

Think Exponentially

The Secure AI Readiness Playbook

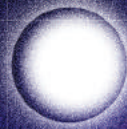
Preparing your enterprise for the transformational impacts of GenAI.

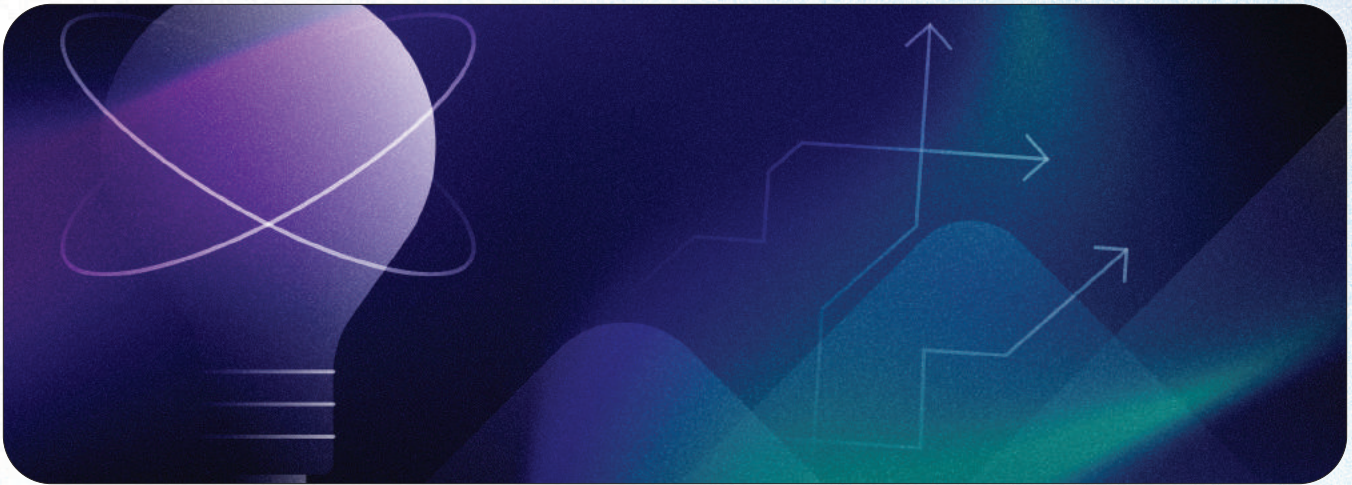
Dean Fantham and Bob Moore,
Wipro Cybersecurity and Risk Services

Moving Away From Linear Thinking	2
Applying Exponential Thinking	6
How GenAI Improves Productivity	11
How GenAI Improves The User Experience	13
GenAI in Cyber Defense	16
Key Takeaways	18

This eBook is a core component of Cybersecurity in the Era of AI, a joint communications campaign by Wipro Cybersecurity and Risk Services (CRS) and Microsoft focusing on the exponential productivity gains expected from Generative AI (GenAI) and the security challenges enterprises face in adopting this new technology.

Moving Away From Linear Thinking





“We believe that enterprise leaders can learn to think exponentially and prepare for the biggest opportunities in GenAI. In the realm of cybersecurity, thinking exponentially means altering approaches to the data, the systems, and organizational structures to secure GenAI at speed and scale. Thinking exponentially is as much a model as it is a mindset.”

Never has a consumer tech category been adopted so swiftly – nor with so much trepidation – as GenAI. One of the reasons for its rapid growth is that it is a digitally networked consumer technology. Like practically every consumer technology, GenAI grows exponentially.

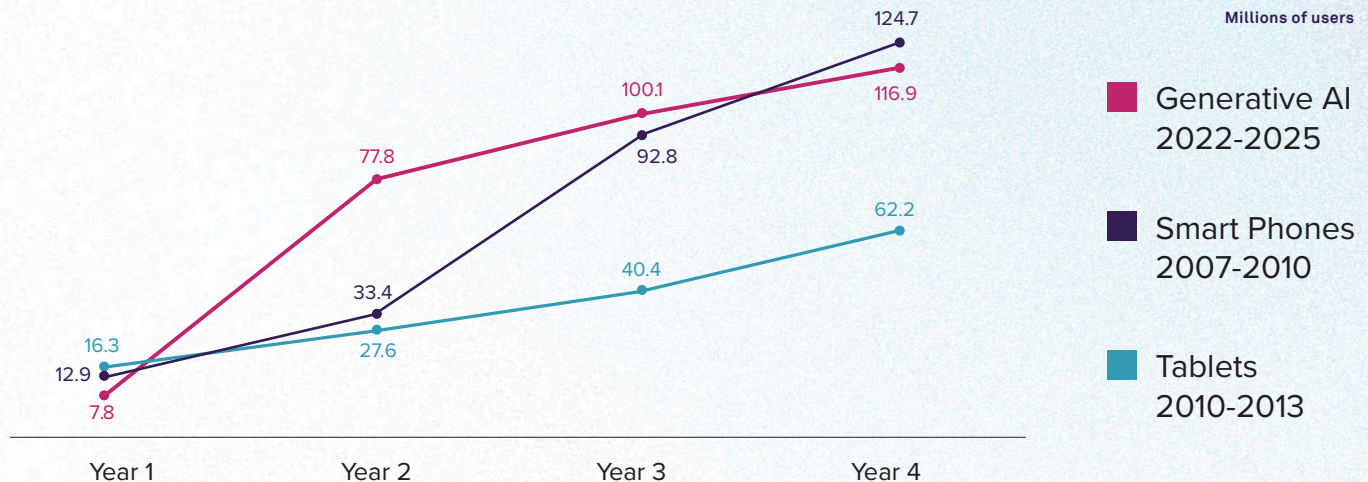
After 18 months of meteoric growth, the promise of GenAI in enterprises is coming into sharper focus. Businesses worldwide are looking at the potential for exponential gains in productivity and user experience. These gains will likely be dramatic, and in many cases, transformational.

But there’s a problem. While the adoption of digital technologies grows exponentially, people tend to think linearly. As inventor and technologist Ray Kurzweil observed, this is why civilization

persistently fails to predict how quickly new technologies come to market. It may also be the reason why many businesses are slow to start seriously preparing for an AI future.

It’s worth noting that Kurzweil overcame his own difficulties in predicting the future by teaching himself to “think exponentially.” We believe that business leaders can learn to alter the way they think about cybersecurity, transitioning from a systems approach to a new way of viewing the organizational structure.

TECHNOLOGY ADOPTION CURVE COMPARISON



We are using processes for tech selection and adoption that were established 10 to 15 years ago. The landscape has changed but our structures and processes have not evolved. While we could get by with these processes in a linear IT world where change is incremental, they don't work well in the exponential world of AI where change comes rapidly. The exponential thinking required to evolve these processes is as much a model as it is a mindset, and it must get buy-in from leaders throughout the enterprise as well as critical industry partners to maintain a competitive technological edge.

LESSONS FROM LAGGING ZERO TRUST ADOPTIONS

An example of how easy it is for an enterprise to struggle in adopting new technology when relying

on the linear model of thinking is Zero Trust — the very foundation of secure AI and one of the top three areas for cybersecurity investment today. Even though it is a solid framework for securing cloud centric IT, enterprise Zero Trust adoption is lagging significantly behind GenAI adoption.

This is alarming given that the robust cybersecurity measures inherent in Zero Trust architecture are essential for the safe and effective implementation of GenAI technologies.

Traditionally, Zero Trust is built on the principle of "never trust, always verify," requiring rigorous identity verification, least privilege access, and continuous monitoring. With GenAI, these principles are being enhanced and revolutionized, offering more sophisticated and effective ways to secure digital environments.

TOP SECURITY INVESTMENT PRIORITIES

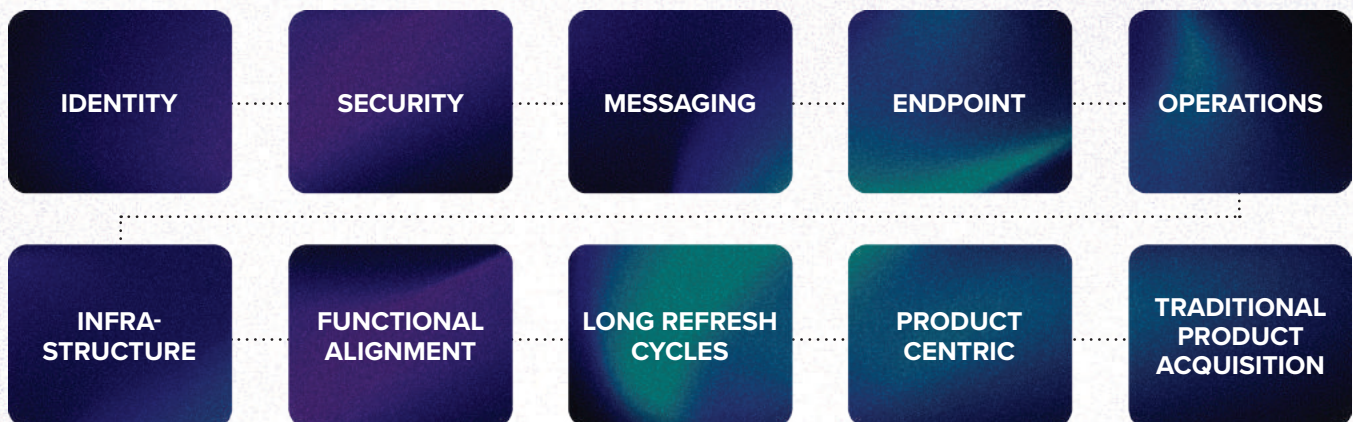


Source - 2023 Wipro State of Cybersecurity Report (SOCR)

Effective Zero Trust requires end-to-end visibility and full management of identities and assets. To do this, organizations need to think differently about tech adoption and change adoption processes. In many cases, individual products are being deployed

claiming “Zero Trust.” But unless the IT environment is integrated and sharing signals and implementing controls across the user lifecycle, these piecemeal efforts are merely incremental steps lacking the promise of reaching true Zero Trust.

LINEAR MODEL



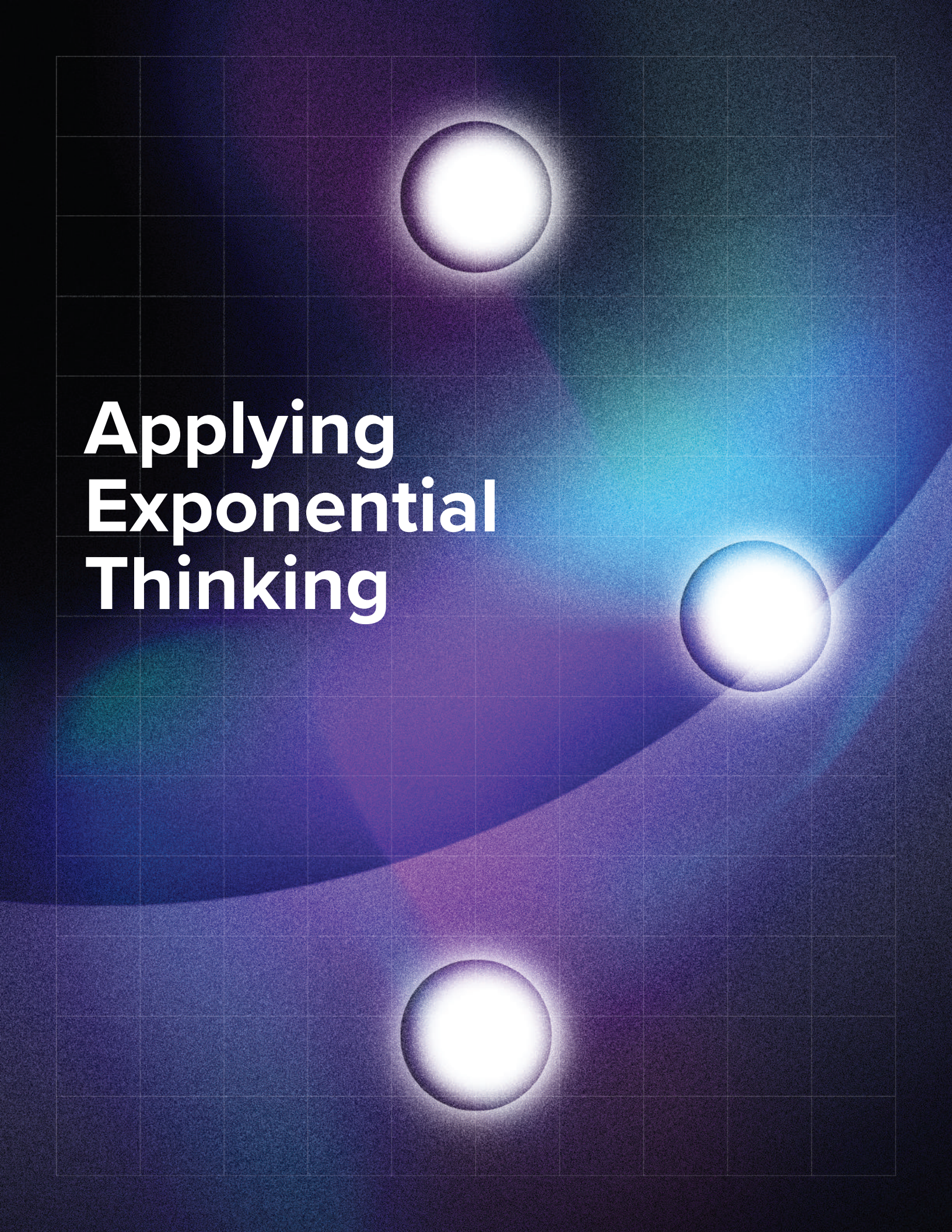
The linear model is functionally focused and uses traditional technology adoption processes. While this model has been effective, it's becoming a blocker to securing the modern environment with new technologies.

Why is GenAI being adopted so quickly while Zero Trust continues to lag? We believe it's related to existing organizational structures.

GenAI is relatively greenfield and it is creating exciting

new executive positions. Zero Trust does not create new executive positions, it costs money (with the promise of ROI), and most importantly it requires us to think differently about selecting and deploying technology.

Our legacy processes of technology evaluation, adoption, deployment, and lifecycle are not appropriate for enabling an enterprise-level integrated solution like Zero Trust. Enterprises that are able to implement an end-to-end Zero Trust architecture are better prepared to secure GenAI.

The background features a dark blue-to-purple gradient with a fine grid pattern. Three bright, glowing white spheres are positioned at the top, middle-right, and bottom. A curved, light-colored line sweeps across the lower half of the image.

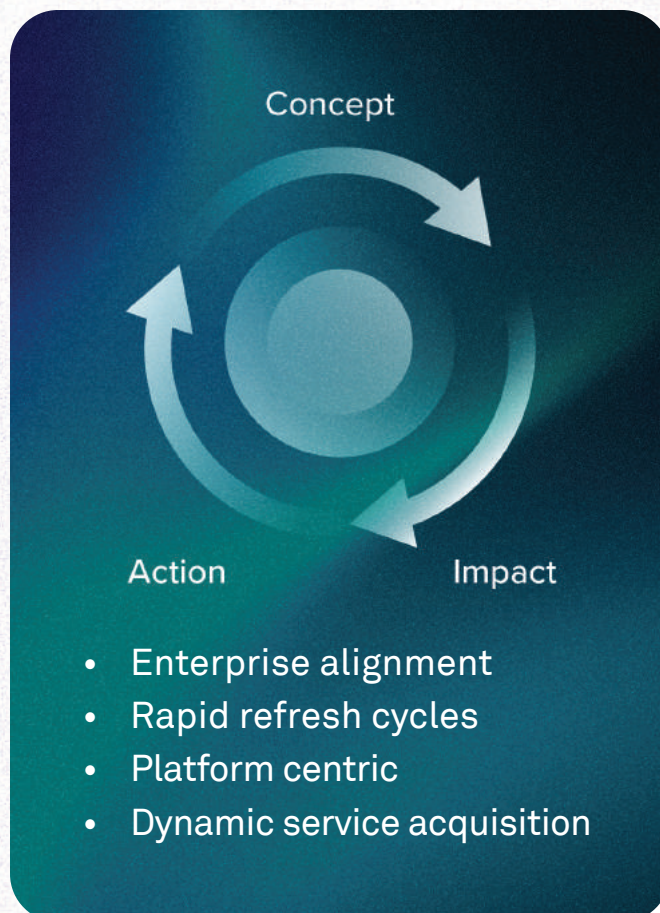
Applying Exponential Thinking

Organizations realize that while GenAI offers immense potential, its secure deployment is crucial, and this requires embracing Zero Trust principles. But we can't rely on our current linear processes to do this. We must think differently about technology adoption if we want to match the speed of GenAI. There is urgency in transitioning to exponential thinking. According to Microsoft, we are now in the operational phase of AI. This means the time to secure the environment is nearing an end.

“We’ve come to the hard part of any tech disruption: moving past experimentation to business transformation. Just as we saw with the advent of the internet or the PC, business transformation comes with broad adoption. Organizations that apply AI to drive growth, manage costs, and deliver greater value to customers will pull ahead.”

AI at Work Is Here. Now Comes the Hard Part (Microsoft)

EXPONENTIAL MODEL



In his book *Banking on Change*, James Robert Lay describes exponential thinking this way:

- **Perspective is Context + Framing, then**
- **Exponential Perspective is (Context + Framing) (Reframing)¹**

While this reframing is most likely happening with GenAI initiatives in many organizations, it has yet to reach the technology selection and deployment process which largely remains stuck in the linear thinking model.

RESTRUCTURING THE IT ORGANIZATION

As our Zero Trust example showed, the current organizational structure built on functional ownership is a roadblock to exponential thinking. These functional silos inhibit the cross organizational collaboration needed to achieve end-to-end signals and controls. We recommend a rethinking of technology acquisition and deployment, moving from a linear model to an exponential model. **Here are five best practices to enable this approach.**

1

Shift commodity workloads to vendor platforms

In the past there were important distinctions between products in the various categories and the role of the IT department was to evaluate, make acquisitions and attempt to make things work together. Now the reality is that much of these workloads are a commodity, and the job of IT should be to configure the vendor's platform. Any system, business function or process that has been around for more than 10 years is a commodity.

Shifting these commodity workloads to a platform vendor increases the exponential thinking of your IT organization. You are freeing yourself from the bondage of your own technology and processes and are acquiring exponential thinking as a service from companies that are structured to think and act quickly. In many cases, this can minimize the need for RFPs, Q&As and short lists.

Non-commodity systems (think new tech like GenAI and machine learning) still require custom development and integration.

2

Create a Zero Trust Governance Group

To drive a successful organizational shift towards exponential thinking and enhanced cyber defense, it is imperative to establish a Zero Trust governance group, empowered directly by the CEO. This group should consist of both functional and enterprise leaders, ensuring a holistic approach to security that transcends departmental boundaries. Giving this group budgetary control is crucial for enabling swift decision-making and resource allocation on the journey to a robust Zero Trust strategy.

Members of this governance group must share a unified vision that prioritizes the enterprise's overall benefit above individual functional optimization. This alignment ensures that all actions and policies adopted by the group serve the broader goals of the organization, fostering a culture of collaboration and shared

responsibility in maintaining stringent security standards.

The group should adopt a comprehensive strategy and actionable roadmap for implementing Zero Trust principles. This includes setting clear milestones, defining metrics for success, and establishing protocols for continuous monitoring and improvement. With a well-defined plan, the organization can systematically address vulnerabilities and enhance its security posture over time.

Finally, it is essential for the Zero Trust governance group to align closely with business partners on direction, AI policy, and frameworks. This collaboration ensures that security measures are integrated seamlessly with business operations, enabling innovation while safeguarding critical assets.

By working together, the organization and its partners can build a resilient ecosystem capable of

withstanding the evolving landscape of cyber threats.

Establishing a dedicated Zero Trust governance group united by a common purpose and equipped with the necessary

authority and resources is fundamental to achieving a secure and agile enterprise defense strategy. Combined with a clear roadmap and collaborative approach, this will position the organization to effectively counter cyber threats and drive sustained business success.

3

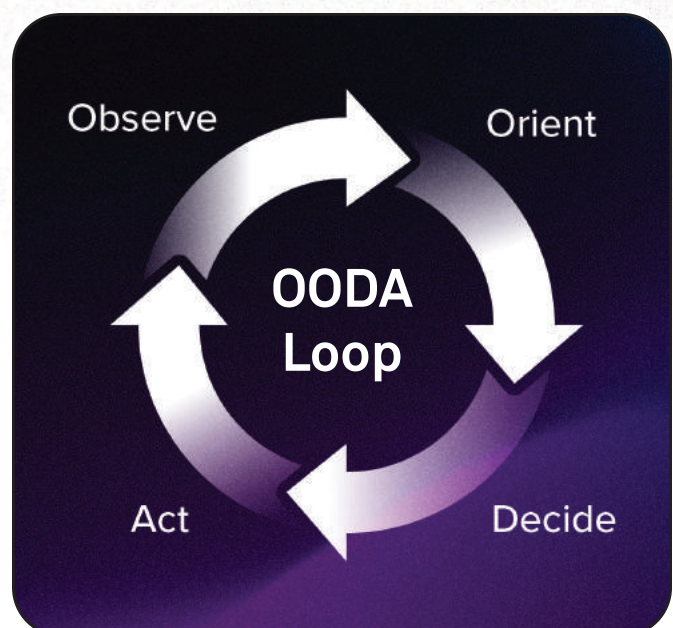
Reform the business-as-usual model

The aim here is to implement new processes, including continual re-evaluation of the environment, situational awareness, and business, threat, and group responsiveness metrics. Closely integrate with your platform provider since their exponential thinking is now yours. Include your managed service providers in this effort and challenge them to incorporate the same processes and visions. Keep in mind the organizational shift that businesses need to undertake to meet the promise of GenAI is just as important as the technology shift.

The dynamic and interactive nature of AI systems requires a more agile and proactive security framework. This is where concepts like the OODA Loop (Observe, Orient, Decide, Act) and the Vitality Score come into play. These approaches emphasize continuous monitoring, rapid adaptation, and proactive threat mitigation. The OODA Loop encourages organizations to observe their AI systems continuously, orient themselves with the latest threat intelligence, swiftly decide on appropriate security measures, and act decisively

to counteract threats. The Vitality Score provides a measure of an organization's resilience and ability to adapt to changing threats, highlighting areas for improvement and ensuring ongoing preparedness.

By rethinking cybersecurity through frameworks like the OODA Loop and the Vitality Score, organizations can enhance their resilience and agility in the face of AI-driven threats. Embracing these new paradigms will ensure that the benefits of AI can be harnessed safely and securely, paving the way for a future where AI-driven productivity and innovation can thrive without compromising security.



4

Understand AI Model Data

As GenAI becomes more integrated into various applications, the nature of data it uses and generates is evolving, necessitating a fresh approach to cybersecurity. Traditional data paradigms are being challenged, and the new kinds of data that AI uses, including model data and prompts, require innovative strategies to ensure security and privacy.

availability. Any compromise in this data can lead to biased, inaccurate, or malicious outputs from the system. For instance, adversarial attacks can introduce subtle manipulations into training data, causing GenAI models to behave unpredictably or make incorrect decisions. Therefore, robust security measures, including advanced encryption, secure data storage, and rigorous access controls, are essential to safeguard the data.

“Large language models have the potential to transform cyber defense for next-gen cybersecurity. Microsoft’s researchers and applied scientists are exploring many scenarios for LLM application in cyber defense.”

Microsoft Digital Defense Report 2023

GenAI model data encompasses the datasets used to train, validate, and test AI models. This data is crucial as it directly influences the performance and accuracy of the systems. Unlike conventional datasets, GenAI model data often includes vast, diverse, and complex information, ranging from structured datasets like spreadsheets to unstructured data such as text, images, and videos. The volume and variety of this data presents unique challenges for cybersecurity.

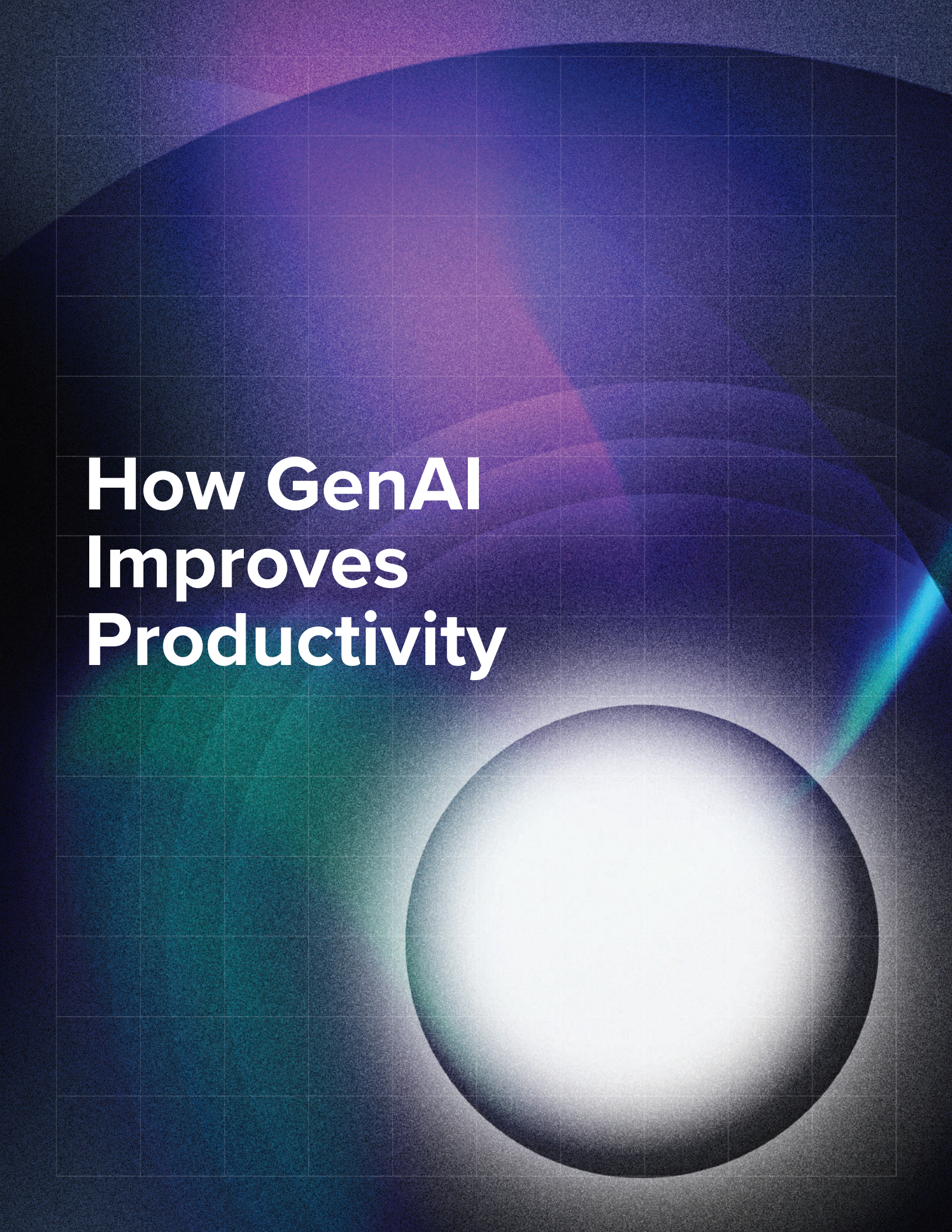
Protecting model data involves ensuring its integrity, confidentiality, and

5

Secure GenAI Prompts

Prompts are another critical component in the functioning of AI, particularly in natural language processing (NLP) models like OpenAI's GPT-4. Prompts are the inputs given to AI systems to elicit desired responses. They can range from simple questions to complex instructions and significantly impact the quality and relevance of GenAI output.

The security of prompts is vital as they can inadvertently reveal sensitive information or be exploited for malicious purposes. For example, malicious actors can craft prompts to extract confidential data or manipulate AI systems into generating harmful content. Ensuring the security of prompts involves not only protecting them from unauthorized access but also implementing filters and checks to prevent the use of harmful or deceptive inputs.

The background features a dark blue and purple gradient with a subtle grid pattern. A large, glowing white sphere is positioned in the lower right quadrant, casting a soft light. A bright blue and green light streak enters from the right side, illuminating the scene.

How GenAI Improves Productivity



ENHANCING EFFICIENCY THROUGH AUTOMATION

GenAI automates routine tasks, freeing up human resources for strategic activities. In customer service, GenAI-powered chatbots can handle numerous inquiries, improving efficiency and customer satisfaction. In manufacturing, GenAI can optimize production and supply chain management, leading to significant cost savings.



DRIVING INNOVATION

GenAI accelerates innovation by analyzing large datasets to uncover insights and suggest new products or features. This capability helps companies bring products to market faster and more effectively, keeping them ahead of competitors.



IMPROVING DATA-DRIVEN DECISIONS

GenAI excels in processing vast amounts of data, providing insights that inform better decision-making in marketing, sales, and operations. This leads to improved outcomes and a stronger competitive edge.



EXPANDING AGILITY

In turbulent markets, agility is crucial. GenAI enables enterprises to quickly adapt to new information and changing conditions, particularly in areas like cybersecurity. This proactive approach helps anticipate and mitigate risks.

The background features a dark blue to black gradient with a fine grid pattern. Two large, glowing spheres are prominent: one in the upper right and another in the lower right. The spheres have a bright white center that fades into a blue and purple glow. The overall aesthetic is futuristic and high-tech.

How GenAI Improves The User Experience

“Getting AI right is about empowering your people to do their best work. We’re off to a good start, and now that we’re underway, we’re laser focused on making sure everything we do empowers our employees to be their best, most creative selves while also protecting them and the company.”

The AI Revolution: How Microsoft Digital (IT) is responding with an AI Center of Excellence

GenAI represents a transformative leap in how users interact with technology. It is redefining the user experience (UX) across various domains — from content creation and customer service to personalized recommendations and creative endeavors. By leveraging advanced machine learning models, GenAI can produce new content, predict user needs, and enhance interactions, leading to significant user experience gains.



ENHANCING PERSONALIZATION

One of the most prominent benefits of GenAI is its ability to deliver highly personalized experiences. By analyzing vast amounts of data, GenAI can understand user preferences, behaviors, and contexts. This allows for the creation of tailored recommendations, whether in entertainment, shopping, or online services. Users receive content and suggestions that align closely with their interests, enhancing satisfaction and engagement. For instance, streaming services like Netflix use GenAI to curate personalized content, improving user retention and their overall experience.



BOOSTING EFFICIENCY

GenAI streamlines processes that traditionally required significant human effort. In content creation, tools like OpenAI's GPT-4 can generate articles, reports, and even creative writing, significantly reducing the time required for these tasks. This efficiency gain is not limited to creating content. Customer service is another area experiencing a revolution. AI-driven chatbots and virtual assistants can handle a high volume of inquiries, providing quick and accurate responses, which enhances user satisfaction while freeing human agents to tackle more complex issues.



LEVERAGING CREATIVITY AND INNOVATION

GenAI acts as a powerful tool for creative professionals, providing new avenues for innovation. Artists, designers, and writers can use AI to generate ideas, explore new styles, and even create complete pieces of work. This collaboration between human creativity and AI capabilities leads to unique and compelling outcomes. For example, AI-generated art can serve as inspiration or even final pieces in visual arts, while writers can use AI to draft stories or develop plots, pushing the boundaries of creative expression.



CREATING MORE INTUITIVE AND NATURAL INTERACTIONS

Natural language processing (NLP) advancements have made interactions with AI more intuitive and human-like. Voice assistants like Amazon's Alexa or Apple's Siri have become more adept at understanding and responding to natural language queries, providing users with a seamless and efficient way to access information and control their smart devices. This natural interaction reduces the learning curve and enhances the overall user experience.



BROADENING ACCESSIBILITY

GenAI plays a crucial role in making technology more accessible. AI-driven tools can assist individuals with disabilities by providing features like real-time speech-to-text transcription, image recognition for the visually impaired, and predictive text input for those with motor impairments. These advancements ensure that technology serves a wider range of users, promoting inclusivity and equal access to information and services.

As GenAI continues to evolve, its potential to transform the user experience will only grow, paving the way for a future where technology seamlessly adapts to and anticipates user needs, and creating richer and more engaging interactions.

The background features a dark blue and purple color palette with a subtle grid pattern. Two large, glowing spheres are positioned at the top and bottom center, emitting a bright white light that fades into the surrounding colors. The overall aesthetic is futuristic and technological.

GenAI in Cyber Defense

“In the coming years, innovation in AI-powered cyber defense will help reverse the current rising tide of cyberattacks.”

Tom Burt, Corporate Vice President, Customer Security and Trust, Microsoft

STAYING A STEP AHEAD OF THE BAD ACTORS

Since bad actors are already using GenAI to exploit vulnerabilities, businesses must have cyber defense technologies and processes that match (or exceed) these capabilities. Threats can range from subtle infiltration of data stores to more overt attacks. Without proper monitoring, the consequences could be disastrous, potentially even threatening lives, and we might not realize it until it's too late.

It's crucial to employ GenAI in our defensive posture, whether it's managed in-house or through a Managed Security Service Provider (MSSP). This requires regular updates — quarterly would be ideal — which should be stipulated in contracts. Although there might be higher initial costs, efficiency gains over time are likely.

TRANSFORMING SECURITY OPERATIONS WITH MICROSOFT COPILOT

Microsoft Copilot is revolutionizing the way security analysts respond to threats by seamlessly integrating automation into their workflows. It allows security teams to upscale their operations, enhancing their ability to detect and respond to threats with unprecedented efficiency. Copilot's advanced automation tools allow analysts to focus on high-level strategic tasks, significantly boosting their productivity.

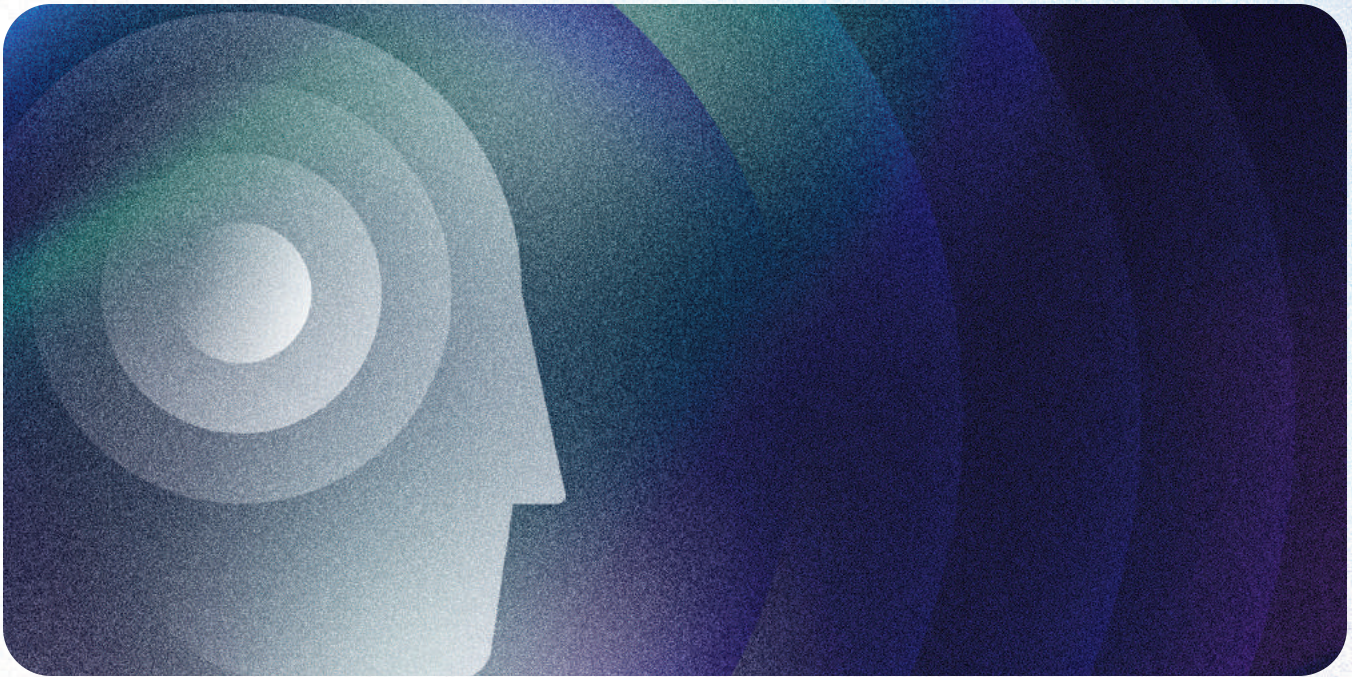
Microsoft Copilot facilitates a holistic approach to threat detection and response, reaching into every aspect of an organization's security infrastructure. From patch management to incident response, Copilot ensures that analysts can perform at their

best, even with limited resources. By automating routine tasks, Copilot frees up valuable time for analysts to focus on critical issues, enabling companies to do more with smaller teams.

The integration of Microsoft 365 tools such as PowerPoint, Word, and Excel with Copilot enhances the overall efficiency of security operations. Companies can now streamline their workflows, utilizing familiar tools to create reports, analyze data, and develop comprehensive security strategies. This synergy between Copilot and Microsoft 365 tools empowers security teams to deliver more effective and timely responses to threats, ultimately transforming their productivity and impact.



Key Takeaways



KEY TAKEAWAYS

- Businesses worldwide are expecting transformational gains in productivity and user experience through the adoption of GenAI technology.
- Tech selection and adoption processes that have been in place for the past 10-15 years are linear in nature. But linear processes don't work well in the rapidly changing world of AI. Organizations need to embrace exponential thinking to change these processes.
- An organizational structure built on functional ownership is a roadblock to the exponential model. Transitioning to this new model requires that organizations shift commodity workloads to vendor platforms, create a Zero Trust governance group, reform the business-as-usual processes model, understand the unique nature of AI model data, and take steps to secure GenAI prompts to guard against exploits.
- GenAI improves business productivity by enhancing efficiency through automation, driving innovation, improving data-driven decisions, and expanding operational agility.
- Gen AI improves the user experience by enhancing personalization, boosting content creation and customer service efficiency, leveraging creative capabilities, creating more intuitive and natural interactions, and broadening accessibility to technological advancements.
- It's crucial to employ GenAI in the enterprise security defensive posture as it can help to foster innovation in implementing robust access and data controls, along with data privacy measures.

WIPRO MICROSOFT COPILOT FOR SECURITY READINESS WORKSHOP: 1 DAY

Wipro Ltd

Wipro's Microsoft Copilot Security Readiness Workshop will demonstrate the value Copilot brings at machine speed and scale and prepare enterprises to embrace GenAI for security.

PROBLEM STATEMENT:

Enterprises worldwide face unprecedented challenges from escalating cyber threats. These challenges are further compounded by the rapidly evolving regulatory landscape. Security Operations teams find themselves in a critical position, requiring effective detection and response capabilities to swiftly identify risks and prioritize them. However, this task has become increasingly daunting, especially in a fragmented security landscape where organizations rely on multiple tools to safeguard their data and environment.

The complexity of managing security incidents requires teams to deduplicate numerous alerts, manually correlate insights, and determine the nature of incidents across various teams and solutions.

Unfortunately, this manual process often results in lengthy investigation times.

Microsoft Copilot for Security is the leading security AI product that combines a specialized language model with security specific capabilities from Microsoft. These capabilities incorporate a growing set of security-specific skills informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals. With our security integration expertise, you can improve the efficiency of enterprise SecOps by summarizing vast data signals into key insights to detect cyber threats before they cause harm and put critical guidance and context at security teams' fingertips so they can respond to incidents in minutes instead of hours or days.

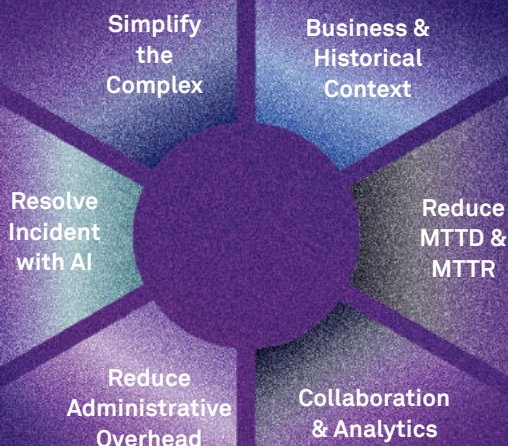
WIPRO'S OFFERINGS

Wipro's Microsoft Copilot for Security solution offering is designed to help SecOps, Identity Management, Data Security, Cloud and Infra Security and Compliance teams achieve more with less by leveraging Generative AI for Security capabilities. Our offering consists of a 1-day Readiness Workshop, Quick Start solution, and a Security Engineering program to ensure a robust security posture.

The workshop goal is to assist customers in identifying use cases and getting started with Microsoft Copilot for Security. Additionally, it enables them to connect with their existing Microsoft 365 Defenders, Microsoft Entra, Microsoft Intune, Microsoft Sentinel, Azure, or even other third-party security services through custom plugins to bring contextual information using natural language prompts.



Microsoft Copilot for Security



MICROSOFT COPILOT FOR SECURITY READINESS WORKSHOP

The workshop will allow you to:

- Learn Microsoft Copilot for Security capabilities with demos
- Identify Copilot for Security use cases and personas for your enterprise
- Set up and configure Copilot for Security for PoC testing
- Discuss and define roadmaps for quick and full adoption

Please visit <https://www.wipro.com/cybersecurity/microsoft-security/> to learn more about our Microsoft security offerings.

wipro: cybersecurity
by cybersecurists

