations/

6. Ready for Cyber Readiness - Any Time Now, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/10/17/ready-for-cyber-readinessany-time-now/

7. Under Siege: Cybersecurity Failures Sound the Alarm, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/10/31/under-siege-cybersecurity-failures-sound-the-alarm

8. How Cloud Computing Revolutionized Business Operations And What Lies Ahead, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/11/28/how-cloud-computing-revolutionized-business-operations-and-what-lies-ahead/

9. Almost Human: The Threat Of AI-Powered Phishing Attacks, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks/

10. Impact of the IoT Trust Mark on Cybersecurity in the United States, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/09/27/impact-of-the-iot-trust-mark-on-cybersecurity-in-the-united-states/

11. Staying Ahead Of The AI Curve: The Imperative Of Prudent Planning, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/12/05/staying-ahead-of-the-ai-curve-the-imperative-of-prudent-planning

12. The Evolving Cloud Landscape: How Private Clouds Are Reshaping the Tech Industry, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/11/07/the-evolving-cloud-landscape-how-private-clouds-are-reshaping-the-tech-industry/

13. Artificial Intelligence and Clouds: A Complex Relationship of Collaboration and Concern, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/08/23/artificial-intelligence-and-clouds-a-complex-relationship-of-collaboration-and-concern/

14. Navigating Multicloud Realities: Practical Approaches For Success, *Forbes*, https://www.forbes.com/sites/emilsayegh/2023/09/07/navigating-multicloud-realities-practical-approaches-for-success/

15. Forbes Contributor - Cybersecurity: Emil Sayegh, *Forbes*, https://www.forbes.com/sites/emilsayegh/

16. The Cyber Hour Podcast, Ntirety.com, https://www.ntirety.com/podcast/

At Bluewave Technology Group, we take the complexity out of optimizing and modernizing technology. As your advisory and sourcing partner, we streamline how businesses acquire cloud, network, and communications solutions. Our goal is to help our clients boost revenue, cut costs, and enhance efficiency. With our Assess, Advise, and Advocate approach, we craft the perfect strategy and implement the right solutions. Our dedicated team of account managers, solution advisors, and technical analysts ensures positive business impact through successful results.

Ntirety is a leader in comprehensive managed services, partnering with organizations to modernize and secure today's complex IT environment. Ntirety's solutions span cloud infrastructure, cybersecurity, data, and compliance, connecting mission-critical data across highly secure, available, and resilient environments. For over 25 years, Ntirety has empowered organizations to reduce risk, increase agility, and optimize IT spend by combining full-stack technical expertise with practical, strategic guidance and a commitment to achieving desired business outcomes. Learn how Ntirety sets the standard for IT modernization at Ntirety.com.

© 2024 Ntirety, Inc. All Rights Reserved. Ntirety is registered trademark of Ntirety, Inc.
All trademarks, logos and brand names are the property of their respective owners.

www.bluewave.net | inquiries@bluewave.net | 800-962-7752