TAG

Security Annual

2026

SPECIAL REPRINT EDITION

HOW ACRONIS SECURES MODERN IT

AN INTERVIEW WITH GAIDAR MAGDANUROV, PRESIDENT, ACRONIS

FACTORS POINTING TO NEAR-TERM OT CYBER DISRUPTIONS

MANAGING AI-RELATED IDENTITIES

TAG DISTINGUISHED VENDOR

Acronis

The need to reduce cyber risk has never been greater, and Acronis has demonstrated excellence in this regard. The TAG analysts have selected Acronis International GmbH as a 2026 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Acronis' platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Security Annual
www.tag-infosphere.com

REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH
GAIDAR MAGDANUROV,
PRESIDENT, ACRONIS

HOW ACRONIS SECURES MODERN IT

As IT environments become more complex and cyber threats more interconnected, organizations can no longer rely on siloed tools for backup, security, and management. We spoke with Acronis about how its Cyber Platform unifies data protection, cybersecurity, and automation into a single, natively integrated solution. By combining backup, anti-malware, workload protection, compliance support, and AI-powered automation, Acronis helps businesses and managed service providers reduce operational strain, close protection gaps, and accelerate recovery across cloud, hybrid, and on-premises environments.

TAG: How is Acronis evolving its Cyber Platform to unify backup, cybersecurity, and endpoint management for modern IT environments?

ACRONIS: Evolving around our mission to protect, manage, and automate all small and medium IT deployments, the Acronis Cyber Platform continues to expand its capabilities. In designing the platform, we focus on enabling our partners and customers to achieve unmatched productivity and efficiency, as growing complexity and user demands put enormous stress on IT professionals, and productivity is a decisive factor for choosing a reliable partner like Acronis.

We continue expanding our focus on integrated data protection and cybersecurity, as they are the only reliable ways to protect IT infrastructure. The protection spans beyond traditional endpoints, including SaaS applications and data, treating backup, anti-malware, and anti-ransomware controls, and workload protection as integrated layers of protection rather than separate tools that create handoff gaps.

For end users, this unification matters because incidents rarely fit neatly into one category; a click on a phishing email can become an endpoint compromise, a lateral-movement event, and ultimately a data-loss recovery scenario.

Effective management of IT infrastructure is essential for cyber protection and requires key elements such as visibility, consistent policy enforcement, and routine IT hygiene—especially patching. Our research and industry reports show that exploited vulnerabilities remain the primary cause of attacks, underscoring the importance of maintaining operational hygiene.

Finally, protecting small and medium IT deployments at scale is impossible without extensive automation, including AI-powered workflows. Modern security threats demand rapid response, and maintaining a continuously evolving IT infrastructure—especially amid the widespread adoption of AI-driven tools—requires both supervised and unsupervised autonomous workflows. Today, nearly all cybersecurity professionals consider automation essential, compared to only half just a few years ago.

Industry evidence shows that deploying integrated AI-powered protection can shorten breach lifecycles by weeks or even months, reinforcing the case for unified platforms that eliminate gaps between detection and recovery.

TAG: In what ways does Acronis ensure fast and reliable disaster recovery across cloud, hybrid, and on-premises workloads?

ACRONIS: Fast and reliable disaster recovery is largely determined before an incident occurs: where data resides, how quickly it can be

Acronis True Image bundles backup with anti-malware and anti-ransomware capabilities, protecting backups and the backup-and-recovery process.

restored, and whether restoration processes are regularly tested. Prevention is equally critical, which is why integrated data protection and cybersecurity are essential. Recovery is only reliable if backup data is protected and systems can be restored to a secure state.

Recovery speed depends not just on infrastructure availability, but on effective management and automation to orchestrate the process—aligning with the Acronis Cyber Platform's native integration of protection, management, and automation. In on-premises environments, Acronis restores systems locally when appropriate while maintaining a clear path to cloud recovery during site-level events. In hybrid scenarios, workloads can move between on-premises and cloud environments without added crisis-time complexity.

Acronis further differentiates itself with Acronis Cyber Frame—an integrated, software-defined infrastructure that combines protection, management, automation, hosting, and storage. Available to select partners starting March 2026 and broadly later in the year, it supports on-premises, cloud, and hybrid use cases, streamlining infrastructure management, protection, and recovery.

TAG: What advantages does Acronis True Image offer for personal and small business data protection compared to traditional backup tools?

ACRONIS: Traditional backup tools are optimized for copying data and restoring it after something goes wrong. But "something going wrong" is increasingly a cyber event, and separating backup from real-time protection creates friction and risk. Ransomware attacks on individuals and home offices are widespread and threaten the livelihoods of businesses and individuals worldwide.

Acronis True Image bundles backup with anti-malware and anti-ransomware capabilities, protecting backups and the backup-and-recovery process. The Active Protection feature uses behavior-based monitoring to stop suspicious activity and automatically roll back affected files. Integrated security enables us to prevent most incidents and avoid recovery, saving our users an enormous amount of time.

For individuals and home businesses without IT expertise, the value is simplifying the path from detection to recovery: fewer tools to manage, fewer gaps between alerts and action, and a more predictable recovery motion.

TAG: How does Acronis help managed service providers (MSPs) scale their cyber protection services while maintaining operational efficiency?

ACRONIS: MSPs scale best when services are repeatable, easily manageable, and automatable. The managed services sector is projected to reach over $600 billion in global revenue this year, driven largely by the need for cybersecurity, compliance, and automation,

including AI productivity tools. Acronis leans into that reality through our "protect, manage, automate" mission. When backup, security controls, management, and AI-powered automation are delivered through a natively integrated platform, MSPs can standardize onboarding, policies, management, and reporting across many customers without multiplying consoles and integrations. Acronis also enables MSPs to protect AI workloads with the GenAI protection solution and offers its customers protected, managed AI productivity tools, available to select partners starting in 2026.

We are also helping MSPs scale through Acronis Academy, a comprehensive training and certification program that equips partners with education on technology and business best practices, including guidance on efficient AI adoption and on delivering effective AI services to their customers.

TAG: With rising regulatory and compliance demands, how does Acronis help businesses meet data sovereignty and security requirements?

ACRONIS: Compliance and data sovereignty are becoming operational requirements for businesses of any size. Over 75% of the world's population now lives under modern privacy regulations, and many enterprises mandate data-sovereignty controls from cloud providers starting in 2025. The landscape is both expanding and fragmenting: GDPR enforcement in 2025 alone reached over €2 billion in fines, the EU's DORA directive enforces strict ICT risk controls on financial entities, NIS2 extends cybersecurity obligations to 18 critical sectors, and cross-border data transfer compliance is one of the top regulatory challenges for global organizations.

Acronis addresses partner and customer needs by offering an integrated solution that enables compliance, and a Compliance Navigator—a free tool that identifies relevant frameworks based on industry and geography, and maps how Acronis capabilities support those controls (available at **acronis.com/en/compliance**).

Data residency is the other half of the equation: even strong security controls can fail to comply if data is stored in the wrong jurisdiction. Acronis enables MSPs and customers to choose where data resides across 54 Acronis-managed data centers globally.

FACTORS POINTING TO NEAR-TERM OT CYBER DISRUPTIONS

DR. EDWARD AMOROSO

At TAG, we believe that operational technology (OT) environments are now entering a period of significantly heightened cyber risk driven by converging technical, economic, and geopolitical forces. Unlike past eras, when OT disruption required insider access, specialized equipment, or physical sabotage, today's threat landscape increasingly enables remote, scalable, and economically motivated attacks with real-world impact.

Several interrelated factors, trends, and predictive models point in this direction. Witness the near-term increase in OT cyber disruption, particularly in critical infrastructure sectors such as energy, manufacturing, transportation, water, and chemicals. This article is intended to make the case that the risk is serious, and all the more dangerous because it has not been sufficiently recognized in the community. Hopefully, this can jog some OT operators into action. Let's get started.

FACTOR 1: AGING OT AND ICS INFRASTRUCTURE

An initial structural weakness of OT cyber risk involves the aging nature of industrial control system (ICS) infrastructure. Many control environments were designed decades ago with assumptions that no longer hold. For example, OT networks are no longer isolated from external networks, OT operators must be assumed to include a percentage of malicious insiders, and adversary capability can no longer be assumed to be limited.

Consider, for example, that PLCs, DCS controllers, safety systems, and field devices in many environments will routinely remain in service for multiple decades—generally far exceeding typical IT lifecycles. These industrial support systems often run older, unsupported firmware, proprietary operating systems, or custom protocols that cannot be easily patched or replaced. When vulnerabilities are found in these systems, they might remain for years.

The challenge is not that these systems are old. Rather, it is that they were never designed to defend against cyber threats. Authentication may be weak or nonexistent. Integrity checks may be absent. And monitoring capabilities may be minimal. In many facilities, asset inventories are incomplete, and operators lack clear visibility into which devices are running what logic. When is involves serious infrastructure like nuclear, then the consequences can be severe.

Figure 1. Aging OT infrastructure and consoles in a nuclear plant

From an attacker's perspective, this whole situation creates a target-rich environment where exploitation does not require cutting-edge techniques. Instead, attacking OT and ICS environments require only patience and access, which our security community has hopefully come to recognize is easy to obtain for any nation-state actor or group with even a modicum of experience and capability.

FACTOR 2: MODERNIZATION PRESSURE AND THE VULNERABILITY OF CHANGE

Paradoxically, efforts to modernize OT environments will often increase short-term cyber risk. That is, most organizations with tangible facilities and operational systems are under pressure to upgrade their aging infrastructure to improve efficiency, enable remote operations, meet regulatory requirements, or integrate with enterprise analytics and cloud platforms. The use of AI to cut cost and the use of off-grid energy for sustainability are also major change drivers.

Each of these changes introduces new attack paths. In fact, any time a system, regardless of its local circumstances, is subjected to some major design, implementation, or operational change, there will be opportunities for adversaries to exploit undetected vulnerabilities. Experience dictates that changes to systems will inevitably lead to vulnerabilities, and OT and ICS systems are no exceptions.

Perhaps exacerbating this risk, configuration changes, firmware upgrades, or controller replacements must be tested carefully (they are complex), often leading to deferred patching and prolonged exposure windows. In fact, during many OT modernization projects, temporary architectures using insecure jump hosts, vendor remote access, and integration gateways are commonly introduced to bridge gaps during change.

These transitional states are particularly attractive to adversaries, as security controls may be incomplete and operational oversight fragmented. In effect, the very act of upgrading or fixing OT creates moments of fragility that sophisticated attackers can exploit. With AI and energy costs driving change, we must therefore expect to see more exploits succeed during this transitional period, which could be lengthy.

Figure 2. Sample OT environments (data centers) with upgraded energy support systems

FACTOR 3: RANSOMWARE AND EXTORTION AS NATURAL EXTENSIONS INTO OT

It appears to our team at TAG that the economics of ransomware and extortion map cleanly onto OT environments. In IT, attackers monetize disruption by encrypting data or threatening leaks. In OT, attackers can monetize downtime. Industrial operations are often measured in millions of dollars per hour, and safety considerations can force rapid shutdowns even when damage is limited. This creates strong incentives for victims to pay quickly.

The barrier to linking ransomware campaigns with OT impact also seems low. For example, disrupting scheduling systems, historian databases, or HMI availability can all halt operations. More aggressive actors may go further, perhaps interfering with control logic to force shutdowns or damage equipment. The extortion can be powerful when attackers understand the physical process, perhaps knowing which valves, motors, or interlocks matter most.

As ransomware groups continue to professionalize, it's perfectly reasonable to expect increased targeting of OT-heavy sectors, either directly or through IT-to-OT spillover. The distinction between cybercrime and cyber-physical disruption is already eroding, in our view, and once these attacks start, we do not see good near-term solutions—which has the effect of making this an attractive threat vector.

It is also important to differentiate here between IT attacks and ransomware that might cause OT disruption and direct attacks on OT. In the case of the well-known Colonial Pipeline cyber-attack, the targeted systems were IT, and while this is nonetheless consequential, the real concern we have here involved direct attacks on the ICS or OT systems.

Figure 3. Colonial Pipeline operations disrupted by cyber threat

FACTOR 4: AI LOWERS THE BARRIER TO SOPHISTICATED OT ATTACKS

Artificial intelligence introduces an accelerant to OT cyber risk. Historically, attacks on industrial systems required deep domain expertise including understanding control theory, process engineering, and vendor-specific logic. AI has the potential to compress that learning curve. With sufficient data captured via historians, sensors, or documentation, AI systems can model industrial processes, infer normal operating ranges, and identify points of leverage.

AI can assist attackers in reconnaissance, discovery, and attack optimization. For example, machine learning models can analyze network traffic to identify control commands, detect timing patterns, or infer safety thresholds. Generative models can help craft malicious logic that mimics legitimate control behavior, reducing the likelihood of detection. Over time, AI-enabled tooling could enable attacks that deliberately induce physical stress or unsafe conditions.

For defenders, this represents a major shift in threat asymmetry. Capabilities that once belonged only to nation-states may become accessible to smaller, well-funded groups, increasing the frequency and diversity of OT-targeted attacks. Certainly, the solution to AI attacks will be better AI-enabled defenses, but until these are available, it seems reasonable to be concerned.

FACTOR 5: STUXNET AS PROOF OF PHYSICAL CYBER DISRUPTION

The Stuxnet operation remains the clearest proof that cyberattacks can produce precise, physical disruption in industrial environments. It demonstrated that software could manipulate control logic, deceive operators, and cause mechanical degradation, all without immediate detection. Importantly, Stuxnet showed that physical destruction does not require explosions or dramatic failures; subtle, cumulative stress can be just as effective.

While Stuxnet was exceptional in sophistication, it was not unique in principle. The underlying lesson is not about a specific exploit or vendor, but about feasibility. If a computer can quietly destroy centrifuges, it can also damage turbines, compressors, pumps, or robotic systems. As OT environments become more digital and interconnected, the pathways for such attacks multiply.

Figure 4. Iranian Natanz facility targeted by Stuxnet

Our view is this: It is preposterous to assume that our industry will never see another attack like Stuxnet. Predictive modeling at TAG suggests that after we see a new type of attack such as worms or DDOS, a period of dormancy follows before we see that attack repeated at scale. This suggests that Stuxnet, which happened in 2010, is likely to surface at scale—and soon.

LOOKING FORWARD: CONVERGENCE TOWARD DISRUPTION

Taken together, these trends point toward a near-term increase in OT cyber disruption. Aging infrastructure provides weak foundations. Modernization introduces instability. Ransomware aligns economic incentives, AI amplifies attacker capability, and Stuxnet offers a proven template for cyber-physical harm. None of these factors alone guarantees disruption, but in combination, they create a risk environment that is difficult to ignore.

For operators of critical infrastructure, the implication is that OT cyber risk is no longer a theoretical concern or a long-term horizon issue. It is an operational reality shaped by forces already in motion. The challenge is not simply to prevent breaches, but to understand how digital threats translate into physical consequences, and to design resilience accordingly.

POSTSCRIPT

Let's hope our community begins to take this threat seriously. We will do everything we can at TAG to ensure an increase in attention. Perhaps you might forward this article to anyone you deem in a position to take preventive action.

MANAGING AI-RELATED IDENTITIES

This chapter provides a high-level introduction to the issues enterprise teams must address to integrate their identity and access management with emerging AI deployment and use.

As enterprises move from experimentation to operational deployment of AI, identity emerges as a foundational security concern. AI systems are no longer limited to isolated analytics or model inference tasks. They increasingly act on behalf of the enterprise, interact with sensitive data, invoke tools, and make decisions that have real operational consequences. This shift forces security teams to reconsider long-standing assumptions about identity, access, and trust.

To understand how identity applies in AI environments, we must first clarify what kinds of entities are participating. Unlike traditional enterprise systems, AI introduces a mix of human users, software workloads, autonomous agents, and fully agentic systems. Each of these requires identity support, but not all require the same level of assurance or privilege control.

A useful starting point is the distinction between passive and active AI systems. Passive systems, such as LLMs responding to prompts, operate in a reactive mode. Active systems, by contrast, are designed to make decisions, initiate actions, and adapt behavior with limited or no human involvement. As autonomy increases, so does the importance of strong authentication, fine-grained authorization, privilege boundaries, and continuous monitoring.

Within this spectrum, it is also important to distinguish between AI agents and agentic AI. An AI agent is scoped to a specific task, such as triaging alerts or enriching data. By contrast, agentic AI systems operate with broader autonomy, chaining tools together, coordinating with other agents, and pursuing goals dynamically. From an identity perspective, agentic AI systems behave less like traditional software and more like independent digital actors.

AI Agent	Agenic AI
Repetitive tasks	Autonomous decisions
Needs instructions	Selects from different options
Predefined objectives	Creates new approaches
Human interactions	Minimal human interactions
Passive or Active	Mostly Active

Figure 5-1. AI Agents versus Agentic AI

However, to avoid getting tangled in distinguishing between (and nitpicking definitions of) Ai agents and agentic AI, we will use "AI agent" broadly throughout this chapter to describe any AI-enabled entity that acts within enterprise systems. Whether passive or autonomous, these agents must be assigned identities, governed by policy, and held accountable through security controls.

EXTENDING IDENTITY SYSTEMS FOR AI

Enterprises have already made substantial investments in identity and access management (IAM), identity governance and administration (IGA), and privileged access management (PAM) platforms. Any realistic AI identity strategy must therefore build on these investments rather than attempt to replace them. Introducing parallel identity systems specifically for AI would increase complexity, fragmentation, and risk.

At the same time, AI agents often replace or augment human roles. They analyze alerts, approve transactions, trigger workflows, and access sensitive resources. Functionally, they behave like members of the workforce, but without the natural guardrails of human intent, judgment, or fatigue. This makes identity extension unavoidable. That is, AI agents must be brought inside the same control framework that governs human and machine access.

This is where non-human identity (NHI) security becomes central. AI agents are not users, but they are also not static applications. They are non-human identities with dynamic behavior, evolving permissions, and variable context. Treating them as first-class identities allows enterprises to apply lifecycle controls, risk assessment, and auditability in a consistent way.

BUILDING AN AI IDENTITY PROGRAM

In today's environments, the most practical approach is to model AI agents similarly to existing non-human workloads such as service accounts or machine identities. This is an advantage, not a limitation, because enterprises already understand many of the risks associated with non-human identities, including credential sprawl, excessive privilege, and lack of visibility.

Modern cloud platforms address these issues through workload identity mechanisms that emphasize short-lived credentials, federation, and elimination of static secrets. Inside service meshes and distributed systems, cryptographic identity frameworks provide mutual authentication and workload attestation. These approaches enable AI agents to participate in zero-trust architectures, inherit enterprise policies, and be monitored like other automated entities.

However, AI agents differ from traditional workloads in one critical way: autonomy. Unlike conventional services that follow predefined call paths, agents discover tools, invoke APIs dynamically, and communicate with other agents. This behavior introduces new attack surfaces and requires more advanced identity threat detection and response capabilities tailored to agent activity rather than static code execution.

As AI agents become more common, identity programs must evolve from simple federation toward interaction-aware security. This includes understanding who an agent is, what it is allowed to do, why it is acting the way it is, and under what conditions its authority should be limited or revoked.

WORKLOAD IDENTITY FOUNDATIONS WITH SPIFFE AND SPIRE

One of the most relevant foundations for securing AI agents comes from the workload identity domain, particularly through the secure production identity framework for everyone (SPIFFE) and SPIFFE runtime environment (SPIRE) frameworks. These technologies were designed to address how to assign strong, cryptographic identities to non-human workloads operating across heterogeneous and dynamic infrastructure.

SPIFFE defines an identity format for workloads, independent of network location, IP address, or underlying platform. Each workload gets a cryptographically verifiable identity that can be authenticated using mutual transport labor security (TLS). SPIRE is the implementation that handles identity issuance, attestation, rotation, and revocation. Together, they provide an identity control plane that works across public cloud, private data center, container, and virtual machine environments.

This model aligns with early-stage AI agent deployments. Like microservices and batch workloads, AI agents are software entities that need to authenticate to APIs, access internal services, and communicate securely with other components. Using SPIFFE/SPIRE allows enterprises to issue short-lived credentials, eliminate static secrets, and enforce mutual authentication without introducing new trust assumptions.

From a zero-trust perspective, SPIFFE/SPIRE provides several advantages. For instance, identity is decoupled from underlying infrastructure, credentials are ephemeral by design, and authentication occurs continuously rather than at login time. These characteristics are well suited for AI agents that may scale dynamically, move across environments, or be instantiated on demand.

However, while SPIFFE/SPIRE is a nice starting point, it doesn't cover all the challenges introduced by AI. Traditional workloads operate within predefined call graphs and static trust relationships. AI agents, by contrast, may autonomously discover tools, chain actions, and collaborate with other agents in ways that were not programmed in advance. This shows that workload identity solves who a software entity is, but nothing about its purpose or authority.

NEW IAM, IGA, AND PAM REQUIREMENTS INTRODUCED BY AI

AI does change the requirements for identity systems. IAM platforms must authenticate agents continuously, not just at session start, and must evaluate access decisions based on changing context rather than static roles. IGA systems must govern agents across their lifecycle, including onboarding, capability changes, and retirement. PAM systems must address privileged actions executed by agents, including delegation from humans and escalation across tools.

These requirements blur traditional identity boundaries. That is, because an AI agent may simultaneously resemble a user, a service account, and an automation framework, identity platforms must converge around capability-based access, policy-driven delegation, and auditable decision trails rather than fixed entitlements alone.

Looking ahead, we expect that emerging identity systems will need to support verifiable credentials and signed capability tokens for AI agents. These mechanisms allow agents to prove what they are allowed to do without exposing unnecessary information, aligning with zero-trust principles in autonomous environments. This will likely be an area in which startups will create capabilities that should be acquired by the bigger IAM and IGA players. Time will tell.

CONTEXT, IDENTITY, AND THE ROLE OF MCP

A recurring concept in AI security involves something that has become known as context. Technically, context includes who initiated a given action, what goal is being pursued through that action, what data sources are involved in the action, and what constraints apply. For humans, much of this context is implicit. For AI agents, it must be explicitly conveyed and enforced.

The model context protocol (MCP) created by Anthropic defines how AI systems communicate in a structured, identity-aware manner. MCP provides a mechanism for agents to declare intent, request access, and receive responses in a way that can be inspected, authenticated, and authorized. When combined with enterprise identity controls, MCP identifies why an agent is calling an API and under whose authority it is doing so.

This use of MCP is a critical shift, because identity becomes more than a credential. Rather, it becomes a carrier of context. Agents can present identity-bound context to security controls, enabling more precise enforcement, better auditability, and safer delegation between humans and machines. Luckily, many vendors are now providing excellent support for practitioners to leverage this protocol in their infrastructure.

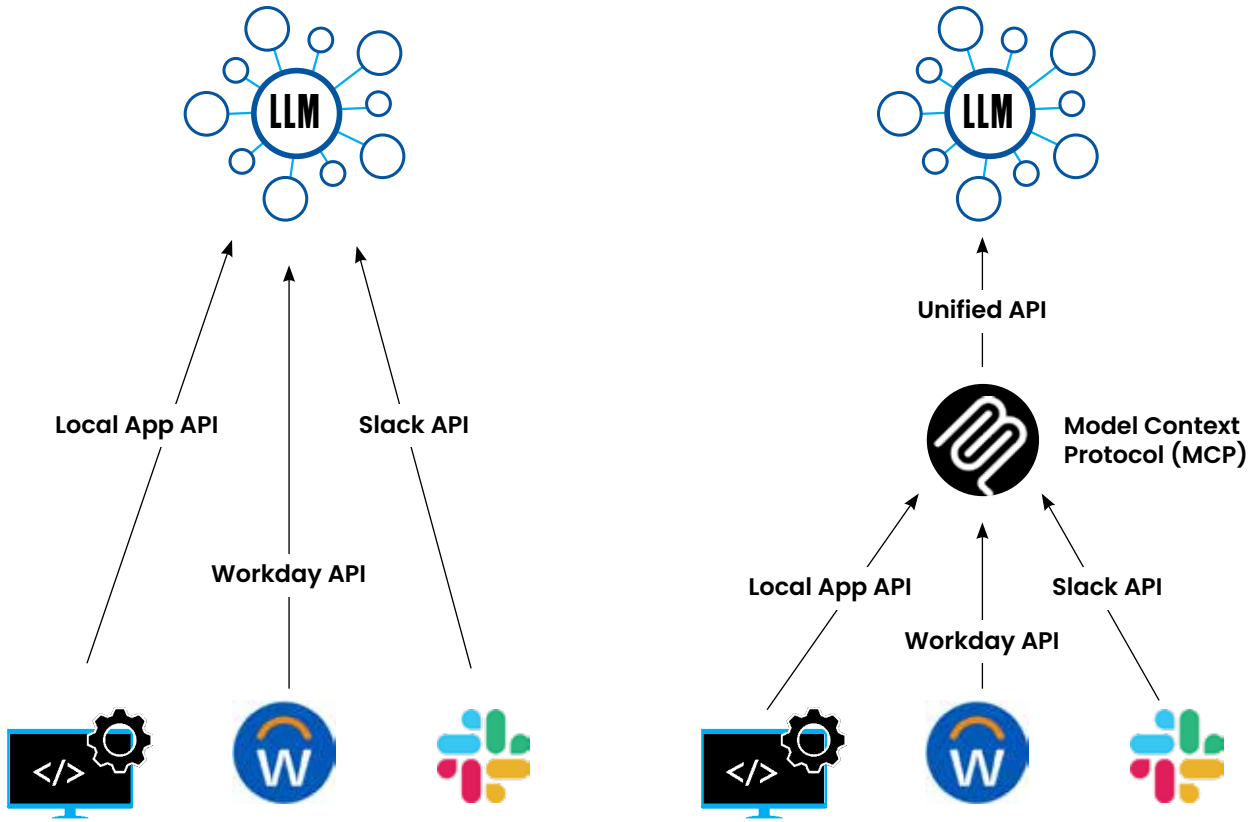


Figure 5-2. Before and After Use of MCP for AI APIs

RECOMMENDED STEPS FOR AI AGENT IDENTITY

In the near term, we recommend that enterprises treat every AI agent as a non-human identity with a defined lifecycle. This includes registration, attestation, credential issuance, monitoring, and retirement. Existing workload identity services and cryptographic identity frameworks can provide a solid foundation.

Second, enterprises should expect the emergence of AI access gateways that broker interactions between agents, models, and tools. These gateways will likely enforce identity, inspect prompts, track delegation, and serve as policy enforcement points for AI activity.

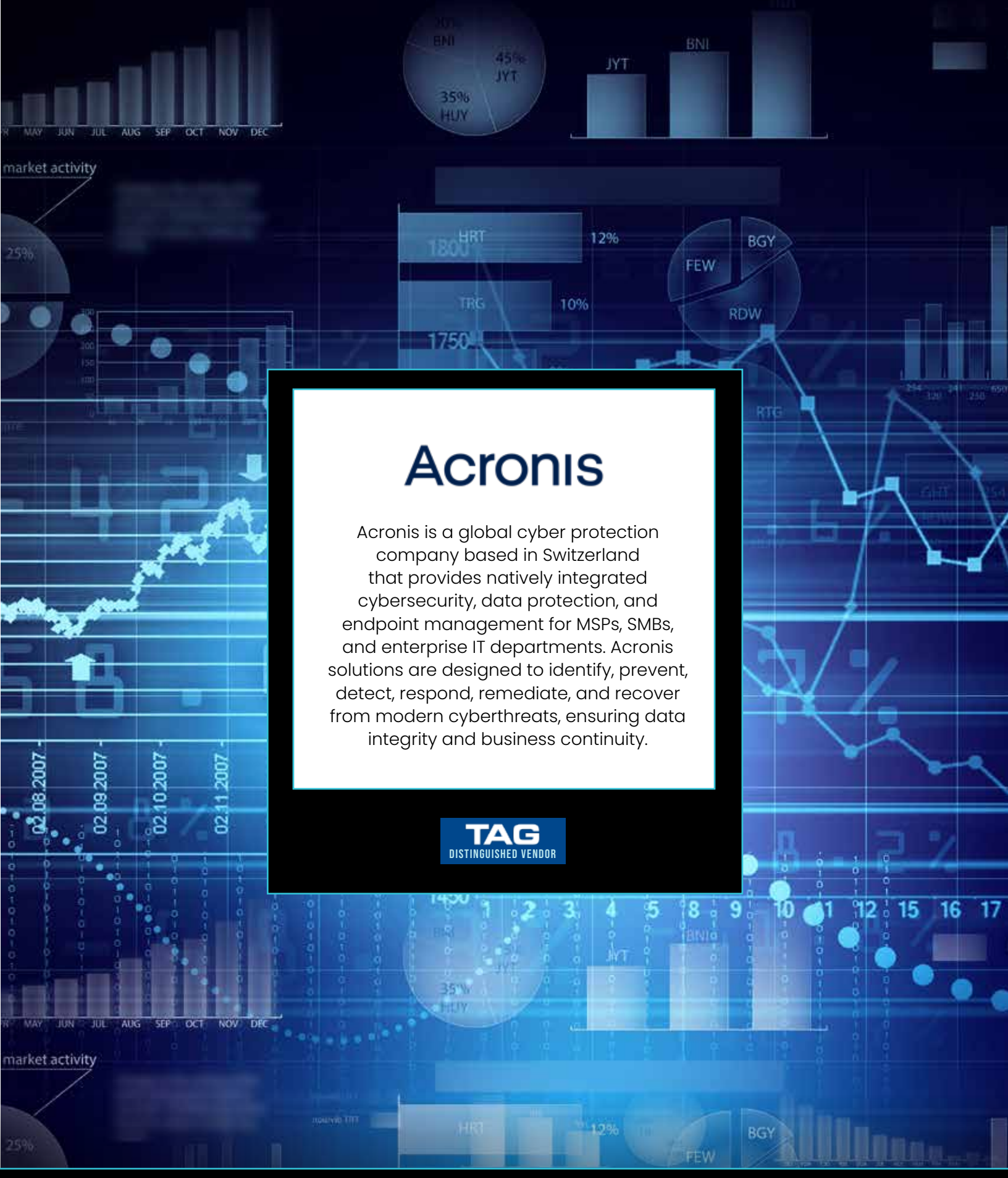
Third, when exposing enterprise resources to agents, organizations should standardize on MCP-based interfaces with strong authentication and authorization overlays. Maintaining an internal inventory of agents, permissions, and context sources will become as important as traditional asset management.

Finally, enterprises should plan pilot efforts in 2026 to explore secure agent-to-agent communication, recognizing that standards and tooling remain immature. These pilots will inform future production architectures as identity systems evolve to support autonomous software at scale.

LOOKING AHEAD

Identity for AI is still in its early stages. As of early 2026, standards, protocols, and commercial solutions are evolving rapidly. Security leaders should communicate clearly to executive stakeholders that AI identity is not a solved problem but a developing discipline. The goal is not perfection, but controlled progress grounded in zero-trust principles, strong governance, and continuous learning.

In the next chapter, we examine how commercial vendors are responding to these challenges and where enterprise teams can expect practical support as AI systems move from experimentation to mission-critical deployment.



Acronis

Acronis is a global cyber protection company based in Switzerland that provides natively integrated cybersecurity, data protection, and endpoint management for MSPs, SMBs, and enterprise IT departments. Acronis solutions are designed to identify, prevent, detect, respond, remediate, and recover from modern cyberthreats, ensuring data integrity and business continuity.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL