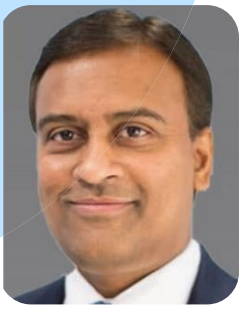
FROM DEFENSE TO RESILIENCE:

Infosys' AI-First Cybersecurity Lens on 2026

Infosys®
Navigate your next

CONTENTS



Umashankar Lakshmipathy

EVP and Head of Cloud, Infrastructure, and Security Services, EMEA, Infosys

In an era where the definition of change evolves rapidly, driven by the diverse effects of geopolitics, AI and new business models, it's table stakes now for enterprises to be on the edge. Add to it the need to remain competitive, relevant and most importantly be adaptable.

Against this backdrop, the boundaries of technologies and their capabilities have ceased to exist. And enterprises need to constantly navigate complexities to build robust ecosystems that help them accelerate in their growth journey. This is where the role of strong, preemptive cyber capabilities comes in to play for leaders to build, scale and secure their ecosystems.

For decades, the core mission of cybersecurity has been defense—building taller walls and more complex tools in an attempt to keep attackers out. This approach, centered on human control and a growing collection of disparate technologies, is no longer sufficient. We are at an inflection point where the sheer volume and velocity of threats have outpaced our ability to manage them manually. A fundamental change is not just necessary; it is already underway.

The future of cybersecurity is not about accumulating more tools, but about building greater resilience. It is about creating systems that can withstand and adapt to attacks, ensuring that business operations remain steady and trust remains unshaken. This requires a new playbook, one where security is not a reactive function but an intelligent, proactive, and integrated part of the enterprise fabric.

At Infosys, we are building this future today.

> **Our approach is centered on three core principles: Resilience at the Core, Platform-Driven, and AI-Powered.**

We believe that by embedding AI agents and automated services directly into the security framework, we can shift from a state of constant defense to one of perpetual resilience. This is the essence of our Cyber Next platform, which unifies posture, protection, and prevention into a single, intelligent system that learns and strengthens with every event.

This report outlines our playbook for this new era of AI-first cybersecurity. It details how concepts like Cybersecurity as a Service (CSaaS) and our Agentic AI Foundry are transforming security operations from a manual, high-pressure effort into a calm, automated, and highly effective function. We share not just our vision, but also tangible proof of how these principles are delivering measurable results for our clients across the globe—reducing risk, enhancing efficiency, and enabling growth.

The goal is no longer just to defend, but to endure and thrive. This is resilience by design, delivered at scale, with AI. This report provides perspectives on what's next in cybersecurity, helping to not just prepare but also to accelerate businesses exponentially.

From Defense to Resilience: The Infosys Playbook for AI-First Cybersecurity

1. Cybersecurity is at an Inflection Point

Something fundamental is changing in how we protect the digital world. For years, cybersecurity meant tools, consoles, and dashboards that people had to learn and operate. That model is fading. A new one is taking shape, built around the idea of Service-as-Software. Instead of handing people more tools, enterprises are beginning to rely on AI agents that deliver results independently. These systems do not wait for direction; they sense what matters, make choices, and act in the moment. The concept may sound technical, but the meaning is straightforward. Security is shifting from something a team controls to something that quietly takes care of itself.

At Infosys, this belief forms the center of the One Services Stack. Think of it as a living system that connects AI Agents, Services, and Models to help enterprises run efficiently, evolve continuously, and remain secure as they grow. At Infosys, engineering at scale is what makes this shift practical. The Stack brings together four core areas that define today's digital organization: Transformation, Operations, Quality Engineering and Validation, and Cybersecurity and Responsible AI. Cybersecurity anchors all of them. It connects each part of the enterprise, keeping it safe by design and learning from every event to strengthen its judgment over time.

There's really only one way forward now: design for impact, not accumulation. More tools won't save anyone; better structure will. At Infosys, we've learned to treat resilience as the real target of cybersecurity. It's about keeping operations steady and trust unshaken, even when everything else feels uncertain. We work around three habits that guide everything we build: **Resilience at Core, Platform Driven,** and **AI Powered**. Resilience is about preparing before a crisis, not repairing after one. This vision of resilience is further strengthened by Infosys' strategic acquisition of **The Missing Link**, an Australian cybersecurity services specialist firm. With its expertise across the full stack of cyber solutions, The Missing Link enhances Infosys' ability to deliver end-to-end cybersecurity offerings. Its highly skilled teams, including Red Team, Blue Team, and a state-of-the-art Global Security Operations Centre (GSOC), complement Infosys' global cyber defense centers, creating a robust network of capabilities. Together, we are redefining what it means to secure enterprises at scale, ensuring that resilience is not just a goal but a built-in feature of every system.

The platform view ties every part of defense together so nothing falls through the cracks. And AI brings the speed and foresight that human teams simply can't sustain on their own for long.

This isn't theory. Through **Cyber Next**, our integrated security platform, and the **Agentic AI Foundry**, we help organizations turn fragmented defenses into a single, intelligent fabric. It's about making security work together—predicting when it can, adapting when it must, and always learning.

The shift from defense to resilience is already under way. The question is no longer if an organization will be targeted, but how prepared it will be to stay standing when it is.

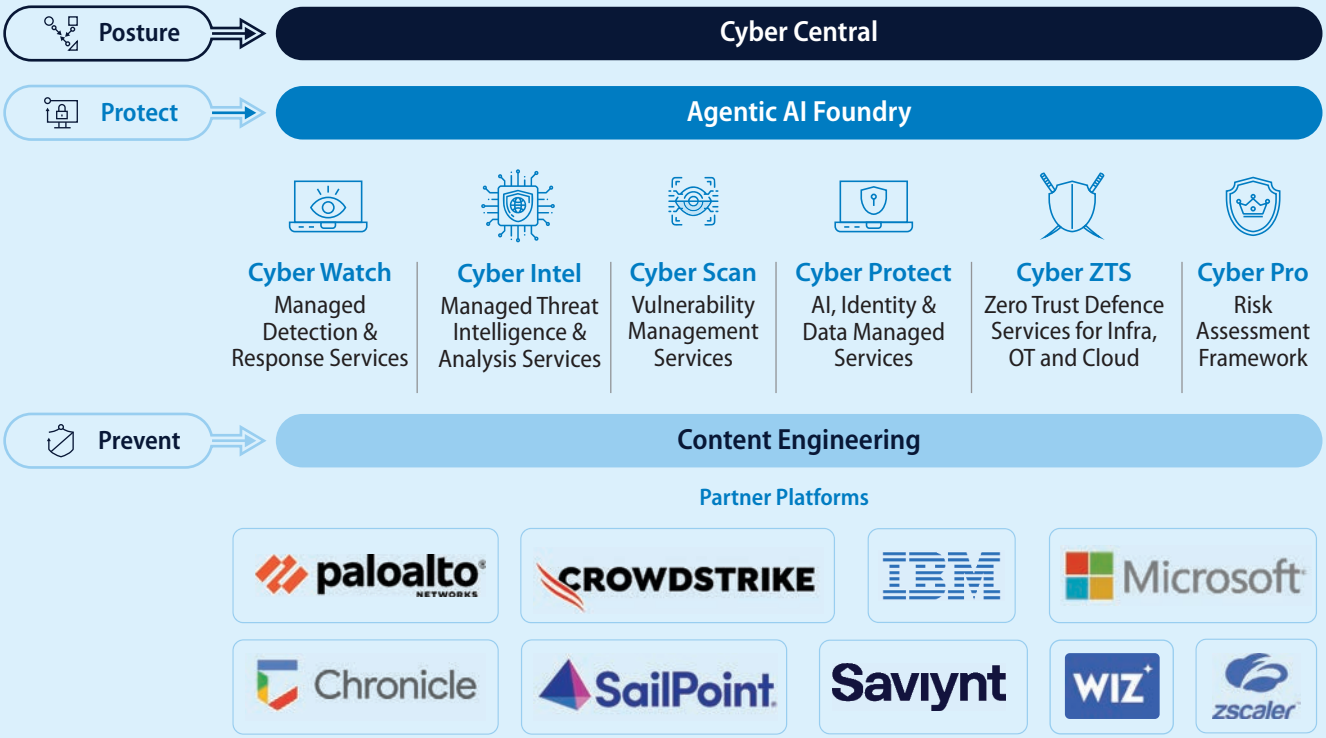
2. Infosys Cyber Next Platform: Posture, Protect, Prevent

For years, enterprises have tried to improve what they call their security posture. Most ended up with long inventories of tools and vendors, added one incident at a time. On paper, the setup looked strong. In reality, it behaved like scaffolding built under pressure, solid until the next breach exposed the gaps.

Cyber Next changes that. It sits at the heart of the Infosys One Services Stack, uniting every part of defence into one continuous system. The model works across three layers: Posture, which shows where an organisation stands; Protect, which keeps it safe; and Prevent, which helps it stay that way. Instead of piling on more technology, Cyber Next makes what already exists work together. It connects assessment, protection, detection, and recovery so that information flows both ways and every cycle makes the next one stronger.

This is the "platform of platforms" idea in practice. Cyber Next links existing enterprise systems, third-party security tools, and AI-driven services through one intelligence layer. It draws data from multiple sources, interprets what it finds, and responds with accuracy and speed. A signal from a compromised identity in the cloud can trigger automated isolation of an endpoint, a cross-check with threat-intelligence feeds, and a notification to the operations centre within minutes. What once required a chain of human hand-offs now happens as one coordinated response.

Cyber Next protects more than one hundred and forty clients across industries and regions. Five Cyber Next Labs feed the system with new insights each day, and more than a hundred AI agents take care of repetitive work that once consumed analysts' time. Partners such as Palo Alto Networks, CrowdStrike, Zscaler, and Microsoft extend the platform's reach.



Early pilots with AppViewX on post-quantum cryptography show how it continues to evolve. Client retention remains above ninety-five percent because the benefits are visible within weeks: fewer false positives, faster triage, and calmer teams.

Each module inside the platform plays a defined role but gains full value only through connection with the rest.

Together they replace isolated dashboards with one clear view of threat, exposure, and response.

Cyber Watch monitors and responds through an AI-enabled operations center.

Cyber Scan finds weaknesses and ranks them by business impact rather than by raw severity.

Cyber Protect manages identity, data, and privacy across hybrid environments.

Cyber Intel adds live context from threat data so that every response carries insight, not guesswork.

Cyber Pro translates technical exposure into the language of business risk.

Automation handles the routine, yet human judgment remains essential. The platform drafts the first version of each investigation and leaves the final call to the analysts. Every incident becomes another training run. Over time, Cyber Next learns what normal looks like for each enterprise, when to raise an alert, and when to stay quiet.

As adoption grows, Cyber Next begins to shape how organisations measure value. Budgets and dashboards no longer multiply without control; they converge. A manufacturer that once needed twenty minutes to triage an incident now resolves it in under seven. A global bank cut false positives by nearly half after connecting its cloud and on-premise environments. These gains are not just about speed. They build confidence that the system learns and improves on its own.

The platform model also makes governance easier. Boards now see business-aligned data: how risk is trending, how much value has been protected, and where fresh investment will matter most. Security finally speaks the language of strategy.

Perhaps the most overlooked advantage is calm. When everything runs through a single platform, duplication disappears. Licences shrink. Documentation becomes automatic. Teams stop firefighting and start thinking again. The work feels measured instead of frantic.

For large, distributed enterprises, this connected model is the only sustainable path forward. It scales because it learns. Each response sharpens the next one, and every new threat becomes another opportunity to train the system. Over time, resilience stops being an initiative and becomes instinct.

That is the strength of Cyber Next within the Infosys One Services Stack. It does not just protect the business; it gives it balance. When security works as part of everyday operations, growth stops feeling risky and starts feeling possible.

3. Cybersecurity as a Service (CSaaS): From Analyst to AI Worker

Spend a day inside any security operations centre and you can feel the weight of the work. Alerts arrive faster than people can read them. False positives mix with real threats. Analysts juggle dashboards, trying to keep up. **Cybersecurity as a Service (CSaaS)** is designed to take that weight off their shoulders. It shifts protection from a patchwork of tools to a service that runs in the background, twenty-four hours a day. In this approach, **AI agents do the groundwork.** They map the attack surface, support the defenders, and act automatically when a problem appears. The difference is striking. Work becomes steady instead of frantic.

CSaaS combines what already works in security with the precision and scale of artificial intelligence. The goal is not complexity; it is control. Systems, networks, and data stay protected while people get space to think. Instead of buying hardware that goes obsolete, organisations treat cybersecurity as a utility. CSaaS runs as an operating expense, not a capital burden, so protection can expand or shrink with business needs. **Agentic AI makes that possible**, faster, more precise, and less expensive than anything before it.

At **Infosys**, CSaaS sits within the **One Services Stack** and draws its strength from the **Agentic AI Foundry**. The Foundry builds agents that take on repetitive tasks and never tire. More than a hundred of these digital coworkers already work across identity, cloud, and infrastructure environments. They learn from every case, getting sharper over time.

Inside a security team, the change shows up fast. The **SOC Agent** filters alerts before analysts see them. The **Vulnerability Agent** sorts patches by how much business risk they carry. The **Threat Hunter Agent** connects behavior patterns and logs to find what looks out of place. Within hours, the noise fades. Analysts finally focus on the few events that matter.

The numbers back it up. An energy company cut investigation time by two-thirds and improved analyst output by forty percent. A large bank used AI assistants to automate policy checks and onboarding. Work that once took days now takes minutes. These are not lab tests; they run in production, beside people who still make the final calls.

Money matters here too. Traditional security demanded large capital budgets and constant upgrades. The service model changes that. Costs move to predictable monthly spending that adjusts with the business. Smaller companies can now access enterprise-level defense, and global firms can apply the same standard everywhere. Security becomes part of operations rather than a drain on them.

No system earns trust on its own. Every AI model inside **Cyber Next** goes through review before it is allowed to run. Teams test for fairness, accuracy, and privacy, and they keep a close watch for anything that looks odd, such as a data leak, an unexpected pattern, or behavior that feels off. Sensitive information is hidden automatically, and every action leaves a trace so that the reason behind a decision is always clear.

CSaaS is not just about saving money or automating routine work. It shows what the future of defense looks like. By 2030, a CISO's team could include thirty or forty digital AI workers sitting next to human analysts. They will act as the first line of response, communicating like a swarm, containing risks before people even know they exist. The goal is not to replace talent but to give it more reach. Machines handle the scale; humans handle the sense-making.

Regulation is moving quickly.

Europe's AI Act, India's Data Protection Law, and the U.S. NIST framework are shaping how systems must operate. Infosys moved early. Its **ISO 42001 certification** gives clients confidence, and open-source tools let them test how models behave in their own setups. Transparency is built into the process.

Partnerships have played a crucial role in building this Responsible AI and Data Protection framework.

Working with Microsoft, Infosys integrated its Agentic AI approach with Purview DSPM and AISPM to secure data movement across both Microsoft and non-Microsoft environments. With AppViewX, the company ran pilots on post-quantum cryptography, proving that even highly regulated industries can prepare for the next computing era without disrupting existing systems.

Accountability still sits with people.

The **Responsible AI Office** brings together engineers, ethicists, lawyers, and compliance specialists who look at every model with a simple goal: keep asking the questions the software cannot. Where did this data come from? Who approved the outcome? What happens if the answer does not look right? Their work builds a rhythm of oversight that keeps the system honest and under human control.

Together they create calm in a field that once lived in constant tension.

CSaaS turns security into a steady habit rather than an emergency drill. It gives organizations time to think, room to grow, and confidence that their systems will stay upright when tested. The next section looks at what this means in the real world, where these ideas are already working in production.

4. Proof in Production: Cyber Resilience at Work

The real test of any platform isn't what it promises on paper; it's how it behaves when something breaks. In cybersecurity, theory lasts about five minutes. After that, the only thing that matters is whether the system can keep the business running.

That's where **Cyber Next** has earned its place. The platform is live inside some of the world's most complex enterprises: factories that run around the clock, banks that move billions a day, and utilities that can't afford a second of downtime. These are not controlled pilots or proof-of-concepts. They are production environments where a missed alert can turn into front-page news.

Each of these stories has one common thread: resilience. The ability to adapt, recover, and keep going when the unexpected happens. That's what separates a capable system from a trustworthy one.

What stands out most is how quickly the benefits appear once the platform goes live. Teams find themselves spending less time chasing alerts and more time improving defenses. Reports that once took days to compile are available instantly. Risk conversations move from "what went wrong" to "what we learned." Cybersecurity stops being a technical department and becomes part of business planning.

This isn't theory or marketing language. It's the everyday rhythm inside client environments that runs Cyber Next. The platform proves that large enterprises can modernize their security without losing stability and that AI, used responsibly, can raise standards instead of risks.

The measure of success isn't that incidents never happen. It's that when they do, the organization bends but doesn't break. That's what **Cyber Next** delivers: resilience you can measure and confidence you can see in operation.

A global manufacturer felt the impact first. Before Cyber Next, its analysts were handling a constant flood of alerts, most of them false alarms. The team spent so much time sorting signals that real threats often hid in plain sight. After moving its operations to the platform, investigation times dropped by almost two-thirds. Automation took over routine checks; the AI agents grouped and prioritized incidents; and analysts could finally focus on what mattered. The change wasn't subtle; productivity rose, fatigue fell, and the security posture became clearer overnight.

In another case, an energy client used AI-powered assistants from the Agentic AI Foundry to handle onboarding and policy enforcement across multiple regions. Manual reviews that once took days now finish in minutes. That speed didn't just save time; it built confidence that policies were applied the same way everywhere, every time.

5. Cyber ARC: From Applied Research to Competitive Edge

The nature of cyber risk is changing faster than ever. Every new technology creates both opportunity and exposure. To stay ahead, security innovation must move from theory to action in real time. That is what Cyber ARC, the Applied Research Center at Infosys, is built to do. It is where ideas become prototypes, and prototypes become living defenses that protect clients every day.

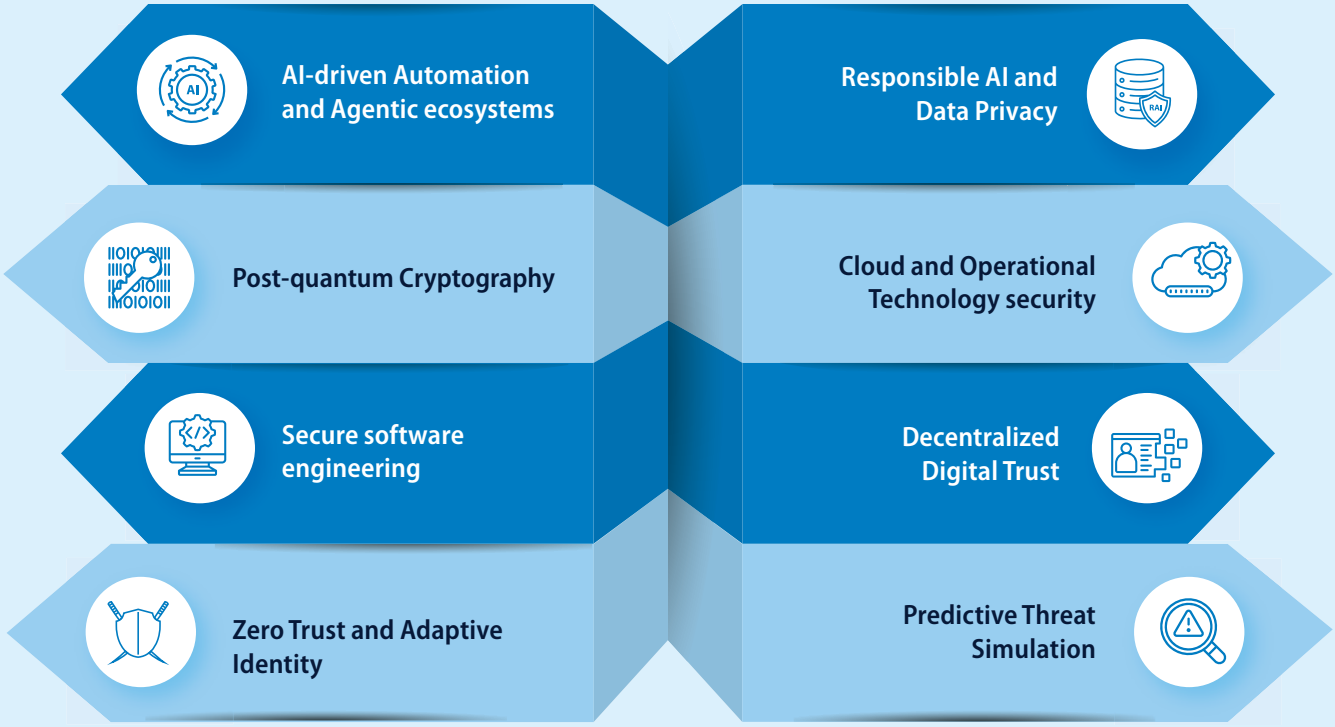
Cyber ARC focuses on eight advanced research areas where cybersecurity is expected to evolve most rapidly. These include AI-driven automation and agentic ecosystems, post-quantum cryptography, secure software engineering, zero trust and adaptive identity, responsible AI and data privacy, cloud and operational technology security, decentralized digital trust, and predictive threat simulation.

Each theme reflects a direction where enterprises will need new engineering and new thinking to stay secure.

Research here is not theoretical. Every project follows a simple rhythm of Idea -> Proof of Concept -> Production. Concepts are tested with real-world data, refined by engineers, and then deployed through Cyber Next or as part of Cybersecurity as a Service offerings. This continuous loop ensures that innovation is not isolated from operations. It feeds directly back into the systems that clients use every day.

Cyber ARC is also integrated with Infosys Living Labs, giving clients a place to bring their own cyber defence use cases to life. Enterprises can experiment with new controls, test automation ideas, or co-develop AI-driven defences alongside Infosys researchers and engineers. Successful experiments are scaled

Fig. Key focus areas of Cyber ARC



into production environments where they deliver measurable impact. This approach makes innovation practical, transparent, and fast.

Collaboration has always been part of how ARC works. Universities remain one of its strongest partners, helping explore ideas that range from cryptography to AI ethics and data privacy.

The centre also works closely with technology companies, regulators, and industry groups to make sure what is built inside the lab stands up in the real world. Together they form a community that keeps learning from one another and turning research into something that can actually be used.

Cyber ARC is not just about creating new tools. It is about shaping the conditions in which security can thrive. The center's work supports Infosys's broader goal of building a composite cyber workforce for the decade ahead, where human analysts, AI workers, and platform intelligence operate as one. By 2030, the outcome will be defense systems that learn, adapt, and act together, keeping organizations resilient even as the threat landscape keeps shifting.

Cyber ARC represents the forward edge of Infosys's cybersecurity vision. It keeps discovery alive, connects innovation with execution, and turns research into a competitive advantage.

Conclusion: Resilience by Design, at Scale, with AI

What if the future of cybersecurity looked less like a wall and more like a living network?

What if defense could think for itself, learn from experience, and act before an attacker made the next move?

That is the question shaping the decade ahead. The next phase of cybersecurity will not depend on a single system or static control. It will come from swarms of interoperable AI agents that work together the way human defenders do. They will share information, divide responsibility, and respond in seconds, not hours. Each will bring a specific skill, but their strength will come from the way they collaborate and adapt.

At Infosys, this vision is already taking shape. The building blocks are here in the One Services Stack, in Cyber Next, and in the Agentic AI Foundry. These foundations give enterprises a way to grow defenses that are resilient at core, platform driven, and AI powered. The aim is not only to keep pace with attackers but to stay one step ahead, always learning, always ready.

Picture the CISO's team of 2030: human analysts working side by side with digital AI workers, each tuned to anticipate, reason, and respond as part of a single fabric of defense. Threats will emerge, but they will meet a system that collaborates faster than they can spread. This is the frontier Infosys is preparing for, where resilience is built in by design and scaled by intelligence.

The question now is not whether such a swarm can exist, but how quickly we can bring it to life. The answer begins here.

For more information, contact askus@infosys.com

Infosys®
Navigate your next