AMERICAN
TECHNOLOGY
SERVICES

Cybersecurity 2024

Strategic Insights for the Evolving Digital Security Environment

FAIRFAX

2751 Prosperity Ave
Suite 600
Fairfax, VA 22031

NEW YORK

250 Broadway
Suite 610
New York, NY 10007

ATLANTA

4360 Chamblee
Dunwoody Rd, Suite
517 Atlanta, GA 30341

CONTACT

(703) 876-0300
info@networkats.com
networkats.com

Table of Content

Executive Overview 3

Emerging Cybersecurity Trends 4

Cyber Risk Management as a Business Enabler 6

Innovation in Cybersecurity 7

Empowering Cybersecurity Excellence through Talent Development 10

Dealing with Sophisticated Cyber Attacks 11

Incident Response and Impact 13

Ensuring Comprehensive Compliance 15

Enhancing Cybersecurity Through Strategic Collaborations 16

Looking Ahead: Cybersecurity in the Future 18

Conclusion 19

Appendices 20

Executive Overview

Entering 2024, the cybersecurity sphere is at a critical crossroads, with digital security challenges becoming increasingly complex and multifaceted. This report thoroughly examines the latest trends, technological innovations, and strategic approaches essential for navigating these challenges. Aimed at equipping organizations with deep insights and practical strategies, we focused on evolving security practices to maintain pace with the dynamic digital security environment.

We dissect a range of cyber threats that are of immediate concern to businesses, including advanced phishing operations, malware, and the security implications of emerging technologies. We spotlight the role of artificial intelligence (AI) and machine learning (ML) in enhancing threat detection and response mechanisms, demonstrating their significance in developing more sophisticated cybersecurity solutions.

The evolving regulatory framework also receives attention, with an analysis of essential compliance requirements and their impact on business operations. The report encourages a proactive approach to cybersecurity, emphasizing the need for organizations to adapt their strategies to address current risks and anticipate future challenges.

This report offers a precise blend of current knowledge and practical guidance to support informed decision-making and strategic planning. It aims to prepare organizations to effectively secure their digital assets and maintain operational resilience in the face of the continuously evolving cybersecurity landscape.

ATS' approach is rooted in the understanding that healthy security measures should act as facilitators of progress, not barriers.

By coordinating our cybersecurity efforts with our strategic objectives, we reinforce that our commitment to security complements our ambition for innovation.

Emerging Cybersecurity Trends

The cybersecurity landscape in 2024 navigates an intricate web of evolving threats, demanding innovative defenses and strategic foresight. This section explores the key trends shaping this shift, offering insights into how organizations can bolster their defenses in response to these fast-paced advancements.

Advancements in Threat Landscape

The sophistication of cyber threats continues to escalate, with adversaries deploying increasingly advanced techniques to breach security measures. AI-driven attacks are on the rise, utilizing artificial intelligence to automate and optimize phishing schemes, malware propagation, and ransomware attacks. These AI capabilities enable threats to evolve rapidly, outpacing traditional security measures and demanding a more dynamic defense strategy.

The Rise of Zero Trust Architectures

In response to the evolving threat landscape, the adoption of Zero Trust architectures has become a cornerstone of modern cybersecurity strategies. Zero Trust operates on the principle that no entity, internal or external, should be trusted by default. This framework requires continuous verification of all access requests, regardless of their origin, significantly reducing the attack surface and mitigating the risk of breaches.

Supply Chain Security

The security of supply chain operations has emerged as a critical concern, spotlighting the interconnected nature of modern business ecosystems. Cyber adversaries increasingly target vulnerable points in the supply chain to exploit and launch widespread attacks. Robust security measures, including thorough vetting of third-party vendors and implementation of secure communication channels, are essential to safeguard against these threats.

Emerging Cybersecurity Trends

Regulatory and Compliance Evolution

The evolving landscape of regulatory compliance reveals a pivotal shift in the digital age: achieving compliance is increasingly seen not merely as a checklist or an end goal but as a natural outcome of a steadfast commitment to cybersecurity excellence. This perspective is important for understanding the transformative power of frameworks like the NIST Cybersecurity Framework 2.0. With its latest enhancements, including the critical 'Govern' function, the Framework sets up a governance-centric approach that inherently aligns with an organization's broader objectives.

By adopting a security-first mindset, organizations inherently lay the groundwork for meeting and surpassing regulatory standards. This approach ensures that compliance becomes a byproduct of a culture that prioritizes security, where the rigorous application of Zero Trust principles, comprehensive supply chain protections, and adaptive measures to evolving threats naturally guide organizations to exceed regulatory expectations.

As we navigate the complexities of this digital era, it's crucial to recognize that the strongest defense against the myriad of cybersecurity challenges lies in the proactive embedding of security into every layer of organizational strategy. This not only fosters resilience against sophisticated threats but also seamlessly achieves compliance, marking a strategic evolution from reactive adherence to a proactive and integrated security posture.

Cyber Risk Management as a Business Enabler

Cyber risk management emerges as a cornerstone, enabling businesses to navigate the complex cyber threat landscape effectively. This approach transcends traditional threat mitigation, evolving into a comprehensive framework harmonizing cybersecurity efforts with key business objectives. By leveraging advanced risk management frameworks, organizations can ensure that their cybersecurity strategies not only respond to current threats but also anticipate future challenges, thereby supporting business agility and innovation.

The process begins with meticulously identifying and assessing potential risks that could impact digital assets and operations. This assessment isn't a static, one-off exercise but a dynamic, ongoing process that adapts to the evolving cyber threat environment and business dynamics. The insights gained from this process inform the development of tailored cybersecurity policies, controls, and procedures. These measures are designed to protect, enable, and accelerate business initiatives, ensuring that security considerations enhance rather than hinder new digital service offerings and operational innovations.

Integrating risk management strategies across the organizational culture promotes heightened security awareness and proactive engagement with potential risks. This integration empowers all organizational tiers, from executive leadership to operational staff, to make informed decisions that align with immediate security needs and long-term strategic goals.

Cyber risk management in cybersecurity is about forging a symbiotic relationship between security practices and business growth. It's about creating an operational ethos where security measures act as enablers of innovation, driving forward not just the safety but the organization's success in the digital ecosystem. As we move into 2024, embracing this balanced, forward-looking approach to cybersecurity will be key for organizations aiming to thrive amidst the complexities of the modern technological landscape.

Innovation in Cybersecurity

AI and Machine Learning: Enhancing Cyber Defenses

Integrating Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity represents a pivotal advancement. These technologies are improving defenses by overcoming data shortages and enhancing threat detection accuracy. Large Language Models (LLMs), in particular, have shown promise in gathering and synthesizing data to build new detection mechanisms. Moreover, they facilitate SOC automation by translating natural language instructions into actionable API calls, streamlining operations and incident responses. Utilizing AI and ML is critical in managing the vast amounts of data within cybersecurity operations and making more informed decisions rapidly.

Processes and Culture

In this era of digital ubiquity, fostering a culture of security awareness and proactive risk management has become indispensable for maintaining operational excellence and safeguarding long-term business success. Organizations that excel view cybersecurity not as a standalone function or a necessary evil but as a fundamental component of their business strategy. This integrated approach ensures that cybersecurity considerations are woven into every facet of the business from the ground up, influencing everything from product development to customer service, supply chain management, and beyond.

A key aspect of cultivating such a culture is all employees' continuous education and empowerment. In 2024, businesses that lead the charge in cybersecurity recognize every team member, regardless of their role, as a vital link in the security chain. Through regular training sessions, simulations, and awareness programs, these businesses ensure that their workforce is aware of the latest cybersecurity threats and best practices and equipped to act as the first line of defense.

Blockchain for Enhanced Security

Blockchain technology is increasingly recognized for its potential to bolster cybersecurity measures. Its decentralized nature offers a new layer of security by enhancing data integrity and transparency, making it significantly more challenging for unauthorized changes to go unnoticed. While specific applications within cybersecurity are still being explored, the technology's ability to secure transactions and verify the authenticity of data without centralized authority marks a significant step forward in protecting digital assets and sensitive information.

Innovation in Cybersecurity

Cloud Security Developments

The evolution of cloud security has become integral to modern cybersecurity strategies, responding to the expansion of cloud computing and its associated risks. Innovations in cloud security aim to protect data, applications, and infrastructure from new threats. Enhanced encryption methods, identity and access management improvements, and advanced threat detection capabilities are among the key focus areas. These developments ensure that as organizations leverage the scalability and efficiency of cloud computing, they can also maintain robust security postures to protect against breaches and unauthorized access.

In 2024, the cybersecurity landscape is characterized by rapid advancements and shifting paradigms, underscored by AI's dual role in facilitating and defending against cyber threats. As organizations navigate this complex environment, staying informed about and adopting these innovations is crucial for maintaining robust cybersecurity defenses and ensuring compliance amidst evolving regulations.

Evolving Product and Technology Trends in Cybersecurity

2024 has witnessed a transformative leap in cybersecurity strategies, primarily through the accelerated adoption of Artificial Intelligence (AI). This year, AI has significantly enhanced the capabilities of cybersecurity solutions, marking a pivotal shift towards more intelligent and responsive defense mechanisms. The integration of AI has revolutionized threat detection by employing advanced algorithms to analyze patterns and predict potential breaches with a level of accuracy previously unattainable.

AI-driven response mechanisms have introduced a new era of cybersecurity agility. These systems autonomously address vulnerabilities and respond to threats in real time, drastically reducing the potential impact on organizational infrastructures. The specific advancements of 2024 highlight the evolution of cybersecurity technologies and emphasize a broader commitment within the industry to leverage AI for creating safer, more resilient online environments.

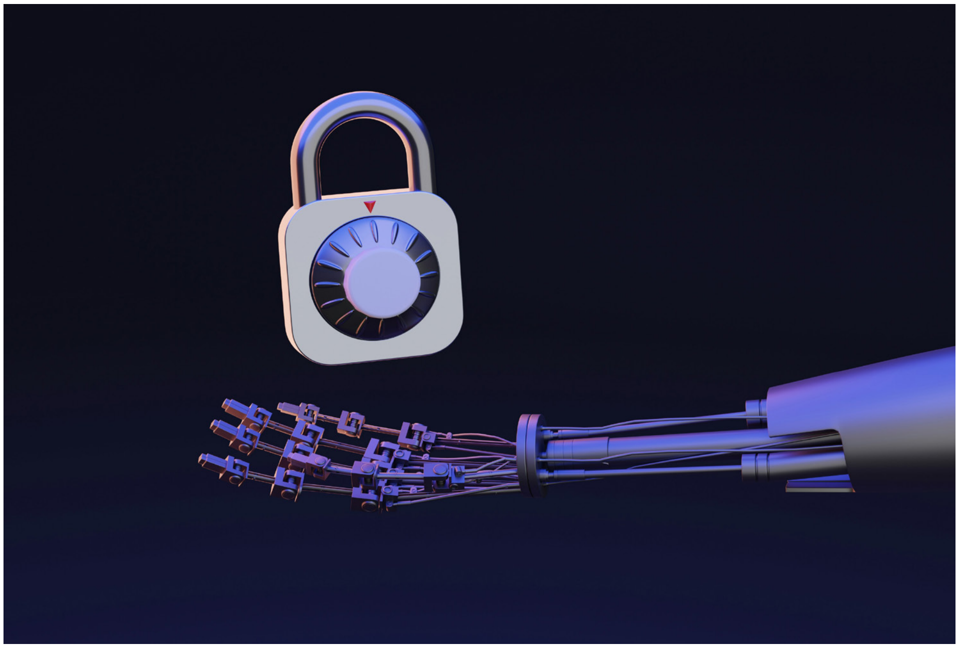
Innovation in Cybersecurity

Generative AI

Generative AI models have the ability to simulate potential cyber attack scenarios, analyze vast datasets for suspicious patterns, and predict future threats with a high degree of accuracy. This has enabled businesses to adopt a more proactive stance in their cybersecurity measures, staying ahead of threats.

However, the adoption of generative AI in cybersecurity is not without its challenges. As these AI models become more sophisticated, ensuring their security becomes increasingly complex. The very technology designed to protect digital assets can also become a target for cyberattacks, necessitating advanced protective measures to safeguard AI systems from manipulation or exploitation.

Businesses are navigating this emerging landscape by investing in secure AI development practices, emphasizing transparency, and ethical AI use. They also foster collaborations with AI security experts and researchers to bolster their defenses against potential AI-driven threats. As we move forward, the intersection of generative AI and cybersecurity remains a dynamic field, promising significant advancements in digital security and presenting new challenges to address.



Empowering Cybersecurity Excellence through Talent Development

The people factor—our collective talent pool—ultimately activates our cybersecurity defenses.

However, a persistent challenge within this domain is the cybersecurity skills gap, which calls for strategic foresight and innovative solutions. Addressing this gap head-on, the industry has pivoted towards a multifaceted approach to talent development, a critical endeavor to empower cybersecurity excellence.

Implementing comprehensive internal training programs is one of the most effective strategies for bridging this skills gap. These initiatives are designed not just to enhance the existing skill sets of our workforce but to foster a culture of continuous learning and adaptability. By leveraging the latest in educational technology, these programs offer personalized learning paths that cater to the diverse needs of employees, ensuring that everyone, from the tech novice to the seasoned professional, can elevate their cybersecurity acumen.

Recognizing the importance of a pipeline that continuously feeds fresh talent into the cybersecurity ecosystem, businesses have created symbiotic partnerships with educational institutions. These collaborations range from offering co-op and internship programs that provide hands-on experience to students, to advising on curriculum development that aligns with the real-world demands of the cybersecurity field. Such initiatives ensure a steady influx of trained professionals into the industry and strengthen the ties between academia and the practical, ever-evolving needs of the cybersecurity sector.

Another innovative approach to talent development has been the creation of upskilling programs aimed at transitioning existing employees into cybersecurity roles. Acknowledging that talent can come from within, these programs identify potential candidates from various departments, equipping them with the necessary skills to pivot into cybersecurity positions. This not only helps in mitigating the skills shortage but also offers a pathway for career development to employees, enhancing job satisfaction and loyalty.

Through internal training, partnerships with educational institutions, and upskilling programs, we not only close the skills gap but also pave the way for a future where cybersecurity excellence is not just an aspiration but a reality.

Leveraging AI-driven platforms to simulate real-world cybersecurity scenarios significantly augments traditional education methods by providing practical, hands-on experience. This integration of technology into training programs accelerates skill acquisition and deepens understanding of cybersecurity challenges, preparing professionals with the competencies required to navigate and mitigate the complexities of the cyber landscape effectively. Such an approach not only addresses the skills gap but also equips our workforce with the necessary tools and knowledge to confront future cybersecurity challenges with confidence and precision.

Dealing with Sophisticated Cyber Attacks

As the digital world evolves, so too do the threats that target our systems and data. In 2024, the sophistication of these threats has reached unprecedented levels, demanding equally sophisticated defenses. Here's how businesses are rising to the challenge:

Enhancing Detection and Response

The foundation of our defense against cyber threats is the expertise and quick action of dedicated incident response teams. These professionals stand at the forefront, ready to tackle and neutralize threats, ensuring minimal disruption to our operations. Their strategic importance is further enhanced by the latest technological tools, including AI and ML algorithms, which provide indispensable support in detecting threats with greater speed and accuracy. This dual strategy advances human expertise while leveraging technology to extend defensive capabilities further.

Adopting Comprehensive Security Frameworks

Adopting structured and comprehensive security frameworks is crucial in response to the complexity of modern cyber threats. These frameworks provide a blueprint for managing cybersecurity risks, focusing on continuous improvement and adaptation to the changing threat landscape.

Dealing with Sophisticated Cyber Attacks

NIST Cybersecurity Framework 2.0: A Paradigm for Resilience

The introduction of NIST Cybersecurity Framework 2.0 marks a significant evolution in our approach to cybersecurity, particularly with the strategic addition of the 'Govern' function. This enhancement not only broadens the framework's applicability but also deepens its impact across various industries by emphasizing the crucial role of governance in cybersecurity. The 'Govern' function integrates seamlessly with the foundational pillars—Identify, Protect, Detect, Respond, and Recover—underscoring the importance of aligning cybersecurity initiatives with an organization's broader business objectives and risk management strategies.

Key elements of the 'Govern' function include:

- **Organizational Context and Risk Management Strategy:** Tailoring cybersecurity measures to the organization's mission, values, and risk tolerance, ensuring strategies are practical and aligned with business goals.

- **Policies, Procedures, and Roles:** Establish comprehensive policies and procedures to support the cybersecurity framework and clearly define roles and responsibilities to enhance accountability and collaboration.

This forward-thinking update to the NIST Framework underscores the necessity of a holistic, governance-focused approach in today's complex cyber environment. By adopting NIST 2.0, organizations can ensure their cybersecurity practices are strong and strategically integrated with their operational objectives, facilitating a more resilient and responsive security posture.

Regular System Updates and Patch Management

An often overlooked but critical aspect of cybersecurity defense is the maintenance of system integrity through regular updates and patch management. In the face of sophisticated cyber threats, keeping systems updated with the latest patches is essential. These updates address known vulnerabilities that attackers could exploit, forming a fundamental part of a proactive cybersecurity strategy.

Incident Response and Impact

The necessity for readiness and proficient incident management to mitigate cybersecurity threats is crucial. An effective response can significantly limit both immediate and long-term damage to an organization.

Common Cybersecurity Incidents

Cybersecurity incidents like data breaches, ransomware attacks, and DDoS attacks profoundly impact business operations and reputation. These incidents disrupt services and can lead to substantial financial losses and regulatory penalties.

Effective Incident Response Strategies

Developing a vigorous incident response plan involves multiple steps:

- **Preparation** involves creating a detailed incident response plan, defining the incident response team's roles and responsibilities, and ensuring the team is well-equipped and trained.
- **Detection and Analysis** are crucial for identifying signs of a cybersecurity incident, analyzing them to confirm a genuine threat, and then documenting and prioritizing the incident.
- **Containment, Eradication, and Recovery** focus on stopping the incident from causing further damage, removing the threat, and restoring systems to normal operations. This stage requires careful planning to balance the need for quick action with the preservation of evidence for further analysis or legal requirements.
- **Post-incident Activity** involves learning from the incident to improve future response efforts. This could include reviewing the incident handling process, updating the incident response plan based on lessons learned, and communicating with all stakeholders about the incident and the organization's response.

Incident Response and Impact

Tools and Technologies

Utilizing the right tools for incident detection, analysis, and recovery is vital. This includes security information and event management (SIEM) systems for monitoring and alerts, as well as tools for threat intelligence, forensic analysis, and automated incident response.

Proactive Incident Management

Highlighting the importance of adaptability and resilience in reducing the impact of cybersecurity incidents on business operations is essential. A well-prepared and responsive organization can not only withstand cyber threats but also emerge stronger and more secure.

This section aims to ensure that readers understand the critical importance of an organized and efficient incident response capability. Integrating these insights into the report underlines the organization's commitment to cybersecurity and its capacity to protect its clients' interests in the evolving digital landscape.

Ensuring Comprehensive Compliance

Staying ahead of regulatory changes is crucial for maintaining not just legal compliance, but also for safeguarding data and trust. Strategies include:

- **Proactive Monitoring of Regulatory Developments:** Keeping up with changes in laws and standards affecting cybersecurity practices is essential. This includes familiarizing oneself with frameworks and regulations pertinent to the U.S. market.

- **Conducting Regular Audits:** Periodic assessments of cybersecurity practices against compliance requirements can identify gaps and areas for improvement, ensuring that organizations remain compliant over time.

- **Embedding Compliance into Cybersecurity Strategy:** Compliance should not be an afterthought but a key consideration in developing cybersecurity strategies. This ensures that security measures protect against threats and align with regulatory requirements.

In conclusion, tackling the challenges presented by the cybersecurity skills gap, sophisticated cyber threats, and the evolving regulatory environment requires a multifaceted approach. Organizations can successfully navigate these challenges by investing in talent development, leveraging cutting-edge technologies for threat detection and response, and ensuring compliance is woven into the fabric of cybersecurity strategies.

Enhancing Cybersecurity Through Strategic Collaborations

Strategic Collaborations for Advanced Defense

The complexity of cybersecurity threats in 2024 necessitates a collaborative approach to defense. Strategic alliances with cybersecurity innovators and technology service providers have become essential. These partnerships enable the integration of external expertise with in-house security operations, fostering a comprehensive security architecture. By uniting the strengths and resources of diverse entities, organizations can develop more resilient defenses capable of countering sophisticated cyber threats. This collaborative model amplifies defensive capabilities and enhances organizations' overall resilience against digital adversaries.

Intelligence and Resource Sharing for Security Optimization

Effective cybersecurity in an interconnected digital world is influenced by the organizations' ability to acquire and utilize their own threat intelligence and collaborate with external partners for additional insights. This dual approach is essential for a comprehensive understanding of the cyber threat landscape, especially for identifying specific risks such as compromised employee credentials, leaked customer data, or proprietary information available on the dark web.

Gathering internal threat intelligence involves deploying sophisticated tools and methodologies to monitor and analyze potential threats within an organization's own network and digital assets. This should be complemented by external threat intelligence from specialized providers, which offers broader visibility into emerging threats and cybercriminal tactics.

Sharing intelligence and resources between organizations and strategic partners enhances the collective cybersecurity posture. It enables proactive defenses and a state of readiness to respond to incidents more effectively. By pooling capabilities and information, organizations can develop a more dynamic and resilient security infrastructure, capable of adapting quickly to new challenges and threats.

The importance is not only reacting to known threats but also anticipating potential vulnerabilities and exposures. Organizations equipped with comprehensive threat intelligence, both internal and externally sourced, are better positioned to protect their digital assets and respond decisively to cyber incidents.

Enhancing Cybersecurity Through Strategic Collaborations

Compliance and Governance through Collaborative Frameworks

Navigating the dynamic and often complex regulatory landscape requires a concerted effort. Strategic collaborations are crucial in ensuring compliance with evolving standards and regulations. By leveraging shared governance models and compliance frameworks, organizations can benefit from collective expertise and insights, simplifying the compliance process. These partnerships often result in implementing best practices and innovative solutions that exceed basic compliance requirements, thereby strengthening the security posture. Success stories from these collaborations highlight significant enhancements in security measures and achievements in surpassing compliance goals, showcasing the tangible benefits of strategic partnerships in the cybersecurity domain.

The modern cybersecurity landscape demands a collaborative and strategic approach to defense, intelligence sharing, and compliance. By forging considered partnerships, organizations can leverage collective expertise, optimize their security operations, and navigate the complexities of compliance more effectively, setting a new standard for cybersecurity excellence in the digital age.

Looking Ahead: Cybersecurity in the Future

Preparing for Tomorrow’s Cyber Threats

As we look past 2024, the cybersecurity environment is set to confront an array of sophisticated challenges. Key trends indicate a surge in generative AI’s role in cybersecurity, offering new methodologies for threat detection and analysis but also presenting unique vulnerabilities that malicious actors may exploit. Simultaneously, the expansion of remote workforces and mobile device usage continues to redefine traditional security perimeters, emphasizing the need for stronger security protocols adaptable to these evolving environments. Moreover, the omnipresence of IoT devices and the accelerated shift towards cloud computing necessitate advanced strategies for safeguarding interconnected ecosystems against breaches and ensuring compliance amidst this digital transformation.

The Unspoken Advantage

In the dynamic field of cybersecurity, ATS stands out with exceptional expertise, adeptly integrating advanced technologies such as generative AI, cloud security, and IoT protection. Our profound knowledge and strategic approaches establish us as a central partner for organizations seeking to enhance their digital security posture. The advantage ATS offers lies in its commitment to innovation, adaptability, and a proactive stance towards emerging threats and regulatory requirements, ensuring clients not only withstand but thrive amidst the cybersecurity challenges of tomorrow.

These insights into the anticipated cybersecurity trends highlight the importance of adopting a forward-looking, proactive preparation strategy. As organizations prepare to face these future threats, partnering with entities with a profound understanding of cybersecurity and the capability to deliver adaptive solutions will be necessary.

Conclusion

As we conclude our exploration into the cybersecurity landscape of 2024, it's evident that the digital sphere is becoming increasingly complex and risky. The advancements in technology that drive our society forward also propel the sophistication of threats we face. This dynamic emphasizes the importance of businesses adopting a forward-thinking cybersecurity strategy, one that is not reactive but anticipatory, not isolated but integrated, and not static but evolutionary.

Embracing such a strategy requires staying informed about the latest trends, innovations, and regulatory developments. The emergence of AI in cybersecurity, the shift towards cloud-based infrastructures, and the persistent threat posed by state-sponsored cyber activities are but a glimpse of what the future holds. These developments are not just technological challenges; they are business imperatives that require strategic attention and action.

Moreover, the role of strategic partnerships in navigating this landscape cannot be overstated. Collaborations with entities that possess deep expertise and the ability to deliver adaptive, innovative solutions are invaluable. As demonstrated throughout this report, partnering with knowledgeable and capable entities provides an unspoken advantage—a partnership that not only secures your digital assets but also empowers your organization to thrive in the face of cybersecurity challenges.

Therefore, we call upon businesses to proactively engage with the future of cybersecurity. By staying up-to-date on developments, investing in innovation, and forging strategic collaborations, organizations can safeguard their digital landscapes and secure their place in the rapidly evolving digital future.

In closing, the journey through the cybersecurity landscape of 2024 and beyond is one of constant vigilance, strategic foresight, and collaborative strength.

Let this report serve as a guide and a call to action for all who navigate this terrain, inspiring informed decisions, and proactive measures to ensure a secure digital world.

Appendices

Appendix A: Glossary of Key Terms

AI and Machine Learning: Technologies that enable computers to learn from data and perform tasks that typically require human intelligence. In cybersecurity, these are used for threat detection and response.

Zero Trust Architecture: A security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are within or outside the network perimeter.

Blockchain: A decentralized ledger of all transactions across a network. Used in cybersecurity to enhance the integrity and security of data.

Cloud Security: Policies, controls, procedures, and technologies that protect cloud-based systems, data, and infrastructure.

IoT (Internet of Things): The network of physical objects—devices, vehicles, appliances—that use sensors and APIs to connect and exchange data over the Internet. IoT security focuses on protecting these devices and their data from unauthorized access and attacks.

Appendix B: Further Reading

Strategic Approaches to Zero Trust Implementation: Offers guidance on adopting Zero Trust architectures to improve security posture.

NIST Cybersecurity Framework 2.0: An updated framework developed by the National Institute of Standards and Technology to help organizations better understand, manage, and reduce their cybersecurity risks.

Securing the Cloud: Best Practices for Cloud Security: A guide to securing cloud environments against potential threats.

AMERICAN
TECHNOLOGY
SERVICES

FAIRFAX

2751 Prosperity Ave
Suite 600
Fairfax, VA 22031

NEW YORK

250 Broadway
Suite 610
New York, NY 10007

ATLANTA

4360 Chamblee
Dunwoody Rd, Suite
517 Atlanta, GA 30341

CONTACT

(703) 876-0300
info@networkats.com
networkats.com