2024

Cybersecurity Pulse Report

From AI to Zero Trust: A Comprehensive Guide to The Key Themes and Expert Opinions from This Year's RSA Conference

ISMG | CYBER THEORY

Table of Contents

Introduction

Welcome to ISMG's Inaugural Cybersecurity Pulse Report.

Each year, the RSA Conference leverages the collective expertise of more than 80 of the world's top security professionals, technology experts, researchers, government employees, attorneys, and scientists to review all submissions and make speaking selections based on the quality of submissions and balance of topics desired to be covered. This year, more than 450 sessions were presented.

In conjunction with those speaking sessions, ISMG editors, working with our broadcast studio, spent four intensive days interviewing more than 150 industry executives, practitioners, and thought leaders from the top cybersecurity vendors, investment firms, government agencies, and the world's largest private companies. This report is the result of those interviews and is guided by the work of the RSA Program Committee.

450+

SESSIONS

How did we organize the report?

The ISMG Thought Leadership Content Lab leveraged multiple AI platforms utilizing Retrieval Augmented Generation (RAG) to categorize and classify the 450+ RSA sessions into 13 high-level themes. We then categorized and classified the insights extracted from more than 550 pages of ISMG interview transcripts into one or more of the 13 high-level RSA themes.

The result is a blueprint covering the most pressing issues and emerging trends in cybersecurity, directly informed by the top minds in the industry. This report will be an essential resource for the upcoming year in planning, investment, and operational effectiveness.

Thank you for joining us on this journey. We look forward to continuing to provide unparalleled insights and thought leadership to support your cybersecurity efforts.

Sincerely,

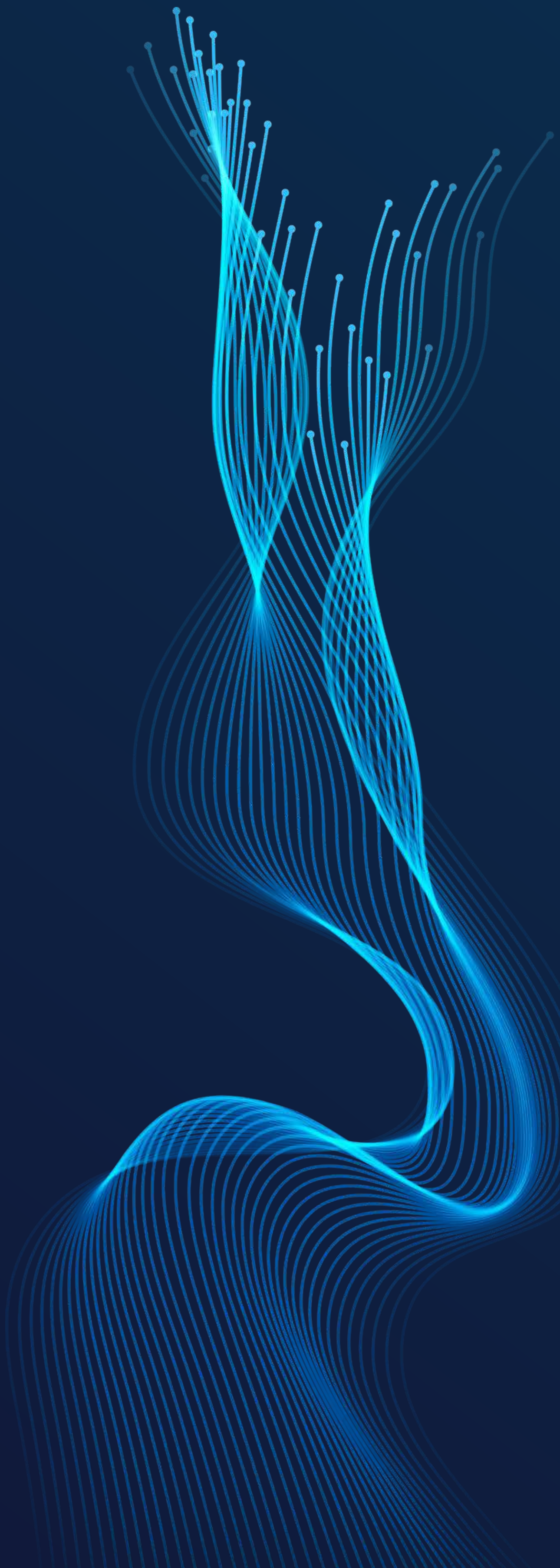
Daniel Verton

Dan Verton
Vice President, Content Intelligence and AI Innovation
ISMG

Executive Summary

The “Cybersecurity Pulse Report” report was produced through a meticulous three-step process. Initially, an AI-powered analysis of the session titles, descriptions, and speakers from this year’s RSA Conference (RSAC) was conducted. This analysis aimed to synthesize key topics and technology categories presented at the conference, identifying 13 primary themes. Each session was reviewed to ensure a comprehensive capture of the topics covered during RSAC, providing a detailed foundation for further analysis.

Subsequently, ISMG’s proprietary knowledge base and AI platform were leveraged to develop SEO Content Briefs for the identified themes. This technology facilitated the efficient categorization and synthesis of vast amounts of data, ensuring accuracy and relevance. The final step involved analyzing more than 550 pages of interview transcripts with industry thought leaders conducted during the RSAC conference. These interviews were mapped to the 13 themes identified from the session content, highlighting the overlap and convergence between session discussions and expert insights. This comprehensive approach ensured a holistic view of the dominant themes and emerging trends in the cybersecurity industry.



The report delves into several key areas, starting with the transformative impact of artificial intelligence (AI) and machine learning (ML) on all aspects of cybersecurity. Additional topics of note include:

Cloud Security:

Securing distributed applications across multiple cloud environments is complex, necessitating constant vigilance and advanced security measures due to the volume and sophistication of attacks.

Cybersecurity Framework:

Evolving to address the broadening scope of cyber threats, these frameworks emphasize governance and identity's critical role in zero-trust models, recognizing cybersecurity as a fundamental business risk..

Ransomware Defense:

With evolving tactics posing significant challenges, the report advocates for advanced recovery solutions and "cyber storage" to ensure rapid data recovery and prevent data leakage.

Operational Technology (OT) Security:

Given OT's critical role in industrial processes, specialized OT security measures are needed to gain deep visibility into industrial control systems and address legacy systems' vulnerabilities.

Nation-State Threats:

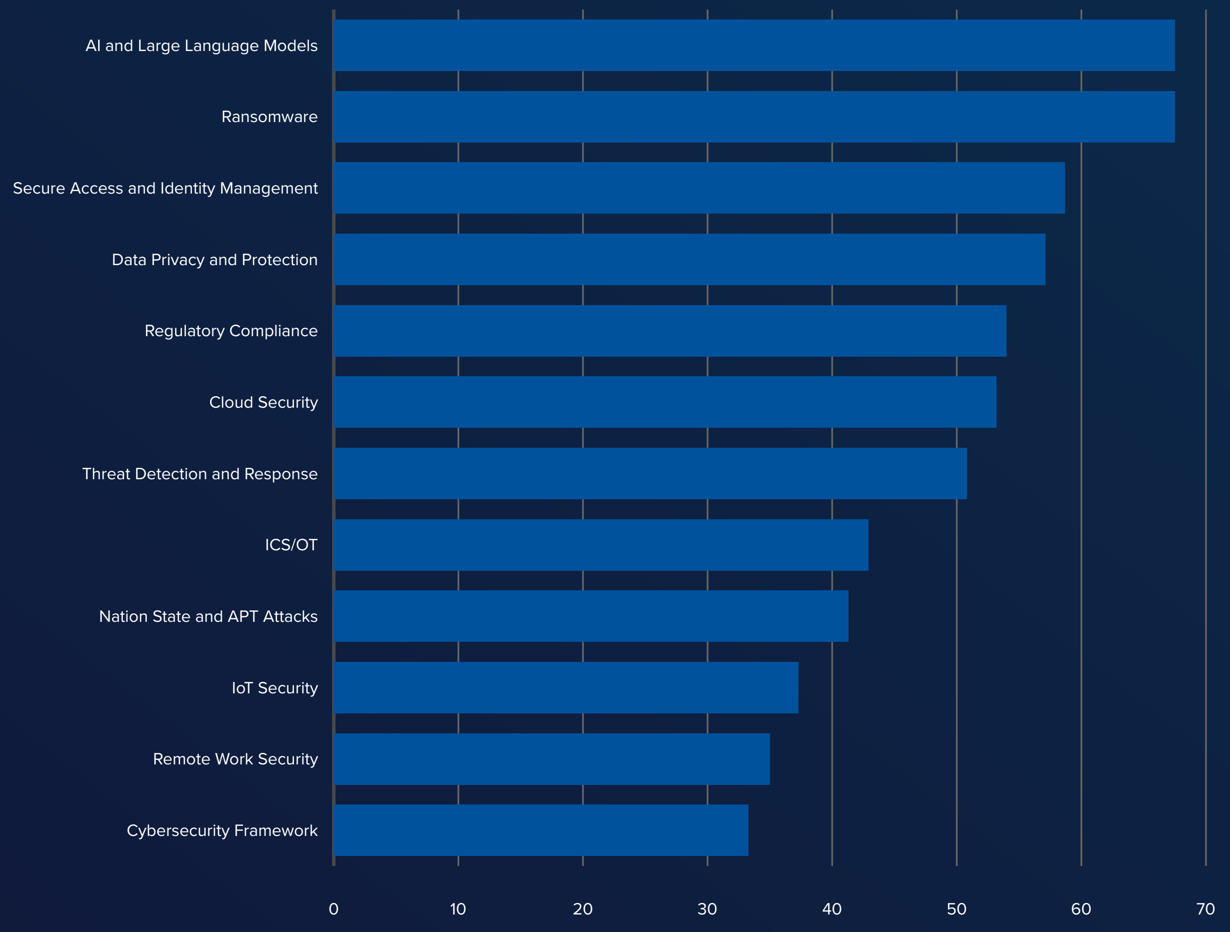
These increasingly sophisticated threats require a coordinated global response, robust policy frameworks, and international cooperation to be effectively mitigated.

IoT Security and Remote Work:

The complexities of IoT security, regulatory challenges, and the expanded attack surface from remote work necessitate a human-centric cybersecurity architecture integrating endpoint and network protection based on zero-trust principles.

This "Cybersecurity Pulse Report" is an unparalleled resource for cybersecurity planning, investment, and operational effectiveness. It provides a detailed roadmap for navigating the complex and evolving landscape of cyber threats, ensuring organizations are well-equipped to protect their digital assets and maintain robust security frameworks.

What The Industry is Talking About

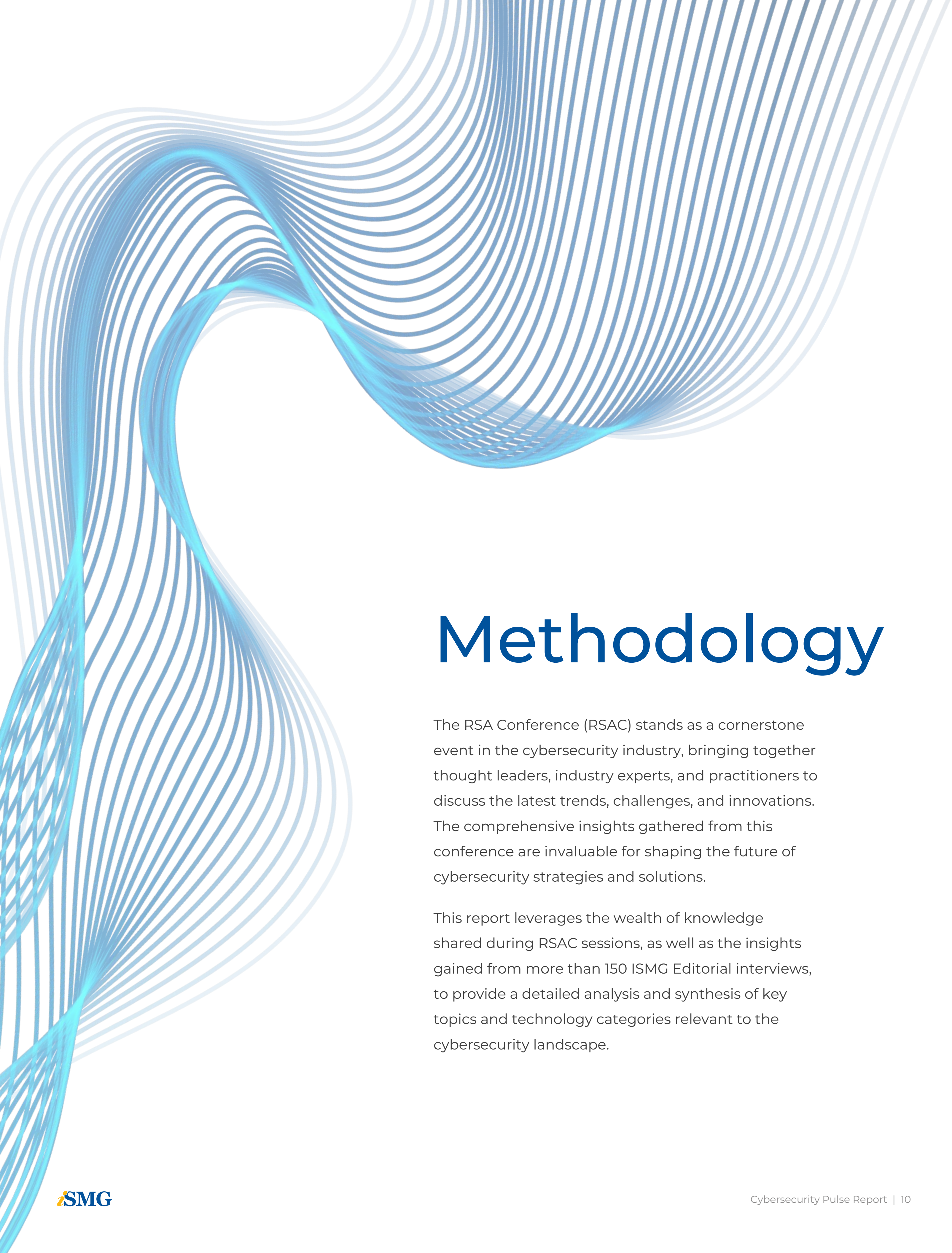


The trend data depicted in the above chart reveals key focus areas within the cybersecurity industry for the next 12 months. Leading topics include “AI and Large Language Models” and “Ransomware,” highlighting the industry’s emphasis on leveraging AI for enhanced security measures and addressing the persistent threat of ransomware attacks. AI, particularly large language models, is being used to predict, detect, and mitigate cyber threats more effectively. Meanwhile, ransomware remains a significant concern, driving investments in advanced defense mechanisms to protect data and infrastructure.

“Zero Trust,” “Secure Access and Identity Management,” and “Data Privacy and Protection” also feature prominently, reflecting a shift toward more granular security frameworks. The Zero Trust model, which mandates thorough authentication for every access request, is increasingly essential in remote and hybrid work environments. Emphasis on secure access and identity management underscores the need for effective controls over sensitive information access. Concurrently, data privacy and protection are driven by stringent regulatory requirements and the necessity to safeguard personal and corporate data against breaches.

> “The Zero Trust Security market size is expected to reach $51.6 billion by 2028.”
>
> **Grand View Research**

Further trends include “Regulatory Compliance,” “Cloud Security,” and “Threat Detection and Response.” These areas highlight the industry’s response to the growing complexity of cybersecurity threats and the imperative for comprehensive regulatory compliance. With the migration to cloud services, ensuring cloud security is paramount, leading to the development of strategies to protect cloud infrastructures. Advanced threat detection and response mechanisms are critical for identifying and responding to cyber threats in real-time, minimizing potential damage. The focus on “ICS/OT,” “Nation State and APT Attacks,” critical infrastructure, defending against sophisticated attacks, and protecting the expanding network of connected devices.



Methodology

The RSA Conference (RSAC) stands as a cornerstone event in the cybersecurity industry, bringing together thought leaders, industry experts, and practitioners to discuss the latest trends, challenges, and innovations. The comprehensive insights gathered from this conference are invaluable for shaping the future of cybersecurity strategies and solutions.

This report leverages the wealth of knowledge shared during RSAC sessions, as well as the insights gained from more than 150 ISMG Editorial interviews, to provide a detailed analysis and synthesis of key topics and technology categories relevant to the cybersecurity landscape.

Extracting and Analyzing Session and Interview Content

STEP 1

of our younger employees came to me
to ask me, hey, Mikko, you're a global cybersecurity

Data Analysis of RSAC Session Content

The first step in our methodology involved a thorough AI-powered analysis of the session titles, descriptions, and speakers from this year's RSAC. This analysis aimed to produce a detailed synthesis of the key topics and technology categories presented at the conference.

Each session was carefully reviewed to identify 13 primary themes, technological focus areas, and key discussions. This step ensured that we captured the full spectrum of topics covered during the conference.

RSAC 2024 Themes

AI & Machine Learning

Cloud Security

Cybersecurity Framework

Data Privacy & Protection

Threat Detection & Response

Future of Ransomware Defense

Secure Access & Identity Management

APTs & Nation State Threats

Cybersecurity in Operational Technology (OT)

Cybersecurity in Remote Work

Regulatory Compliance and Cybersecurity

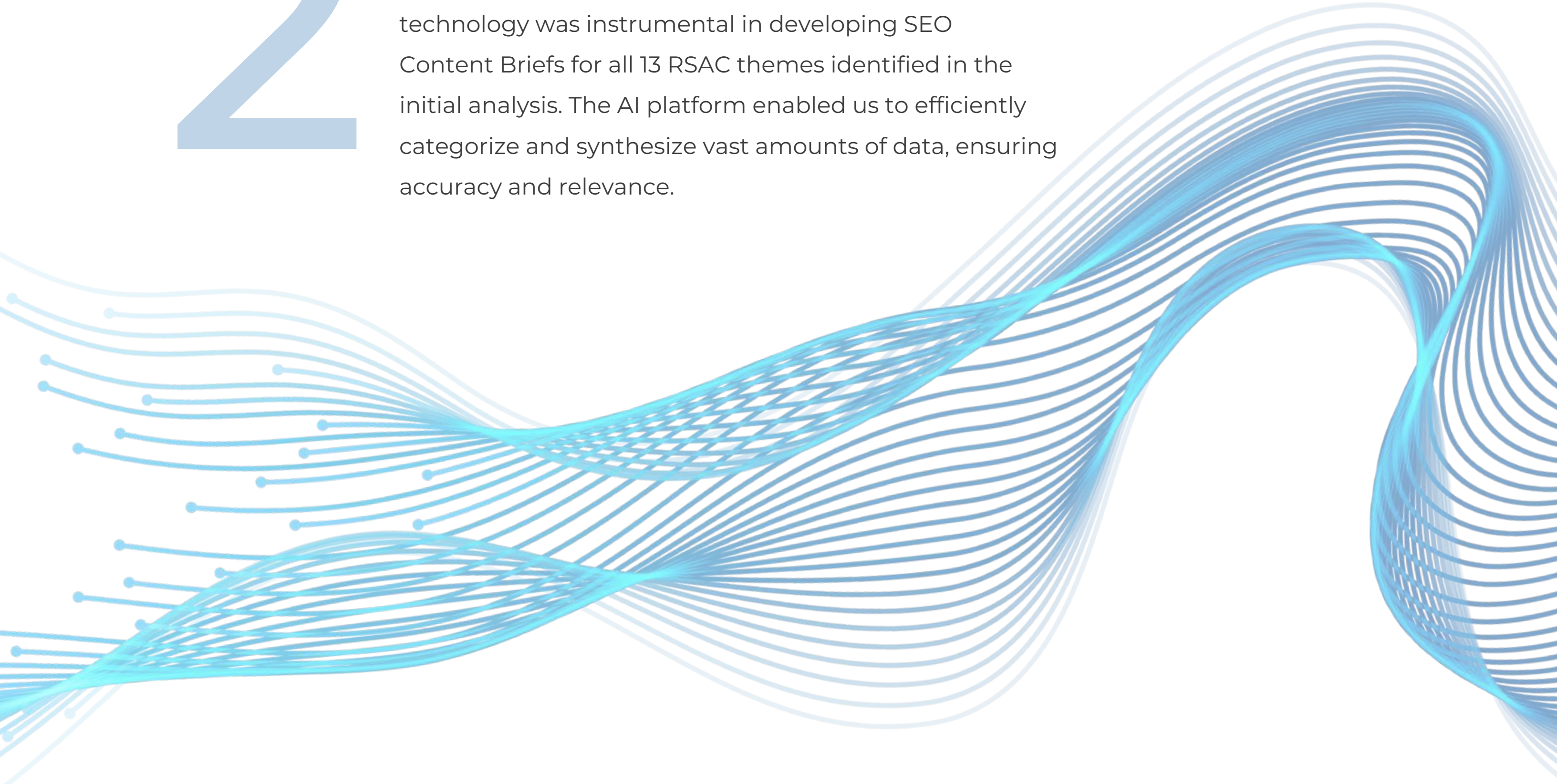
IOT Security

Zero Trust Security

STEP 2

Leveraging ISMG's Proprietary Knowledge Base and AI Platform

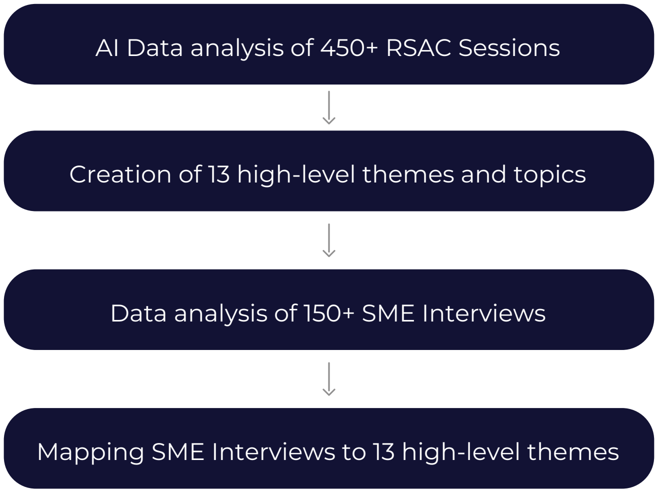
To further enhance the analysis, we leveraged ISMG's proprietary knowledge base and AI platform. This technology was instrumental in developing SEO Content Briefs for all 13 RSAC themes identified in the initial analysis. The AI platform enabled us to efficiently categorize and synthesize vast amounts of data, ensuring accuracy and relevance.



STEP 3

Data Analysis of Interview Transcripts

The final step involved analyzing more than 550 pages of transcripts from ISMG Editorial interviews conducted with industry thought leaders and subject matter experts during the RSAC conference. These interviews were meticulously mapped to the 13 RSAC themes identified from the conference agenda. The objective was to identify the overlap and convergence between the session content and the expert insights gathered during the interviews. This mapping process provided a comprehensive view of the dominant themes and emerging trends in the cybersecurity industry.



AI Data analysis of 450+ RSAC Sessions

Creation of 13 high-level themes and topics

Data analysis of 150+ SME Interviews

Mapping SME Interviews to 13 high-level themes

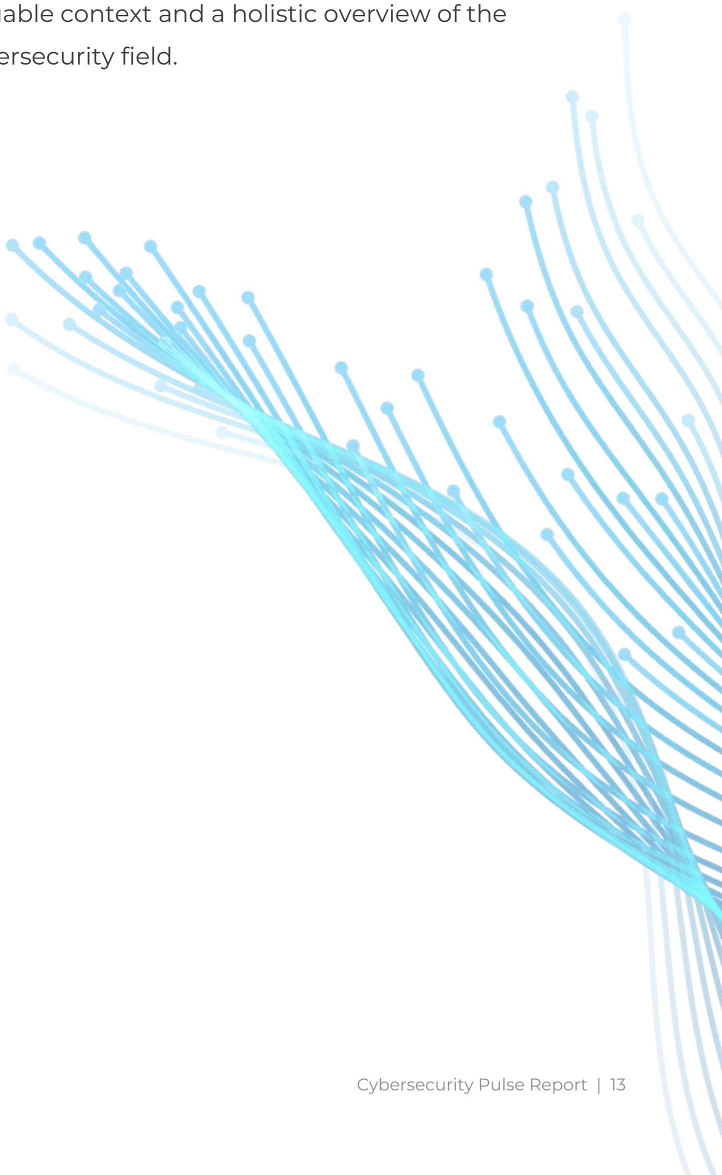
Categorization and Visualization

Our categorization and visualization process began with AI-driven analysis of over 450 RSAC sessions. This comprehensive data analysis identified key patterns and insights, forming the basis for the creation of 13 high-level themes and topics. These themes encapsulate the core subjects and emerging trends discussed during the sessions, providing a structured framework for further exploration.

This systematic approach not only organizes vast amounts of data but also visually represents the relationship between RSAC 2024 session content and ISMG interview themes. The resulting graphic provides a clear and accessible view of how the discussions and insights from various sources converge, offering valuable context and a holistic overview of the cybersecurity field.

Conclusion

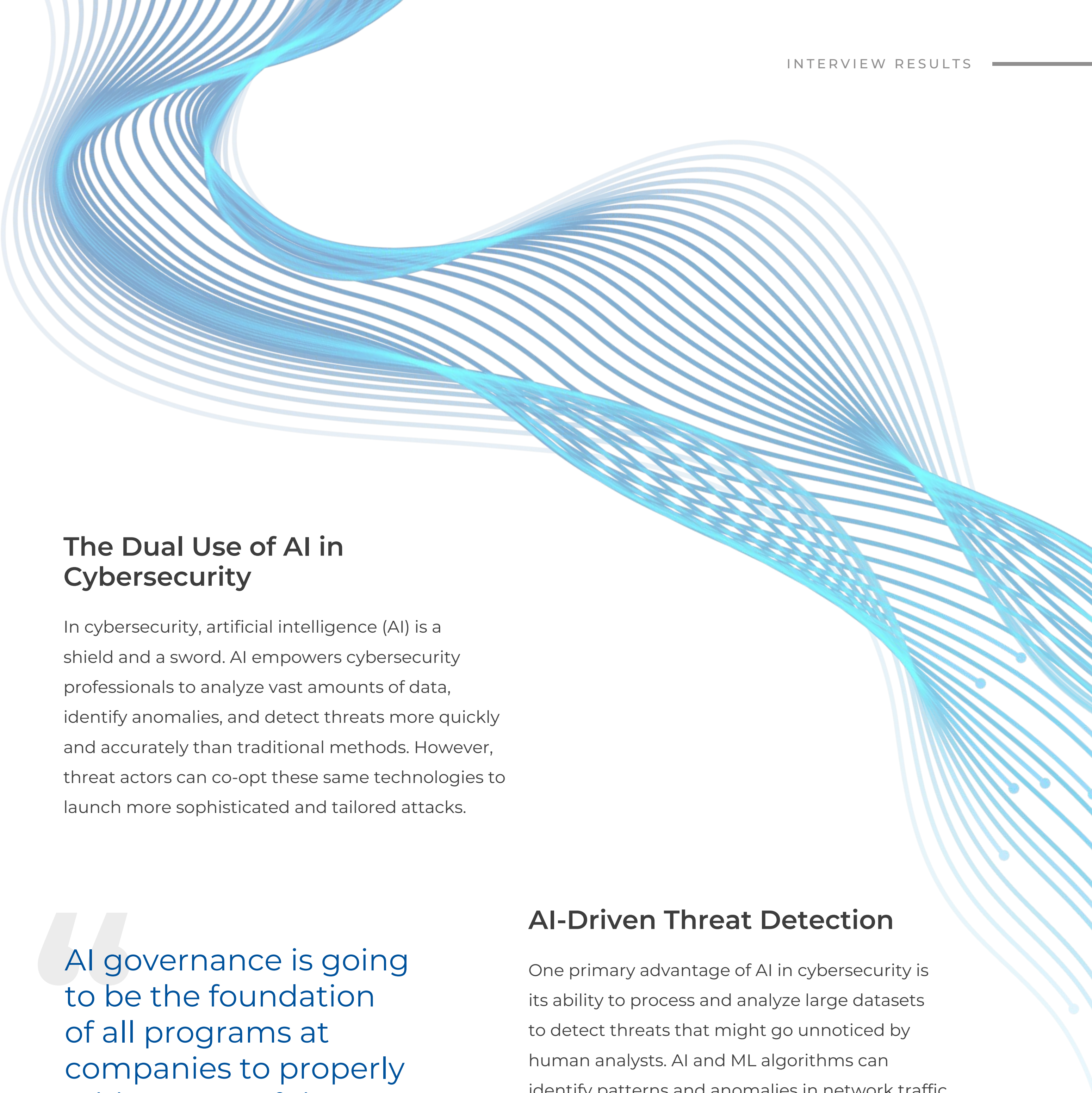
The methodology outlined above underscores the rigorous process undertaken to extract and analyze valuable insights from the RSAC conference sessions and ISMG's editorial interviews. By leveraging advanced analytical tools and combining session content with expert interviews, we have produced a thought leadership report that provides a holistic view of the current state and future directions of the cybersecurity industry. The RSA Conference continues to be a pivotal event for driving innovation and collaboration in cybersecurity, and this report aims to extend the impact of the knowledge shared during the conference.



Topical Analysis

AI and Machine Learning

Integrating artificial intelligence (AI) and machine learning (ML) into cybersecurity represents a dynamic shift in how organizations defend against evolving cyber threats. This exposé delves into AI's dual-edged nature in cybersecurity, highlighting its potential for enhancing defenses and amplifying risks



The Dual Use of AI in Cybersecurity

In cybersecurity, artificial intelligence (AI) is a shield and a sword. AI empowers cybersecurity professionals to analyze vast amounts of data, identify anomalies, and detect threats more quickly and accurately than traditional methods. However, threat actors can co-opt these same technologies to launch more sophisticated and tailored attacks.

> “AI governance is going to be the foundation of all programs at companies to properly address any of those areas of security, risk, governance, audit.”
>
> **Brennen P. Baybeck**
> ISACA Board Vice Chair and SVP &
> CISO for Customer Success Services,
> Oracle Corporation

AI-Driven Threat Detection

One primary advantage of AI in cybersecurity is its ability to process and analyze large datasets to detect threats that might go unnoticed by human analysts. AI and ML algorithms can identify patterns and anomalies in network traffic, flagging potential security incidents in real time. Companies like DeepWatch and CrowdStrike have integrated AI into their security platforms to enhance threat detection and response capabilities. For example, DeepWatch uses AI to improve the responsiveness and effectiveness of its security operations, leveraging strategic partnerships to bolster its AI-driven defenses.

Challenges of AI in Cybersecurity

Despite the benefits, integrating AI into cybersecurity presents challenges. One significant issue is the risk of attackers manipulating AI models. Continuous security assessments and integration of specialized skills, such as advanced mathematics, are necessary to secure AI models effectively. The potential for AI systems to be “jailbroken” and used to extract sensitive information underscores the importance of robust security measures and regular evaluations of AI systems.

Ethical and Regulatory Considerations

The ethical implications of AI in cybersecurity are profound. Ensuring transparency and accountability in how AI tools are trained and deployed is critical. AI models must be frequently evaluated for biases and blind spots, with human oversight to verify the actions taken by these systems. Regulatory compliance adds another layer of complexity. Navigating regulations like GDPR and HIPAA while leveraging AI to enhance security requires a delicate balance. Policymakers and industry leaders must collaborate to develop agile regulations that evolve alongside technological advancements.

AI in Fraud Detection and Prevention

AI and ML are revolutionizing fraud detection, especially in finance. By analyzing transaction patterns and identifying deviations, AI systems can flag potentially fraudulent activities before they cause significant harm. This capability is crucial for combating the rise in digital fraud, which has become more prevalent with the increased use of online transactions. AI-driven fraud detection systems adapt to new fraud tactics, providing a dynamic defense against evolving threats.

Future Directions and Innovations

The future of AI in cybersecurity looks promising, with continuous advancements in AI technologies and their applications. For example, large language models (LLMs) enhance cybersecurity solutions by improving operational efficiency and making these solutions more user-friendly. AI in predictive analytics and breach anticipation is also gaining traction, helping organizations proactively address potential threats before they materialize.

Moreover, integrating AI with other emerging technologies, such as blockchain and quantum computing, can further strengthen cybersecurity frameworks. These technologies can enhance data integrity and provide robust defenses against increasingly sophisticated cyber threats.

Conclusion

AI's capacity to process, analyze, and respond to vast arrays of data at unprecedented speeds enables the detection and neutralization of potential risks with a level of efficiency that is unattainable by human operators alone.

Notwithstanding these advancements, the intrinsic dual-use characteristic of AI technologies dictates a deliberate and judicious application. This duality—where AI serves as both a protective mechanism and a potentially exploitative tool—mandates the establishment of principled guidelines and deployment strategies. Thus, the ethical utilization of AI is non-negotiable; organizations must ensure that the adoption of these technologies adheres to ethical standards which respect privacy, data integrity, and transparency

> "Let the AI assist you with the automation so you can get faster... and create generative workflows that take something that historically might have taken you minutes or hours to perform and have the AI automate that in seconds. And then you can use that freed up spare time to go back to the basics and focus on things like threat hunting."

Elia Zaitsev
Chief Technology Officer, CrowdStrike

Cloud Security

As organizations migrate more operations to the cloud, the complexity and scale of potential security threats have escalated, necessitating a shift in how we approach securing cloud environments.

Cyberattacks targeting cloud infrastructures have become increasingly numerous and sophisticated. “One of the big things that we’re seeing is just a huge increase in the volume and sophistication of attacks out there globally,” said Rich Campagna, VP of Product at Palo Alto Networks. “For example, our platform alone stops over 12 billion attacks per day to give some color to how large that is. As a comparison point...there are about 9 billion Google searches per day. So in one platform, one network security platform, 33% more attacks stopped per day.”

This figure underscores the relentless nature of cyber threats and the daunting task faced by security teams, who must thwart every attack attempt. At the same time, attackers only need to succeed once to cause significant damage.

View the full interview here.

> One of the big things that we’re seeing is just a huge increase in the volume and sophistication of attacks out there globally.
>
> **Rich Campagna**
> VP of Product, Palo Alto Networks

Distributed Nature of Cloud Environments

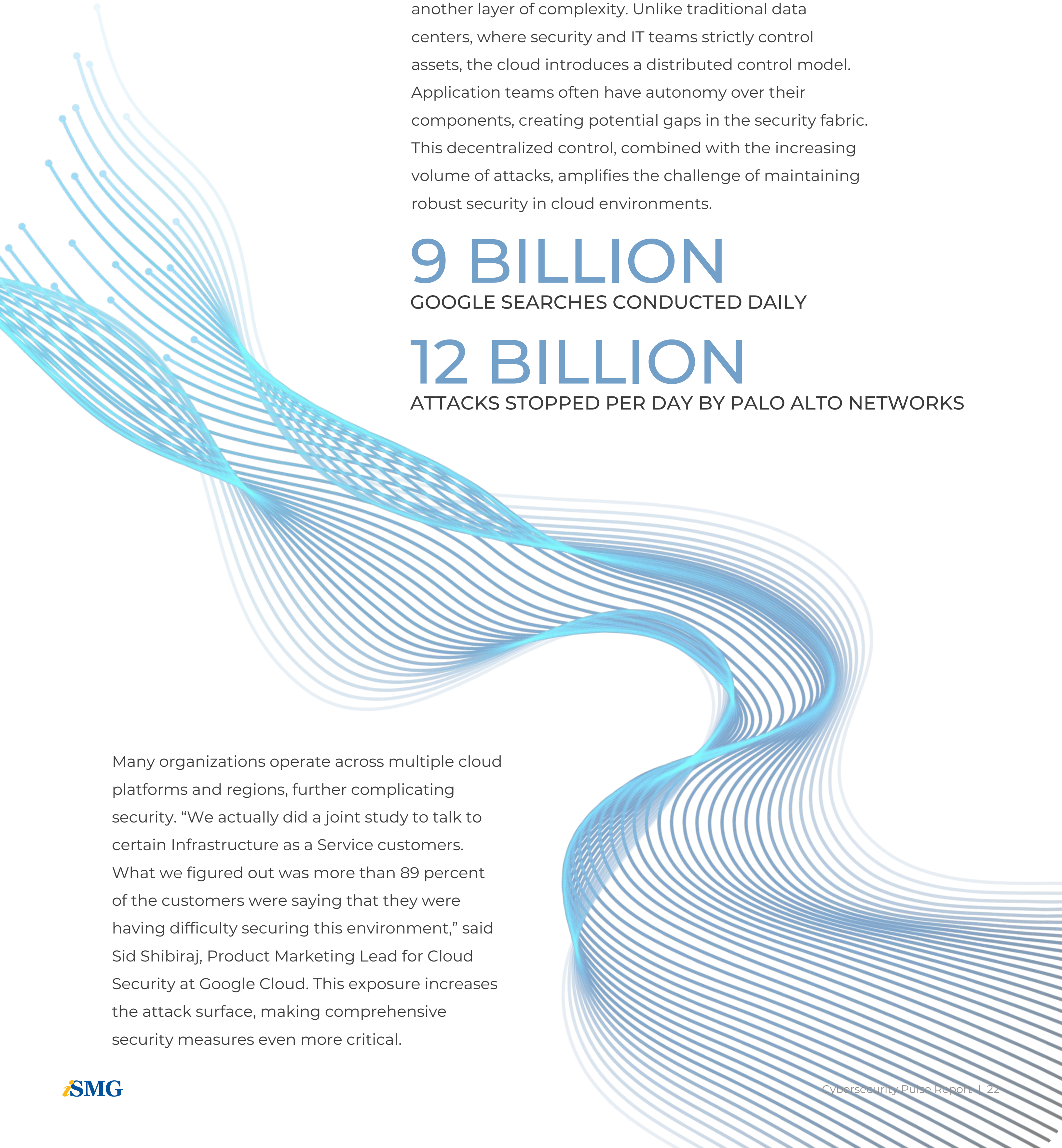
The distributed nature of cloud environments adds another layer of complexity. Unlike traditional data centers, where security and IT teams strictly control assets, the cloud introduces a distributed control model. Application teams often have autonomy over their components, creating potential gaps in the security fabric. This decentralized control, combined with the increasing volume of attacks, amplifies the challenge of maintaining robust security in cloud environments.

9 BILLION

GOOGLE SEARCHES CONDUCTED DAILY

12 BILLION

ATTACKS STOPPED PER DAY BY PALO ALTO NETWORKS



Many organizations operate across multiple cloud platforms and regions, further complicating security. “We actually did a joint study to talk to certain Infrastructure as a Service customers. What we figured out was more than 89 percent of the customers were saying that they were having difficulty securing this environment,” said Sid Shibiraj, Product Marketing Lead for Cloud Security at Google Cloud. This exposure increases the attack surface, making comprehensive security measures even more critical.

Cloud-Native Security Tools

The advent of cloud-native security tools explicitly tailored for cloud environments marks a pivotal shift. Unlike retrofitting traditional security appliances for the cloud, these new tools address the unique challenges of cloud security. Tools developed for cloud detection and response (CDR) provide security operations centers (SOCs) with the capability to monitor and defend cloud infrastructures in ways that traditional on-premises solutions cannot. These advancements are crucial for protecting against cyber adversaries' evolving tactics, which increasingly exploit the nuances of cloud environments.

View the full interview here.

> "We actually did a joint study to talk to certain Infrastructure as a Service customers. What we figured out was more than 89 percent of the customers were saying that they were having difficulty securing this environment."

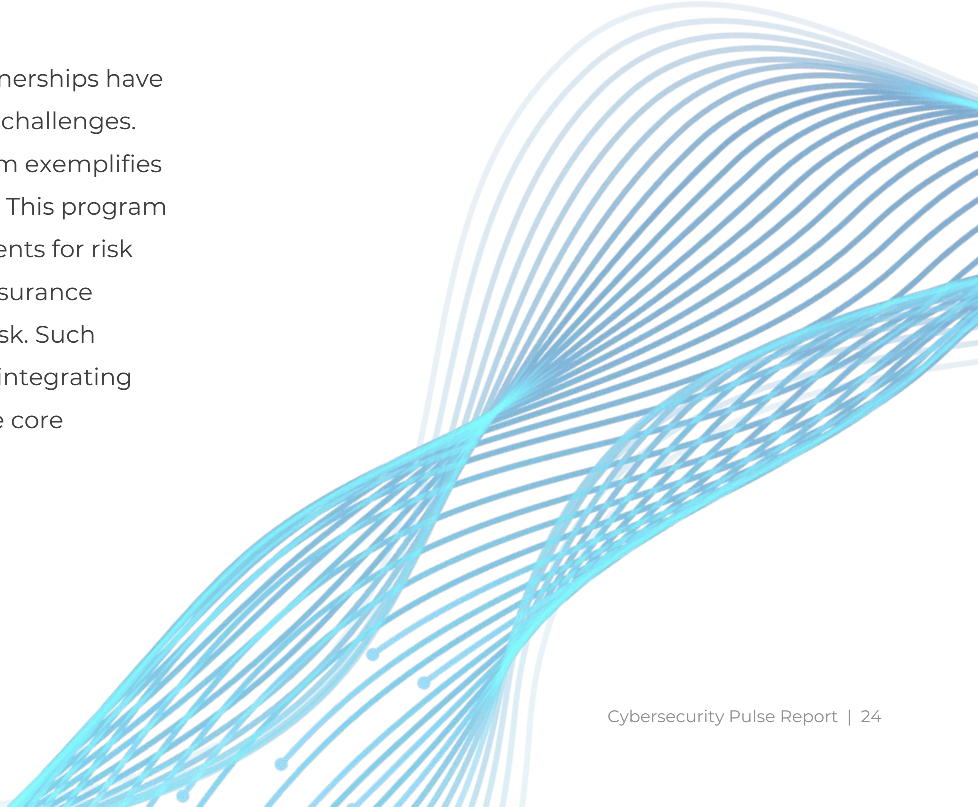
Sid Shibiraj
Product Marketing Lead,
Cloud Security at Google Cloud

Data Protection

The narrative of cloud security also encompasses the critical role of data protection. Ensuring data safety, whether at rest or in motion, is a foundational aspect of cloud security strategies. Modern data backup systems now incorporate zero-trust principles, making data immutable and encrypted by default. This approach is vital in defending against ransomware attacks, which often target backups to cripple an organization's ability to recover. Organizations can significantly enhance their security by securing backups and making data resilient to tampering.

Innovative Solutions and Strategic Partnerships

Innovative solutions and strategic partnerships have become essential in response to these challenges. Google's Cloud Risk Protection Program exemplifies a proactive approach to cloud security. This program involves scanning customer environments for risk indicators and sharing findings with insurance partners to better price and manage risk. Such initiatives highlight the importance of integrating security and risk management into the core operations of cloud service providers.



Conclusion

Organizations must commit to the implementation of security protocols that extend beyond conventional perimeters. This includes adopting behavior analytics that go beyond static rule-based security to dynamically respond to potential threats by learning normal user behaviors and detecting anomalies.

Organizations should integrate encryption protocols for both data at rest and in transit, ensuring all data is encrypted using robust cryptographic standards to prevent unauthorized access. Furthermore, leveraging cloud access security brokers (CASBs) will enable better visibility and control over data, irrespective of where it resides. The use of virtual private clouds (VPCs) should also be standardized to provision logically isolated sections of the cloud where resources can be securely stored.

In concert with technological advancements, strategic partnerships amplify an organization's ability to secure its digital assets. Partnering with reliable cloud service providers and cybersecurity specialists can foster a collaborative approach to security. These alliances enable organizations to gain from shared security intelligence and the best practices in cloud security, ensuring a unified defense mechanism against cyber threats.

Transitioning to cloud-native security solutions—such as microsegmentation to create secure zones in cloud deployments, and employing zero trust models that verify everything trying to connect to the system before access is granted—highlights a transformative approach in safeguarding assets.

Data Privacy and Protection

The conversations among industry experts reveal a landscape marked by rapid evolution and heightened complexity in data privacy and protection. As organizations embrace digital transformation and leverage cutting-edge technologies, safeguarding sensitive data has become increasingly challenging.

One of the primary concerns today is the proliferation and distribution of data across diverse environments. Data is no longer confined to on-premises data centers but is spread across multiple platforms, including private and public clouds, SaaS applications, and various endpoints. This distribution has created numerous entry points for potential breaches, complicating maintaining robust data security. Traditional measures designed for centralized data repositories often fall short in this new paradigm, necessitating innovative approaches to data protection.

> This is the first time that I think I see a light at the end of the tunnel where the defender might have an advantage, largely because of data. I think security needs a new architecture, but the data advantage that we can provide with AI … is going to be material..
>
> **Jeetu Patel**
> Executive Vice President and General Manager of Security and Collaboration, Cisco

Data Discovery and Classification

Experts emphasized the critical need for comprehensive data discovery and classification. Organizations often struggle with the sheer volume of data they generate, including millions of files across different storage solutions. It is virtually impossible to implement effective security measures without a clear understanding of what data is being stored and where it is stored. Modern data protection strategies must incorporate advanced technologies such as AI and machine learning to automate the discovery and classification process. By leveraging these tools, organizations can identify sensitive data, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), and assign appropriate risk scores to facilitate better protection.

Evolving Data Usage and AI Integration

Another significant challenge is the evolving nature of data usage and the increasing integration of AI technologies. AI and machine learning applications can process vast data to deliver insights and drive business innovation. However, this also introduces new risks, as organizations may not fully understand how their data is being used or exposed. Ensuring the security of AI systems involves protecting the data they use and securing the algorithms and models themselves from adversarial attacks and manipulation.

"You have to have security defenses put in front of every IoT device, in front of every OT device, in front of every Kubernetes container, cluster, VM, microservice," said Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration, Cisco. "And if you don't do that, you have a woefully inadequate security infrastructure compared to what the demand signals are going to be for the volume that's going to be processed in these AI-scale data centers."

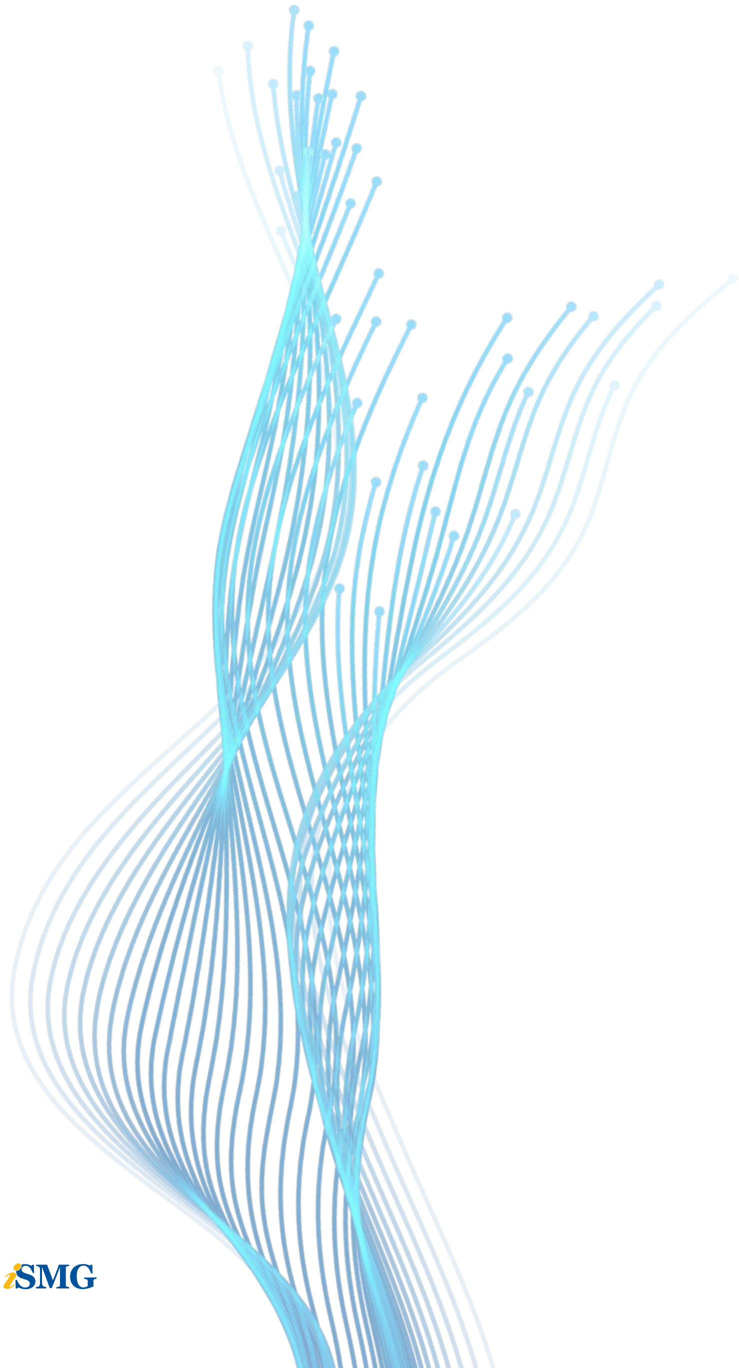
View the full interview here.

> You have to have security defenses put in front of every IoT device, in front of every OT device, in front of every Kubernetes container, cluster, VM, microservice.
>
> **Jeetu Patel**
> Executive Vice President and General Manager of Security and Collaboration, Cisco

Ransomware Threats

Ransomware attacks pose a significant threat to data privacy and protection. The rise of double extortion ransomware, where attackers encrypt data and threaten to leak it, underscores the need for robust backup and recovery solutions. Protecting backup data is paramount, as compromising backups can severely hinder an organization's ability to recover from an attack. Implementing immutable backups and multi-layered encryption can mitigate the risk of ransomware impacting critical data.

Amit Sinha, CEO, DigiCert, discussed how quantum computing gives malicious actors the opportunity to break encryption algorithms and exploit legitimate applications and websites.



Regulatory Compliance

Maintaining compliance with evolving regulations requires a proactive approach to data governance. Organizations must implement policies and procedures that ensure data protection across all departments and functions. This includes educating employees at all levels about data security best practices and fostering a culture of security awareness.

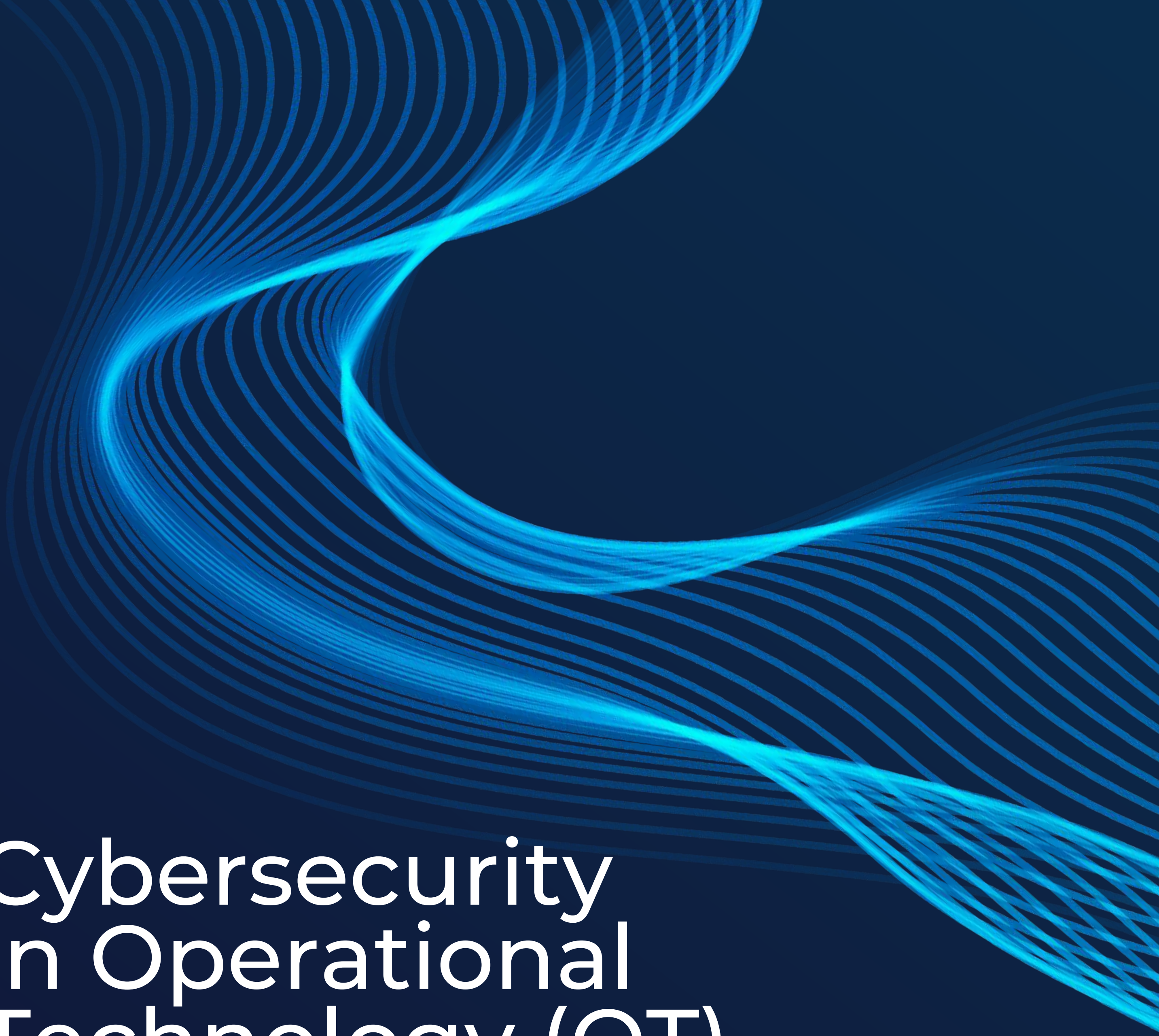
The role of privacy professionals has expanded in response to these challenges. Privacy leaders are increasingly involved in AI governance and compliance initiatives, ensuring that ethical considerations are integrated into developing and deploying AI systems, processes, and procedures. They are also pivotal in crafting organizational strategies that balance innovation with data protection, enabling businesses to leverage modern technologies while safeguarding their customers' trust.

Conclusion

The narrative of data privacy and protection is one of continuous adaptation and vigilance, necessitated by the increasing complexity and interconnectedness of data environments. Organizations must adopt holistic and dynamic security strategies to address these evolving challenges. This includes implementing comprehensive frameworks such as Zero Trust Architecture, robust Governance, Risk, and Compliance (GRC) programs, and advanced encryption techniques to ensure all facets of data management are secure.

Artificial intelligence and machine learning enhance threat detection and response capabilities, providing real-time analysis and predictive insights that help preempt breaches. Cloud security solutions and Secure Access Service Edge (SASE) models protect data in hybrid and remote work environments, reflecting the need for innovative solutions in a rapidly changing digital landscape.

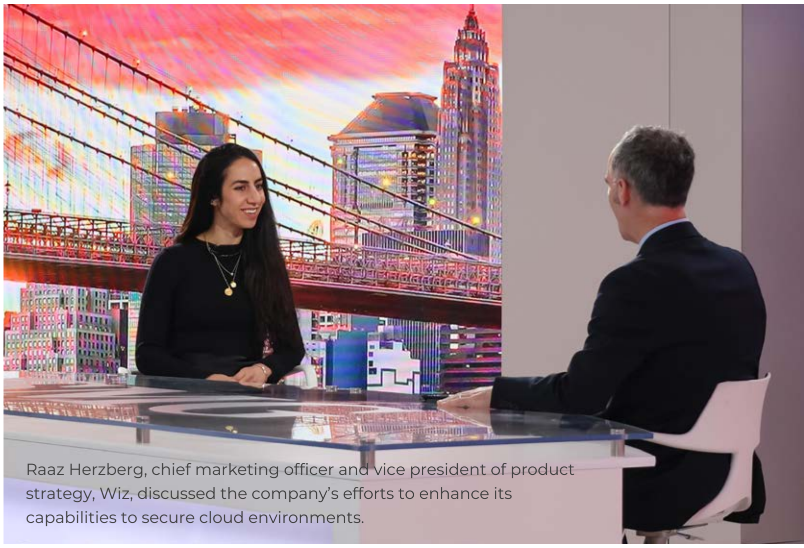
Fostering a pervasive security culture within the organization is equally important. This involves continuous training for employees to recognize and respond to security threats, promoting best practices for data handling, and ensuring that security is ingrained at all levels. Additionally, staying abreast of regulatory changes and ensuring compliance with laws such as GDPR and CCPA through proactive privacy management is essential.



Cybersecurity in Operational Technology (OT) Environments

The challenge of cybersecurity in Operational Technology (OT) environments has become increasingly critical. The interconnected nature of industrial systems exposes significant vulnerabilities, which, if exploited, could lead to catastrophic consequences for critical infrastructures.

One of the major themes that emerged from ISMG's discussions with experts in OT cybersecurity is the persistent and evolving threat landscape. Unlike IT systems, which can often be patched or rebooted without major repercussions, OT systems are deeply integrated into physical processes. Shutting down crucial industrial equipment for a security update can lead to significant operational disruptions and financial losses. Many OT systems are legacy systems, designed long before cybersecurity was a concern. They lack the built-in security features of modern IT infrastructure, making them more vulnerable to attacks.



Raaz Herzberg, chief marketing officer and vice president of product strategy, Wiz, discussed the company's efforts to enhance its capabilities to secure cloud environments.

Another focal point is the convergence of IT and OT. While beneficial for operational efficiency and data sharing, this convergence introduces new vulnerabilities. IT security strategies cannot be directly applied to OT environments without adaptation. The need for specialized OT security measures is paramount. One critical challenge is the lack of visibility in OT networks. Traditional IT security tools often fail to provide adequate monitoring and detection capabilities for OT environments, necessitating developing and deploying specialized solutions to bridge this gap.

Experts advocate for a systemic and scalable approach to OT security. This involves building a strong foundation of security practices that can be continuously improved. One effective strategy is implementing a multi-layered defense mechanism that integrates various security controls and measures. This includes traditional IT security measures and specialized OT security tools that provide deep visibility into industrial control systems and can detect anomalies and potential threats in real time.

Dawn Cappelli, Head of OT-CERT at Dragos, said the convergence of IT and OT environments introduces new vulnerabilities, necessitating specialized frameworks addressing the distinct characteristics of OT systems. She discussed how the unique challenges faced by critical infrastructure sectors, such as nation-state attacks and hacktivism, underscore the need for tailored security measures within these environments.

Vulnerability management is another critical area. Given the long lifespan of industrial equipment, many OT systems operate with known vulnerabilities that cannot be easily patched. This makes real-time monitoring and quick response capabilities essential. Organizations must prioritize vulnerabilities based on their potential impact and focus on mitigating the most critical ones. Vendors' lack of practical mitigation advice further complicates this task, highlighting the need for more comprehensive and actionable guidance.

Sophos Field CTO John Shier shared insights from the latest annual report on the state of ransomware.

Regulatory requirements also play a significant role in shaping OT cybersecurity strategies. New regulations mandating the reporting of cybersecurity incidents and the disclosure of cybersecurity postures force companies to pay closer attention to their OT security practices. This regulatory pressure is driving investment in OT security and elevating the importance of cybersecurity at the board level. Boards are now more aware of the risks and increasingly demand robust security measures to protect critical infrastructure.

The human element cannot be overlooked. It can be difficult for organizations to train and retain skilled personnel who understand both the cybersecurity components as well as the OT environmental components specific to their organization and industry. Skill gaps often force organizations to rely on a combination of internal expertise and external partners to manage OT security effectively.

Conclusion

Securing Operational Technology environments is a complex and multifaceted challenge. It requires a tailored approach considering industrial systems' unique characteristics and constraints. As threats continue to evolve, so must the strategies and technologies used to defend against them. By focusing on visibility, vulnerability management, regulatory compliance, and the human element, organizations can build more resilient OT security postures that safeguard critical infrastructure against a wide range of cyber threats.

> "7 out of 10 industrial OT attacks originate in Informational Technology (IT) environments, signaling an urgent need for OT and IT departments and technologies to start working more closely together."
>
> **Palo Alto Networks**
> The State Of OT Security: A Comprehensive Guide To Trends, Risks, & Cyber Resilience

Future of Ransomware Defense

The future of ransomware defense hinges on integrating advanced technologies and innovative strategies to counter the growing sophistication of cyber threats. A crucial aspect of this evolution is using Artificial Intelligence (AI). AI, particularly generative AI, democratizes cyber offense, enabling even less skilled threat actors to launch complex and malicious attacks. This has increased the volume and severity of ransomware attacks, necessitating the elevation of defensive strategies.

For cybersecurity professionals, incorporating AI into defensive mechanisms is essential. AI systems, especially those using behavioral detection, can detect and mitigate threats with remarkable speed and accuracy. These systems analyze vast amounts of data in real time, identifying potential threats that manual processes might miss, thereby enhancing overall cyber defenses.

A significant challenge in ransomware defense is protecting unstructured data, which constitutes most digital information today and is a prime target for ransomware attacks.

"If you look at the standard type of data that tends to be attacked, exfiltrated, or encrypted today, a lot of it is known as unstructured data, file, and object," said Alex Hesterberg, CEO of Superna. "And this data is actually 90% of the digital data created today. Only 10% is structured and in databases. So it's a huge threat landscape, and it's the number one area where these attacks are taking place."

The use of AI to monitor and secure unstructured data is critical. By focusing on the data layer itself—often the last line of defense—organizations can detect anomalies and potential breaches in real time, significantly enhancing their defensive posture.

View the full interview here.

> If you look at the standard type of data that tends to be attacked, exfiltrated, or encrypted today, a lot of it is known as unstructured data, file, and object.
>
> **Alex Hesterberg**
> CEO, Superna

Menlo Security's Ben-Efraim discusses enhancing existing browsers with additional security.

"Cyber storage" is emerging as a crucial element in ransomware defense. This approach directly applies traditional network security measures, such as intrusion detection and prevention, to the data storage layer.

"They're going after backups much more than they have before," said John Shier, Field CTO of Threat Intelligence at Sophos. "We've also unfortunately seen a five times increase in the median ransomware payments. Threat actors out there steal data about a third of the time."

Companies can bridge the gap between data security and operational resilience by creating a fortified environment where data is backed up and recoverable, actively monitored, and protected against unauthorized access and exfiltration.

Intelligent security operations centers (SOCs) are transforming how organizations handle cybersecurity. Traditional SOCs, often overwhelmed by the sheer volume of alerts and data, are being reimagined to incorporate AI-driven intelligence that can prioritize threats and provide actionable insights. This intelligent integration of data sources allows for a more nuanced and effective response to ransomware threats, reducing alert fatigue and improving overall security efficacy.

Conclusion

The future of ransomware defense is shaped by the strategic integration of AI, robust data protection measures, and innovative approaches to data resilience. As threat actors evolve, leveraging these advanced technologies will be crucial in staying ahead. The narrative from these interviews highlights a clear path forward: a comprehensive, proactive, and intelligent defense strategy that not only anticipates but effectively counteracts the multifaceted nature of modern ransomware attacks.

> “The average ransom payment has increased 500% in the last year. 63% of ransom demands were for $1 million or more, with 30% of demands for over $5 million.”

Sophos
The State Of Ransomware 2024

Threat Detection and Response

Threat Detection and Response (TDR) emerged repeatedly in various discussions, highlighting the sophisticated nature of current threats and the strategic responses necessary to mitigate them. The interviews reveal how industry leaders address these challenges through technology, partnerships, and innovative approaches.

Unsurprisingly, AI and machine learning technologies have become a core aspect of effective TDR. These technologies enhance security platforms, making them more responsive and effective against increasingly complex cyber threats. AI-driven analytics play a pivotal role in transforming traditional security operations, allowing for the recontextualization of alerts and prioritization of critical threats. This capability reduces the risk of false negatives and streamlines the workload of security analysts by highlighting the most pertinent issues requiring immediate attention.

The application of AI in TDR extends to automating threat hunting and operationalizing intelligence. Automated threat hunting, driven by behavioral and TTP-based (tactics, techniques, and procedures) hunt packages, enables organizations to search for threats based on established patterns proactively.

Phil Venables, VP, CISO, Google Cloud.

Another crucial element in TDR is emphasizing visibility and contextualization. Security experts highlighted the necessity for complete visibility into the attack surface, an effort made complex by modern systems that can sprawl across traditional IT, IoT, IIoT/OT, and even third-party devices in BYOD environments..

Partnerships and collaborative efforts also play a vital role in enhancing TDR capabilities, said Sunil Patel, managing director of IAC with Accenture. Strategic alliances with leading cybersecurity firms enable the development of integrated solutions that address the dynamic nature of cyber threats. These partnerships often bring together the strengths of multiple organizations, creating a more robust and comprehensive security posture.

The shift toward cloud-based environments further complicates the TDR landscape. Cloud security requires new approaches and tools that differ significantly from on-premises solutions. Integrating cloud-native security measures is crucial for protecting evolving infrastructure. This includes employing cloud-specific detection and response tools that can handle the unique challenges posed by cloud environments, such as the speed and scale of operations and the need for continuous monitoring and rapid response.

Conclusion

Overall, the narrative around Threat Detection and Response in the cybersecurity industry is one of continuous adaptation and innovation. By leveraging advanced technologies, fostering strategic partnerships, and focusing on comprehensive visibility and contextualization, organizations are better equipped to detect and respond to threats in real time. This multifaceted approach is essential for staying ahead of adversaries and ensuring the security and resilience of digital infrastructures in an ever-evolving threat landscape.

EXPLOITS ARE THE **#1 INITIAL VECTOR** IN INCIDENT RESPONSE INVESTIGATIONS.

IN **63% OF INCIDENTS** THE ORGANIZATIONS WERE NOTIFIED BY EXTERNAL ENTITIES.

16 DAYS IS THE GLOBAL MEDIUM DWELL TIME.

Source: Mandiant M-Trends 2023

Secure Access and Identity Management

The narratives from our interviews on Secure Access and Identity Management (SAIM) highlight a shift toward identity-centered security frameworks, particularly within Zero Trust architectures.

One critical component discussed is Privileged Access Management (PAM), which traditionally focused on IT administrators with extensive access to servers, network devices, and mainframes. This definition has now expanded to include a broader range of users.

“Now we’re looking at the workforce users and their access to powerful applications that, unmanaged, can do just as much harm as the core network security element,” said Clay Rogers, Vice President of Global Strategic Alliances, CyberArk. “We’re also looking at developers and what they’re managing from a secrets perspective. And then lastly, we talk about machine identities. The whole Privileged Access Management element has expanded.”

View the full interview here.

> Now we’re looking at the workforce users and their access to powerful applications that, unmanaged, can do just as much harm as the core network security element.
>
> **Clay Rogers**
> Vice President of Global
> Strategic Alliances, CyberArk

As businesses digitize their operations, exposing critical data through various applications and platforms necessitates a cohesive identity-centric strategy. Establishing digital identities for employees, third parties, and contractors is essential for maintaining secure access. This governance is integral to understanding who is accessing what systems and data and ensuring access is appropriately managed throughout the identity lifecycle.

“About 70% of all breaches happen because of compromised identities,” said Amit Chhikara, Principal at Deloitte Advisory Cyber Risk and Privileged Access Management Practices. “So if you think about that, you realize the importance of identity security.”

Identity Management Systems (IMS) are evolving to provide comprehensive visibility and control over these identities. Traditional identity frameworks often struggled with fragmented tools and disparate systems, leading to inefficiencies and security gaps. Modern approaches advocate for unified platforms that integrate identity, governance, and administration functionalities, providing a single view of all identities and data within an organization.

View the full interview here.

> About 70% of all breaches happen because of compromised identities. So if you think about that, you realize the importance of identity security.
>
> **Amit Chhikara**
> Principal, Deloitte Advisory Cyber Risk and Privileged Access Management Practices

The emphasis on multi-factor authentication (MFA) and single sign-on (SSO) remains strong, as these tools form the bedrock of identity verification and access control. However, the integration of identity analytics is becoming increasingly vital. Organizations can achieve full visibility by collecting, correlating, and reviewing identity events. This capability allows for real-time alerts and session shutdowns if necessary, providing a proactive defense mechanism against potential threats.

A significant point of discussion is the need for seamless and frictionless user experiences while maintaining high security. Users often resist security measures that impede their workflow. Therefore, solutions like frictionless MFA, which authenticate users based on their device and context without requiring repetitive logins, are gaining traction. These innovations aim to frustrate attackers without compromising the user experience, balancing security with usability.

The rise of non-human identities, such as those associated with IoT devices and automated processes, adds another layer of complexity to identity management. These identities now significantly outnumber human identities, creating new challenges in visibility and management. Effective management of non-human identities involves managing their lifecycle, from creation to deactivation, and ensuring their activities are continuously monitored and secured.

> The terms identity management and access management are often erroneously used interchangeably. The function of identity management is to confirm that an entity is who or what they are presented to be. In contrast, access management uses validated identity information to determine what resources an entity can use and how.
>
> Source: Sailpoint

Conclusion

The discourse around Secure Access and Identity Management reflects an evolving understanding of cybersecurity. Maintaining a proactive and unified approach to identity security will safeguard organizational assets and data as the landscape shifts.

Identity Management	Identity & Access Management
Deals primarily with the digital identity lifecycle of users	Integrates identity management to ensure identities are used in accordance with corporate policies and security requirements
Core Functions	**Core Functions**
Creating, updating, and deleting user accounts	Allowing users to authenticate once and gain access to multiple systems with single sign-on (SSO)
Managing changes to identity information over time	Defining and enforcing policies that determine user permissions
Verifying a user's identity before granting access	Enhancing security by requiring multiple forms of verification (i.e., multi-factor authentication or MFA)
	Granting or denying access to specific resources based on established policies

Nation States and APT Attacks

The menace of Nation-State threats in cyberspace represents one of the most complex and pervasive challenges facing cybersecurity today. Drawing from ISMG's interviews with industry experts, it is clear that these threats are evolving in sophistication and scope, driven by the extensive resources and strategic motivations of state-sponsored actors.

Advanced Persistent Threats (APTs) are characterized by prolonged and targeted cyber-attacks wherein the intruder remains undetected within a system for an extended period. These threats are often associated with nation states due to the significant resources required to maintain such operations. Unlike typical cybercriminals, who may seek immediate financial gain, APT actors have more nuanced objectives, including espionage, data theft, and the disruption of critical infrastructure.

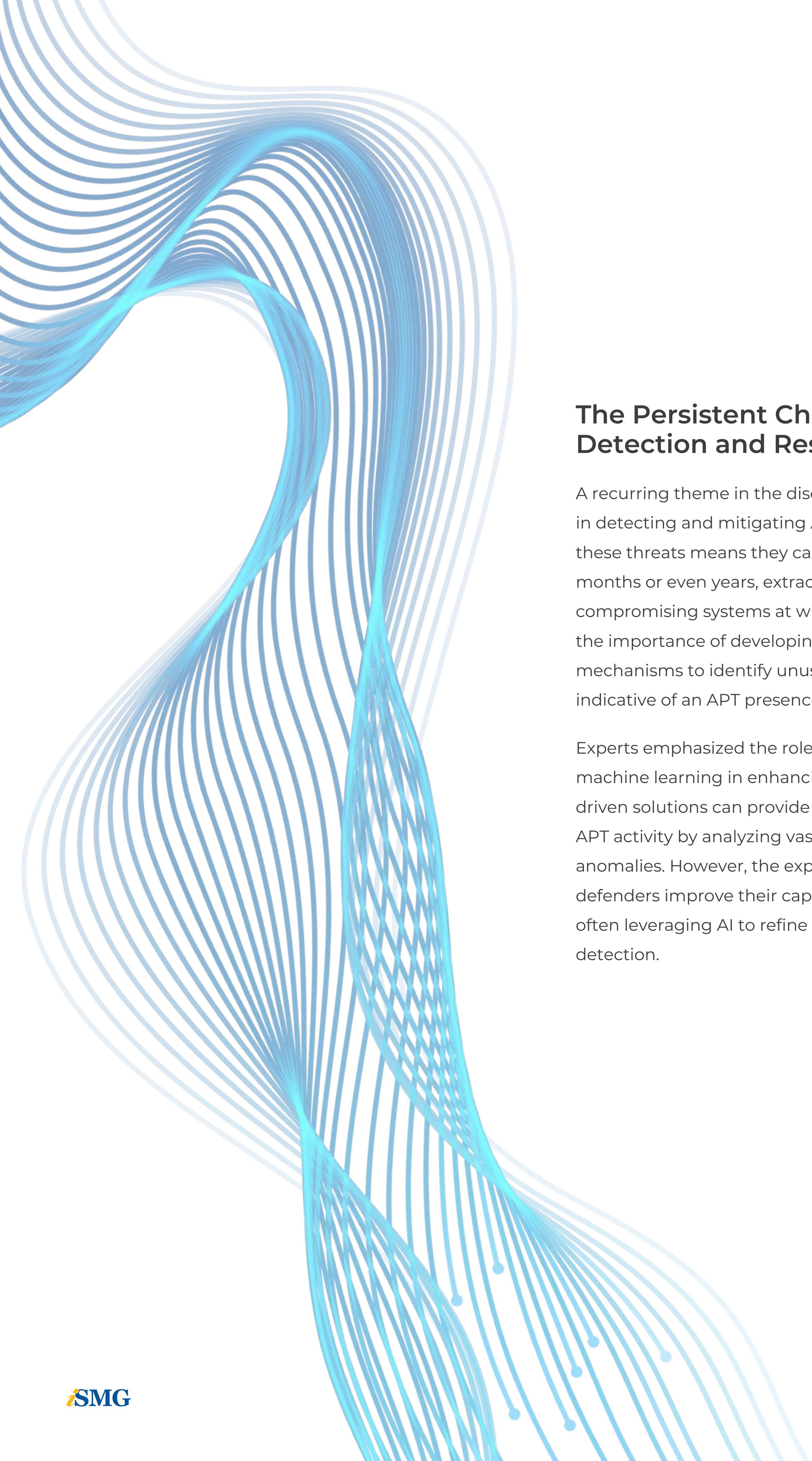
Robert Booker, chief strategy officer at HITRUST.

Nation-state actors are often backed by substantial government funding. They possess the capability to develop sophisticated malware, exploit zero-day vulnerabilities, and conduct operations that blend cyber and traditional espionage techniques. Due to their access to cutting-edge technology and skilled personnel, their capabilities significantly outstrip those of other threat actors.

"The adversary is more sophisticated than ever, more persistent, and more nefarious," said Rohit Ghai, CEO of RSA, adding that organizations must avoid simple mistakes to defend against APTs and nation-state actors. "You would never visit a doctor that does not wash his or her hands. So if you're making rookie mistakes, if you're not paying attention to cyber hygiene, that's a problem. We as a cybersecurity vendor community need to hold ourselves to a higher standard in terms of our own security posture and make sure we aren't making those rookie mistakes."

View the full interview here.

> The adversary is more sophisticated than ever, more persistent, and more nefarious.
>
> **Rohit Ghai**
> CEO, RSA



The Persistent Challenge of Detection and Response

A recurring theme in the discussions was the difficulty in detecting and mitigating APTs. The stealthy nature of these threats means they can operate undetected for months or even years, extracting valuable information and compromising systems at will. The interviews underscored the importance of developing robust detection mechanisms to identify unusual behavior patterns indicative of an APT presence.

Experts emphasized the role of artificial intelligence and machine learning in enhancing detection capabilities. AI-driven solutions can provide earlier warnings of potential APT activity by analyzing vast data and identifying anomalies. However, the experts also cautioned that as defenders improve their capabilities, so do the attackers, often leveraging AI to refine their tactics and avoid detection.

Conclusion

Addressing the threat of APTs and nation-state attacks requires a multifaceted approach. Organizations must invest in advanced cybersecurity technologies that leverage AI and machine learning to enhance detection and response capabilities. A concerted effort must also be made to develop and implement robust cybersecurity policies that promote international cooperation and information sharing.

Continuous education and training for cybersecurity professionals are essential to keeping pace with the evolving threat landscape. As nation-state actors become more sophisticated, so must the defenders who stand against them. By fostering a culture of vigilance and innovation, the cybersecurity community can better prepare for the challenges posed by APTs and nation-state threats.

Cybersecurity Frameworks

Cybersecurity frameworks play a crucial role in combating increasingly sophisticated cyber threats. Interviews with industry leaders highlight the necessity of robust, adaptable frameworks to maintain security in a rapidly evolving threat landscape.

A central theme this year was the need for continuous security assessments.. Traditional periodic reviews are insufficient due to the fast-evolving threat landscape. Aaron Shilts, President and CEO of NetSPI, emphasized that annual assessments are no longer effective. Organizations should adopt continuous security evaluations to keep pace with emerging threats. This shift requires moving from static defenses to dynamic, real-time monitoring and response capabilities.

Shilts also stressed the integration of specialized skill sets, especially in AI and machine learning. Securing AI models requires expertise beyond traditional cybersecurity training. Advanced mathematical skills are increasingly important in identifying and mitigating vulnerabilities within AI systems. This evolution in skill requirements reflects the broader trend of cybersecurity frameworks incorporating diverse and specialized knowledge to address new and complex threats.

Jon Miller, co-founder and CEO, Halcyon, discussed the complex landscape of cybercrime enforcement.

RSA CEO Rohit Ghai discussed the impact of new regulations and trends in identity and AI.

Brian Spanswick, CIO and CISO of Cohesity, and Tom Gillis, Senior Vice President and General Manager of Cisco Security Business Group, emphasized the importance of resilience in security strategies. Modern cybersecurity frameworks must balance proactive defense measures with robust recovery plans. Minimizing the impact of successful attacks through rapid response and recovery is as crucial as preventing breaches. This dual focus on defense and resilience forms the cornerstone of an effective cybersecurity framework.

Greg Touhill, Director of the CERT Division at Carnegie Mellon, underscored the importance of zero trust in creating secure environments. This approach assumes that threats could exist outside and inside the network, requiring stringent verification processes for all users and devices attempting to access resources. Implementing zero trust involves continuous authentication and validation, reducing the likelihood of successful breaches by limiting lateral movement within the network.

Conclusion

The discussions on cybersecurity frameworks paint a comprehensive picture of cybersecurity's current state and future directions. The critical elements include the shift toward continuous assessments, integration of advanced skills, balance of defense and resilience, adoption of zero trust principles, and importance of regulatory compliance and collaboration. Together, these components form the backbone of modern cybersecurity frameworks, equipping organizations to navigate and mitigate the complexities of today's threat landscape.

FRAMEWORKS AT A GLANCE

NIST CYBERSECURITY FRAMEWORK (CSF)

Provides guidance for organizations to assess and improve their ability to prevent, detect, and respond to cyberattacks.

ISO/IEC 27001

Provides guidance for organizations to assess and improve their ability to prevent, detect, and respond to cyberattacks.

CIS CONTROLS

A set of best practices developed by the Center for Internet Security to improve cybersecurity posture.

COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES)

A framework for IT governance and management practices, developed by ISACA.

PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD)

Security standards to ensure companies that handle credit card information maintain a secure environment.

FISMA (FEDERAL INFORMATION SECURITY MANAGEMENT ACT)

US law to enhance computer and network security within the federal government, requiring yearly audits.

NERC CIP (NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION CRITICAL INFRASTRUCTURE PROTECTION)

Requirements to secure assets necessary for operating North America's bulk electric system.

SOC 2 (SYSTEM AND ORGANIZATION CONTROLS)

Framework for managing customer data based on security, availability, processing integrity, confidentiality, and privacy.

CMMC (CYBERSECURITY MATURITY MODEL CERTIFICATION)

Assesses and enhances the cybersecurity posture of Defense Industrial Base contractors to protect controlled unclassified information (CUI).

Regulatory Compliance and Cybersecurity

Navigating the labyrinthine regulatory landscape is a complex endeavor at the intersection of compliance and cybersecurity. ISMG's interviews reveal a pervasive concern among experts about the dynamic and often conflicting nature of regulations, which create significant challenges for organizations striving to maintain robust cybersecurity postures while adhering to various legal mandates.

A recurring theme is the ever-evolving nature of regulatory requirements, which necessitates constant vigilance and adaptability from organizations. Experts emphasized that merely adhering to one set of regulations is insufficient due to modern compliance demands' global and multifaceted nature.

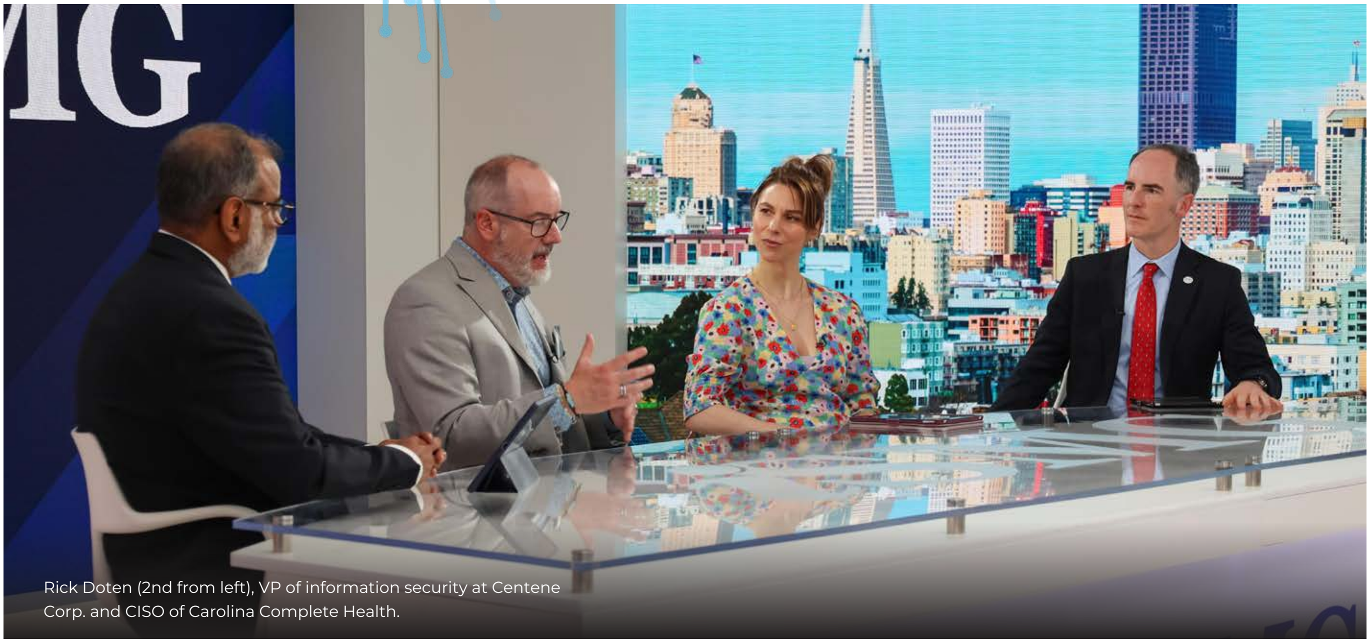
Organizations must track regulatory developments across multiple jurisdictions and understand how each applies to their operations. Adhering to just one framework is insufficient, as regulations frequently conflict or overlap, so organizations face increasingly intricate webs of compliance that they must navigate. Aligning security frameworks with emerging regulations as they arise requires a symbiotic relationship between legal and compliance teams and cybersecurity professionals.

> "We're seeing some really good examples like the LockBit takedown, where multi-country collaboration is the only way that we're going to be able to bring these networks down."

Alberto Yépez
Managing Director, ForgePoint Capital

Furthermore, integrating advanced technologies like AI into cybersecurity strategies presents opportunities and new regulatory challenges. Organizations need to ensure they are using AI responsibly, with transparency and accountability around how these tools are trained and deployed. Alberto Yépez, Managing Director, ForgePoint Capital, discussed the need for rigorous oversight and ethical standards in the deployment of AI technologies, including frequent evaluation for biases or blind spots. Yépez also emphasized the need for human oversight and the ability to double-check any actions taken autonomously by AI systems, a requirement that may go unfulfilled within organizations leveraging AI for speed.

International cooperation emerges as another vital component in the regulatory and cybersecurity discourse. Successful international efforts to dismantle cybercriminal networks underscore the necessity for a cohesive global approach. “We’re seeing some really good examples like the LockBit takedown, where multi-country collaboration is the only way that we’re going to be able to bring these networks down,” Yépez said, highlighting the critical role of cross-border collaboration in combating sophisticated cyber threats.



Rick Doten (2nd from left), VP of information security at Centene Corp. and CISO of Carolina Complete Health.

Conclusion

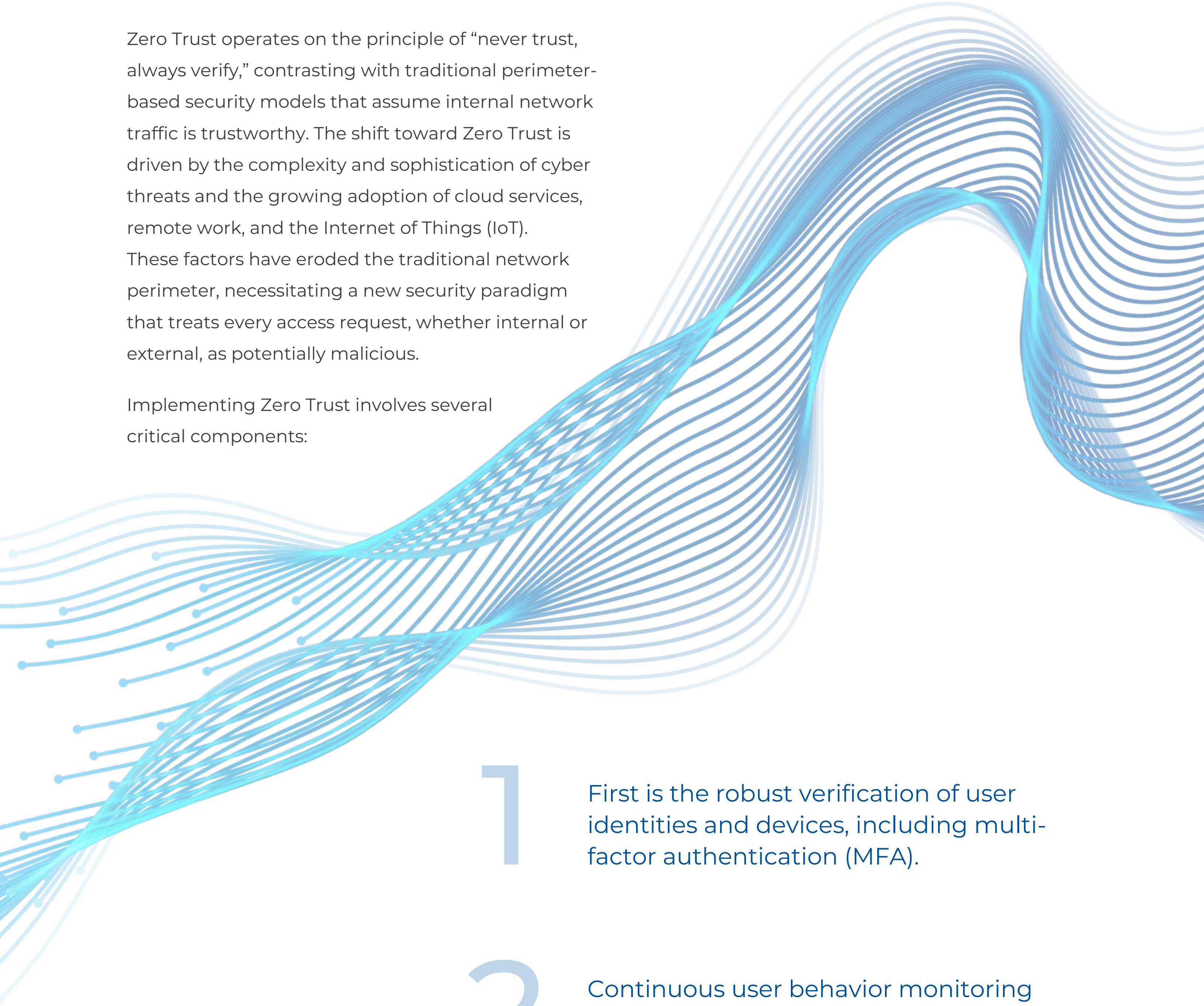
The narrative from these interviews paints a picture of a regulatory environment that is both a formidable challenge and a crucial ally in the fight against cyber threats. Organizations must navigate a complex landscape of overlapping and evolving regulations, align their security frameworks with these mandates, and leverage advanced technologies responsibly. Economic constraints and the need for international cooperation further complicate this task, underscoring the need for a multifaceted and adaptable approach to regulatory compliance and cybersecurity.

Zero Trust

Zero Trust has evolved from a theoretical model to an essential approach for modern enterprises. ISMG's interviews with thought leaders highlight the necessity and implementation of zero-trust principles to mitigate evolving cybersecurity threats.

Zero Trust operates on the principle of "never trust, always verify," contrasting with traditional perimeter-based security models that assume internal network traffic is trustworthy. The shift toward Zero Trust is driven by the complexity and sophistication of cyber threats and the growing adoption of cloud services, remote work, and the Internet of Things (IoT). These factors have eroded the traditional network perimeter, necessitating a new security paradigm that treats every access request, whether internal or external, as potentially malicious.

Implementing Zero Trust involves several critical components:



1 First is the robust verification of user identities and devices, including multi-factor authentication (MFA).

2 Continuous user behavior monitoring to detect anomalies that could indicate compromised credentials or insider threats.

3 Granular access control ensures users have the least privilege necessary to perform their tasks, minimizing the potential damage from any compromised account.

Zero Trust and Secure Enterprise Browsing

One significant application of Zero Trust is in secure enterprise browsing. Vivek Ramachandran, Founder and CEO of SquareX, noted that the browser is a primary vector for cyberattacks.

"The browser is the most important application but also the least understood and the least secure," said Ramachandran. "And this is really where attackers are now targeting employees, where spearfishing attacks are happening, where credentials get stolen, session hijacking. Because in today's hybrid work world employees are using the same work laptop to also do personal stuff." Organizations can significantly reduce the risk of malware, phishing, and other web-based threats by leveraging enterprise browsers that control and monitor browsing sessions.

> The browser is the most important application but also the least understood and the least secure.
>
> **Vivek Ramachandran**
> Founder and CEO, SquareX

View the full interview here.

View the full interview here.

Future Directions and Challenges

The Zero Trust model will continue to evolve with emerging threats and technological advancements. AI and ML will be critical in this evolution, providing new threat detection and response tools. However, successful implementation requires technological solutions and a cultural shift within organizations. This involves fostering a security-first mindset among all employees and ensuring continuous education and awareness about cyber threats and best practices.

"How do you explain the long-term strategy of Zero Trust to clients who think that maybe it's a one-and-done process or a single product?" asked On2IT CTO and Cofounder Lieuwe Jan Koning. "Zero Trust products do not exist. To make Zero Trust happen, you have to embrace it and then execute it time after time."

> How do you explain the long-term strategy of Zero Trust to clients who think that maybe it's a one-and-done process or a single product?
>
> **Lieuwe Jan Koning**
> CTO and Cofounder, On2IT

Conclusion

By implementing Zero Trust principles, organizations can create a more resilient security posture better equipped to handle the complexities and challenges of today's cyber threat landscape. Industry leaders' insights highlight the practical steps and considerations necessary for adopting Zero Trust, emphasizing the importance of continuous verification, advanced threat detection technologies, and strategic partnerships.

ISMG editors and reporters conducted more than 150 interviews at the RSA Conference this year.

IoT Security

The proliferation of connected devices has made IoT (Internet of Things) security a critical issue, combining technology with significant real-world impacts. The discussion around IoT security is marked by numerous challenges, innovations, and the ongoing pursuit of effective solutions.

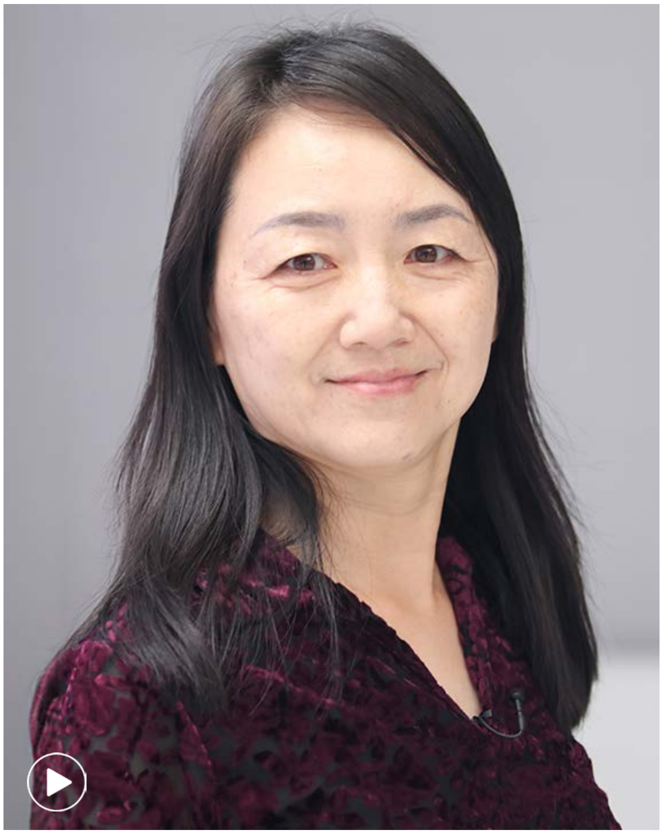
The proliferation of connected devices has made IoT (Internet of Things) security a critical issue, combining technology with significant real-world impacts. The discussion around IoT security is marked by numerous challenges, innovations, and the ongoing pursuit of effective solutions.

The vast array of IoT devices, from surveillance cameras to medical sensors, exhibit considerable differences in hardware, software, and operational frameworks. This variability makes standardizing security measures extremely challenging. Many IoT devices cannot install security agents or patches, rendering them susceptible to exploitation. The risks are amplified as these devices are often embedded in critical infrastructure, where a security breach could disrupt essential services and endanger lives.

Amit Sinha, CEO, DigiCert.

"IoT security is a big challenge because these devices are very different from traditional IT devices. Very often, you cannot even download the agent on these devices, and they don't have the capability to protect themselves," said Dr. May Wang, CTO of IoT Security, Palo Alto Networks.

The introduction of AI has been recognized as a transformative development in addressing IoT security challenges. AI's autonomous learning and adaptation capacity offers a scalable solution to IoT devices' extensive and diverse landscape. Advanced algorithms allow AI to automatically identify and classify devices, detect anomalies, and initiate protective measures. This capability is vital in environments where manual monitoring and intervention would be impractical due to the sheer volume of devices and the complexity of their interactions.



View the full interview here.

> IoT security is a big challenge because these devices are very different from traditional IT devices. Very often, you cannot even download the agent on these devices, and they don't have the capability to protect themselves.

Dr. May Wang
CTO of IoT Security, Palo Alto Networks

However, deploying AI in IoT security is not without its obstacles. A major concern is the accuracy and reliability of AI models. In cybersecurity, even minor inaccuracies can result in significant vulnerabilities. Therefore, precision AI, which emphasizes extreme accuracy, is necessary to ensure that security measures are effective and reliable. The challenge lies in adapting AI methodologies, typically designed for more predictable environments like natural language processing, to the unpredictable and dynamic field of cybersecurity.

Experts also highlighted the importance of supply chain security concerning IoT. A compromised component or a backdoor in manufacturing or software development can introduce difficult-to-detect vulnerabilities. The interconnected nature of global supply chains means that even a minor flaw in one component can have widespread consequences. This necessitates a comprehensive approach to supply chain security, incorporating measures like Software Bill of Materials (S-BOM) to enhance transparency and traceability.

Despite significant advancements, IoT security remains a continuously evolving battlefield. The rapid pace of technological innovation requires security solutions to adapt continually to new threats. This dynamic environment calls for a proactive approach, where continuous monitoring, regular updates, and adaptive security measures are essential.

Conclusion

IoT security is a complex and high-stakes domain that demands a multi-faceted approach. The integration of AI offers promising solutions but presents new challenges that must be addressed with precision and foresight. Supply chain security adds another layer of complexity, necessitating transparency and rigorous oversight. As the landscape of connected devices continues to grow, our efforts to secure them must also expand, ensuring that the benefits of IoT are not overshadowed by its risks.

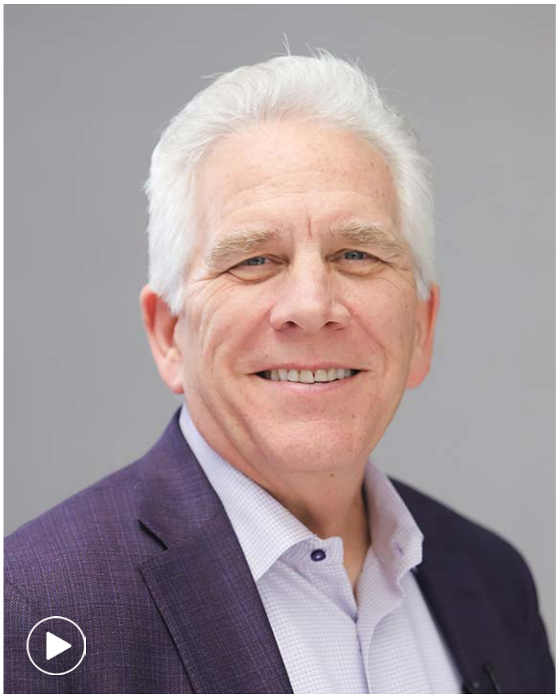
Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly and former Director Chris Krebs (center) discussed how businesses can defend themselves against advanced global cyber threats.

Cybersecurity For Remote Work

The shift to remote work has fundamentally altered how organizations approach security, demanding new strategies and tools to protect distributed workforces. Insights from ISMG's RSAC 24 interviews reveal several critical aspects of cybersecurity for remote work, including the importance of visibility, the evolving nature of threats, and the need for robust endpoint security.

One of the recurring themes in the discussions is the need for enhanced visibility into remote work environments. Organizations must comprehensively understand the applications and data flows within their networks. This visibility extends to knowing what apps are being used, who is using them, and what data is being transmitted. This visibility is crucial for identifying sensitive data and ensuring it remains secure, even as it moves through various applications and devices.

"The challenges most organizations face today is, frankly, they don't have a good handle on who has access to what," said Mark McClain, Founder, and CEO of SailPoint. "Now, everyone is becoming more aware in a world of mobile and cloud that they're not protected solely by a strong perimeter."



View the full interview here.

> The challenges most organizations face today is, frankly, they don't have a good handle on who has access to what.
>
> **Mark McClain**
> Founder and CEO, SailPoint

Endpoint Security Challenges

Another critical issue is the security of endpoints used by remote workers. In today's hybrid work environment, employees often use the same devices for work and personal activities. This convergence creates new vulnerabilities, as attackers can exploit personal browsing habits to infiltrate corporate networks. Organizations need more sophisticated endpoint security solutions that offer real-time protection and visibility into browser activities. The lack of visibility into browser-based threats was highlighted as a significant gap, with attackers leveraging techniques like session hijacking and credential theft to compromise systems.

Identity and Access Management

Managing identities and access in a remote work setting presents its own set of challenges. Maintaining a robust identity governance framework with employees, contractors, and partners accessing systems from various locations is essential. This framework must account for human and non-human identities, such as machine accounts and intelligent devices. Integrating multi-factor authentication (MFA) and continuous monitoring of identity activities are vital components of a comprehensive identity management strategy.

Strategic Recommendations

To address these multifaceted challenges, organizations should adopt a multi-layered security strategy that encompasses the following elements:

1. **Enhanced Visibility:** Implement tools that provide comprehensive visibility into all aspects of the network, from applications to data flows

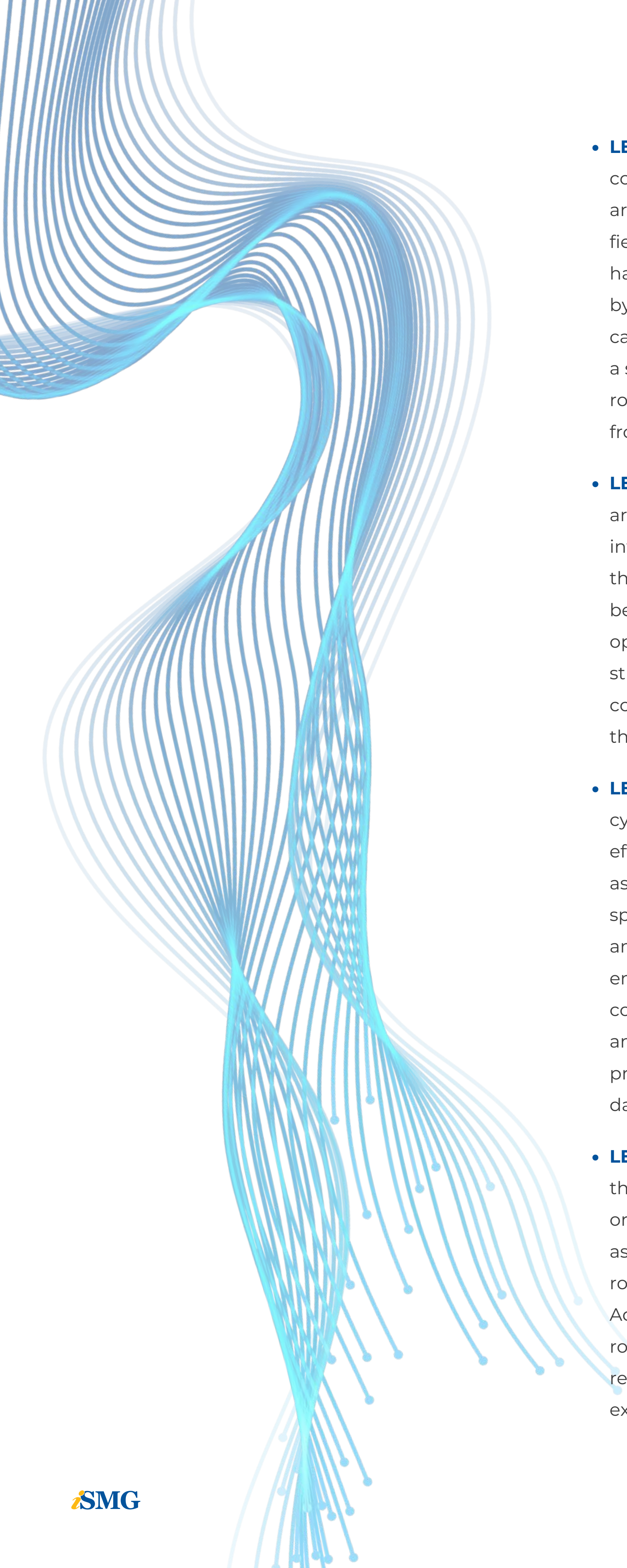
2. **Advanced Threat Protection:** Utilize AI and machine learning to detect and respond to sophisticated threats targeting remote work environments.

3. **Robust Endpoint Security:** Invest in endpoint security solutions that offer real-time monitoring and protection against browser-based threats.

4. **Comprehensive Identity Management:** Strengthen identity governance frameworks to manage human and non-human identities effectively.

5. **Regulatory Compliance:** Continuously assess and update compliance practices to align with evolving regulations and industry standards.

Lessons Learned



- **LESSON 1:** The Cybersecurity Pulse Report provides a comprehensive analysis of the transformative impact of artificial intelligence (AI) and machine learning (ML) on the field of cybersecurity. These cutting-edge technologies have revolutionized the way we approach security by enabling real-time threat detection and response capabilities. However, their dual-use nature also presents a significant challenge, as it is imperative to implement robust security measures to prevent these powerful tools from being exploited for malicious purposes.

- **LESSON 2:** In the realm of cloud security, the stakes are particularly high. As attacks on complex cloud infrastructures become more frequent and sophisticated, the need for cloud-native security tools has never been more pressing. Enhanced visibility into cloud operations, robust data protection strategies, and strategic partnerships with trusted providers are all crucial components for defending against the evolving threats that target cloud environments.

- **LESSON 3:** The implementation of comprehensive cybersecurity frameworks is essential for maintaining effective defenses in this dynamic landscape. Continuous assessments of security postures, the development of specialized skills among cybersecurity professionals, and the adoption of zero trust principles are all key to ensuring that defenses remain robust and resilient. In the context of remote work environments, the ability to verify and manage user identities effectively is paramount to preventing unauthorized access to sensitive systems and data.

- **LESSON 4:** Ransomware continues to be a pervasive threat, and defending against it remains a top priority for organizations worldwide. Advanced technologies, such as AI-driven behavioral detection systems, play a vital role in identifying and mitigating ransomware attacks. Additionally, cyber storage solutions that incorporate robust backup and recovery capabilities are essential for recovering from attacks, particularly in the face of double extortion ransomware tactics.

- **LESSON 5:** Operational technology (OT) security presents a set of unique challenges due to the convergence of information technology (IT) and OT systems. Specialized security measures tailored to the specific needs of OT environments, enhanced visibility tools to monitor system activities, adherence to regulatory compliance standards, and the recruitment and training of skilled personnel are all essential for managing the risks associated with OT systems.

- **LESSON 6:** Data privacy and protection challenges continue to grow as the volume and sensitivity of data increase. AI and ML-driven data discovery and classification tools are becoming increasingly important for identifying and protecting sensitive information. Immutable backups and multi-layered encryption techniques are also critical for safeguarding data against unauthorized access and mitigating the impact of ransomware attacks.

- **LESSON 7:** The proliferation of the Internet of Things (IoT) devices and the shift toward remote work have significantly expanded the attack surface that organizations must defend. A human-centric, zero trust cybersecurity architecture is required to address these challenges effectively. AI-driven solutions offer scalable protection for IoT ecosystems, but ensuring the precision and reliability of these solutions is of utmost importance. Additionally, the complexity of supply chain security has grown, necessitating increased transparency and oversight to secure the interconnected networks of suppliers and partners.

- **LESSON 8:** AI and ML also play a pivotal role in enhancing threat detection and response capabilities. These technologies enable the real-time analysis and prioritization of threats, allowing organizations to respond swiftly and effectively. Automated threat hunting, comprehensive visibility across the digital environment, strategic partnerships with industry leaders, and the deployment of cloud-native security measures are all components of a proactive defense strategy.

- **LESSON 9:** Navigating the complex landscape of global regulations requires a high degree of vigilance and adaptability. Integrating technological solutions with policy responses and fostering international cooperation are essential for combating nation-state threats and dismantling sophisticated cybercriminal networks.
- **LESSON 10:** Organizations must now prioritize enhanced visibility into remote operations, robust endpoint security to protect devices outside the traditional network perimeter, and comprehensive identity management to ensure that only authorized users can access critical resources. A multi-layered approach encompassing advanced threat protection, real-time monitoring, and adherence to compliance standards is crucial for addressing the unique security challenges posed by remote work.

In conclusion, to build resilient security postures capable of withstanding complex and evolving threats, organizations must embrace advanced technologies, implement comprehensive cybersecurity frameworks, and engage in international collaboration. By doing so, they can ensure that their defenses are not only robust but also adaptable to the ever-changing threat landscape.

Contributors

List of Interviews Contributing to This Report

Bob Ackerman Founder and Managing Director, AllegisCyber Capital

Andrew Almeida Partner, Thoma Bravo

Alexander Antukh CISO, AboitizPower

Curt Aubley COO and Chief Product Officer, Deepwatch

Alex Bazhaniuk Co-Founder and CTO, Eclypsium

Brennan P Baybeck ISACA Board Vice Chair and SVP & CISO for Customer Success Services, Oracle Corporation

Amir Ben-Efraim CEO, Menlo Security

Joseph Blankenship Research Director, Forrester

Stas Bojoukha Founder and CEO, Compyl

David Bradbury Chief Security Officer, Okta

Ray Brancato CEO, Tufin

Danny Brickman Co-Founder and CEO, Oasis Security

Brad Brooks CEO, Censys

Edgard Capdevielle President and CEO, Nozomi Networks

Dawn Cappelli Head of OT-CERT, Dragos

Alicja Cade Director Financial Services Office of the CISO, Google Cloud

Rich Campagna SVP Products, Palo Alto Networks

Sébastien Cano SVP for Cloud Protection and Licensing, Thales

Charles Carmakal Chief Technology Officer, Mandiant

Jay Chaudhry Founder Chairman & CEO, Zscaler

Amit Chhikara Principal in Deloitte Advisory's Cyber Risk and Privileged Access Management Practices, Deloitte

Alaina Clark Assistant Director, CISA

Edna Conway CEO & Founder, EMC Advisors

Barbara Cosgrove VP Chief Privacy Officer, Workday

Art Covington Investment Committee Chair, SYN Ventures

Sam Curry VP & CISO, Zscaler

Pieter Danhieux Co-Founder Chairman and CEO, Secure Code Warrior

Dror Davidoff Co-Founder and CEO, Aqua Security

Dave DeWalt CEO & Founder, NightDragon

Thom Dekens Chief Business Officer At-Bay & General Manager
At-Bay Security, At-Bay

Sumit Dhawan CEO, Proofpoint

Lior Div CEO & Co-Founder Okami-AI and Former Co-Founder, Cybereason

Alex Doll Founder & Managing General Partner, Ten Eleven Ventures

Rick Doten Founder VP Information Security Centene Corp & CISO Carolina Complete Health, Centene Corp

Casey Ellis Founder & Chief Strategy Officer, Bugcrowd

Brian Essex Executive Director US Software Equity Research, JP Morgan

Lou Fiorello VP & GM Security Products, ServiceNow

Hamza Fodderwala Executive Director US Software Equity Research, Morgan Stanley

James Foster Founder & CEO, ZeroFox

Brian Fox Co-Founder & CTO, Sonatype

Rohit Ghai CEO, RSA

Tom Gillis SVP & GM of the Security Business Group, Cisco

Vinayak Godse CEO, Data Security Council of India DSCI

Will Gragido Head of Product Management & Intelligence, NetWitness

JJ Guy CEO, Sevco Security

Kyle Hanslovan CEO, Huntress

Raaz Herzberg CMO & VP Product Strategy, Wiz

Alex Hesterberg CEO, Superna

Niloofr Razi Howe Chair of the Board of Directors, Pondurance

J Trevor Hughes CEO & President, IAPP

Floor Jansen Deputy Head of National High Tech Crime Unit, Netherlands Police

Datta Junnarkar CIO Maritime, Boeing

Rick Kaun VP Solutions, Verve Industrial Protection

Rahul Kashyap VP GM & CISO, Arista Networks

Daniel Kennedy Research Director, 451 Research

Schlomo Kramer Co-Founder & CEO, Cato Networks

Subra Kumaraswamy CISO, Visa

Jay Leek Managing Partner, SYN Ventures

Yoav Leitersdorf Managing Partner, YL Ventures

Joe Levy President & Acting CEO, Sophos

Piyusk Malik Chief Digital & Transformation Officer, Veridic Solutions

Mihir Maniar VP of Products - ISG Edge & Managed Security Services, Dell Technologies

Paul Martini CEO, iboss

Mark McClain Founder & CEO, SailPoint

Leigh McMullen Distinguished VP Analyst & Gartner Fellow, Gartner

Dave Merkel Co-Founder and CEO, Expel

Marten Mickos CEO, HackerOne

Sanjay Mirchandani President and CEO, Commvault

Mike Nichols VP of Product Management Security, Elastic

Wendy Nather Head of Advisory CISOs, Cisco

Sarfraz Nawaz Product Executive in Residence, Mighty Capital

Nayaki Nayyar CEO, Securonix

Herain Oberoi General Manager Data Security Compliance and Privacy, Microsoft

Phil Owens VP of Customer Solutions, Stamus Networks

Jason Passwaters CEO & Co-Founder, Intel 471

Jeetu Patel EVP & GM Security & Collaboration, Cisco

Ryan Permeh Founder & CEO Cylance Now BlackBerry and Operating Partner, SYN Ventures

Chris Pierson CEO & Founder, BlackCloak

Alex Pinto Associate Director for Threat Intelligence, Verizon

Mary Lou Prevost Group VP US State Local Government & Education, Splunk

Meerah Rajavel Chief Information Officer, Palo Alto Networks

Niloofar Razi Chair of the Board of Directors, Pondurance

Clay Rogers VP Global Strategic Alliances, CyberArk

Bradon Rogers Chief Customer Officer, Island

Clar Rosso CEO, ISC2

Mark Ryan Director of Amazon Security, Amazon

Christian Schnedler Managing Director Cyber Practice Lead, WestCap

John Scimone President & Chief Security Officer, Dell Technologies

Masha Sedova VP Human Risk Strategy, Mimecast

Rama Sekhar Partner, Menlo Ventures

Dharshan Shanthamurthy CEO, SISA

John Shier Field CTO Commercial, Sophos

Aaron Shilts President and CEO, NetSPI

Jeff Shiner CEO, 1Password

Sid Shibiraj Group Product Manager, Google Cloud

Bupil Sinha Co-Founder Chairman and CEO, Rubrik

Amit Sinha CEO, DigiCert

Kevin Skapinetz Vice President of Security Strategy, IBM

Stu Sjouwerman CEO, KnowBe4

Stu Solomon CEO, HUMAN

Suzanne Spaulding Former Undersecretary, Department of Homeland Security

Brian Spanswick CIO & CISO, Cohesity

Dan Streetman CEO, Tanium

Joe Sullivan CEO, Ukraine Friends

Aravind Swaminathan Global Co-Chair Cybersecurity and Data Privacy, Orrick Herrington
& Sutcliffe LLP

Dean Sysman Co-Founder and CEO, Axonius

Sumedh Thakar President & CEO, Qualys

Greg Touhill Senior Director of Cybersecurity Services, Venable

Brandon Traffanstedt Senior Director Field Technology Office, CyberArk

Bob VanKirk President & CEO, SonicWall

Christophe Van de Weyer CEO, Telesign

Phil Venables VP CISO, Google Cloud

Sheetal Venkatesh Senior Director Product Management, Cohesity

Dr. May Wang CTO Internet of Things Security, Palo Alto Networks

Heather West Senior Director Cybersecurity & Privacy Services, Venable

Dr. Clarence Worrell Sr Data Scientist, CERT Division of Carnegie Mellon University's Software Engineering Institute

Chris Wysopal Co-Founder & Chief Technology Officer, Veracode

Alberto Yepez Managing Director, Forgepoint Capital

Elia Zaitsev Chief Technology Officer, CrowdStrike

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CAREERS INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

CU INFO SECURITY® Just for Credit Unions · Data Breach® Prevention. Response. Notification. TODAY · infoRisk® TODAY · AIToday.io · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QG MEDIA

iSMG