Dynamics AX and AI: New Threats… And New Tools to Fight Back

Microsoft Partner Azure Expert MSP | Microsoft Solutions Partner | INNERCIRCLE for Microsoft Business Applications

Table of Contents

Introduction: An Evolving Threat Landscape 3

The Rise of AI in Business Operations 5

Vulnerabilities of On-Premises Enterprise Software 6

Speed, and the Lack Thereof 6

Scalability, and the Lack Thereof 7

Skilled Teams, and the Lack Thereof 7

The Promise of Cloud Migration 8

The Intwo Difference 9

Six AI-Posed Threats to Dynamics AX (and Other On-Premises Solutions) and Cloud Mitigation Strategies 11

Threat 1: Sophisticated Phishing and Social Engineering Attacks 11

Threat 2: Automated Exploitation of Software Vulnerabilities 14

Threat 3: AI-Driven Ransomware and Malware Evolution 16

Threat 4: Data Exfiltration and Corporate Espionage via AI-Powered Bots 18

Threat 5: AI-Enhanced Denial-of-Service (DoS/DDoS) Attacks 20

Threat 6: AI-Driven Supply Chain Attacks 22

Beyond Threat Mitigation: Additional Benefits Intwo Provides as You Move to the Cloud 24

Scalability and Performance 25

Reduced Operational Overhead 26

Enhanced Business Continuity and Disaster Recovery 26

Innovation and Integration (Copilot, Autonomous Agents, Fabric, and More) 27

Cost Efficiency 27

What's Next...? Preparing for the AI Age 28

Connect With Us (Contact Information & Global Offices) 30

Introduction: An Evolving Threat Landscape.

It’s an era of unprecedented technological advancement with Artificial Intelligence (AI) at the forefront. AI's transformative power is reshaping industries and unlocking new frontiers of efficiency and innovation across virtually every business process.

From predictive analytics in supply chains to hyper-personalized customer experiences, AI is no longer a futuristic concept but a tangible, indispensable component of modern enterprise operations. Its ability to process vast datasets, identify complex patterns, and automate decision-making has propelled businesses into new realms of productivity.

However, this technological marvel, like many powerful innovations, possesses a dual nature.

While AI serves as an unparalleled tool for progress, it simultaneously emerges as a sophisticated and rapidly evolving threat vector. The very capabilities that make AI so beneficial – its speed, its capacity for learning, and its ability to automate complex tasks – can be weaponized by malicious actors.

This duality presents a profound challenge, particularly for organizations still relying on traditional, on-premises enterprise software systems.

This playbook will delve into six key threats that AI poses to these legacy environments, specifically focusing on the vulnerabilities inherent in systems like Microsoft Dynamics AX, and will illuminate how a strategic migration to cloud-native solutions, exemplified by Dynamics 365, offers a robust and proactive defense.

> I would argue that [AI] will be among the most powerful tools that humanity's ever created... But every tool can also be used as a weapon. And the more powerful the tool, then in all probability, unfortunately, the more formidable the potential weapon.

Brad Smith, Vice Chairman and President: Microsoft

The Rise of AI in Business Operations

The pervasive integration of AI into business operations is undeniable. Enterprises are leveraging AI for everything from automating repetitive tasks and enhancing cybersecurity defenses to optimizing logistics and informing strategic decisions. To present just a few examples:

- In finance, AI algorithms are employed for fraud detection, risk assessment, and algorithmic trading.
- In supply chain management, AI powers demand forecasting, inventory optimization, and route planning.
- Marketing departments use AI for customer segmentation, personalized campaigns, and sentiment analysis.
- Human resources departments utilize AI for talent acquisition and employee engagement.

The benefits are manifold: increased operational efficiency, reduced costs, improved decision-making, enhanced customer satisfaction, and the ability to innovate at an accelerated pace. AI's capacity to learn and adapt from data allows systems to become smarter and more effective over time, driving continuous improvement across the enterprise value chain.

Yet, this widespread adoption also introduces a new dimension to the threat landscape. As AI becomes more sophisticated, so, too, do the methods employed by cybercriminals. Malicious actors are now harnessing AI to develop highly advanced attack tools that can bypass traditional security measures, exploit human vulnerabilities with unprecedented precision, and adapt to defensive countermeasures in real-time.

This creates a challenging paradox: the very technology designed to protect and enhance our systems can also be turned against them with devastating effect. The emergence of AI as a sophisticated threat vector necessitates a fundamental re-evaluation of existing cybersecurity postures, particularly for organizations whose foundational enterprise systems were not designed with such advanced threats in mind.

Vulnerabilities of On-Premises Enterprise Software

Traditional on-premises enterprise software systems, such as Microsoft Dynamics AX, were developed in an era when the cybersecurity landscape was far less complex and AI-driven threats were largely theoretical. While robust in their time, these systems possess inherent characteristics that render them increasingly susceptible to modern, AI-driven attacks. Here are three reasons why...

Speed, and the lack thereof

Firstly, on-premises systems typically operate on slower update and patching cycles. Patches and security updates often require manual intervention, extensive testing, and scheduled downtime, leading to significant delays in deployment. This lag creates prolonged windows of vulnerability that AI-powered tools can quickly identify and exploit. In contrast, cloud environments benefit from continuous, automated patching and updates, often applied seamlessly without user intervention, significantly reducing exposure time.

Scalability, and the lack thereof

Secondly, scalability is a major limitation. On-premises infrastructure is provisioned for peak loads, leading to over-provisioning and underutilization, or conversely, an inability to scale rapidly in response to a sudden surge in demand or an unexpected attack. This lack of elastic scalability can leave systems vulnerable to sophisticated Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks that overwhelm fixed resources. (Cloud platforms, by their very nature, offer on-demand scalability, capable of absorbing massive traffic spikes and distributing loads across vast global infrastructures.)

Skilled teams, and the lack thereof

Thirdly, on-premises systems rely heavily on internal IT resources for their security posture. This includes everything from infrastructure maintenance and patch management to threat detection, incident response, and compliance. Smaller IT teams may lack the specialized expertise, advanced tools, or 24/7 global monitoring capabilities necessary to combat AI-driven threats effectively.

The financial and human resource investment required to match the security capabilities of a major cloud provider is often prohibitive for individual organizations. Cloud providers, conversely, invest billions in dedicated security teams, cutting-edge AI-driven security tools, and global threat intelligence networks, offering a level of protection that is virtually unattainable for most on-premises deployments.

These inherent characteristics – slower update cycles, limited scalability, and reliance on internal IT resources – combine to create a fertile ground for modern, AI-driven threats. AI's ability to rapidly scan for vulnerabilities, generate sophisticated exploit code, and adapt attack vectors in real-time fundamentally shifts the balance of power, making traditional on-premises defenses increasingly inadequate against a new generation of adversaries.

The Promise of Cloud Migration

In light of the evolving threat landscape, cloud migration emerges not merely as an operational optimization but as a strategic imperative for enterprise security. Microsoft Dynamics 365 stands as a leading example of a cloud-based enterprise resource planning (ERP) solution designed from the ground up to address the complexities of modern business and, crucially, the sophistication of AI-driven threats.

Dynamics 365 lives in Microsoft Azure, a hyperscale cloud platform renowned for its robust security architecture, global reach, and continuous innovation. This foundation provides inherent advantages over on-premises deployments. Its architecture is designed for resilience, redundancy, and distributed processing, making it inherently more resistant to large-scale attacks. Furthermore, the security capabilities are not an afterthought but are deeply embedded into the platform's core, leveraging Microsoft's vast investments in cybersecurity research, threat intelligence, and AI-driven defense mechanisms.

> “A survey by Deloitte found that businesses using cloud computing enjoyed 21% more profit and grew 26% faster.”

By migrating to Dynamics 365, organizations can offload the immense burden of infrastructure security, patching, and monitoring to Microsoft, a global leader in cloud security. This shift allows internal IT teams to focus on strategic initiatives and business-specific applications rather than the constant battle against evolving cyber t hreats.

The cloud's inherent capabilities - such as continuous updates, elastic scalability, advanced identity management, and integrated AI-driven security services - are precisely what is needed to counter the sophisticated tactics employed by AI-powered adversaries.

The Intwo Difference

Navigating the complexities of cloud migration and fortifying an enterprise against AI-driven threats requires more than just technical implementation; it demands strategic partnership and deep expertise. This is where Intwo distinguishes itself, positioning itself as far more than a mere implementer, but rather as a comprehensive business strategy consultant, security advisor, and provider.

Intwo's profound expertise stems from its extensive experience with Microsoft technologies. As a dedicated Microsoft partner, Intwo possesses an intimate understanding of the Dynamics ecosystem, both legacy Dynamics AX and modern Dynamics 365. This deep knowledge allows for seamless and strategic migration pathways, ensuring that business processes are not simply replicated but optimized for the cloud environment. Intwo's specialized focus ensures that the migration process is not just a technical lift-and-shift, but a transformative journey that enhances operational efficiency and unlocks the full potential of the cloud.

> Our strong collaboration with Intwo played a crucial role in implementing Dynamics 365, accelerating the execution of our strategic plan, and turning our key objectives into reality.
>
> **Sheikha Al-Kaabi, Vice-Chairman: Al-Balagh**

Crucially, Intwo's capabilities extend significantly into the realm of cybersecurity. In an age where AI-driven threats are escalating, Intwo brings a robust cybersecurity practice, equipped with the knowledge and tools to assess, design, and implement advanced security postures. This includes expertise in Microsoft's security stack – from Azure Security Center and Azure Sentinel to Microsoft Defender suite – enabling organizations to fully leverage the cloud's inherent security capabilities. Intwo's cybersecurity specialists understand the evolving threat landscape, including the specific challenges posed by AI, and can tailor solutions that provide proactive defense, continuous monitoring, and rapid incident response.

By combining its deep Microsoft Dynamics expertise with its specialized cybersecurity prowess, Intwo offers a unique value proposition to clients. It goes beyond simply moving systems to the cloud; it advises on how to strategically leverage the cloud to enhance security, optimize operations, and drive business growth.

Intwo acts as a trusted advisor, helping organizations understand their current vulnerabilities, envision a more secure and agile future with Dynamics 365, and execute a migration strategy that prioritizes both business continuity and robust defense against the most sophisticated AI-driven threats. This approach ensures clients are not just adopting new technology, but are fundamentally strengthening their resilience in the face of an increasingly intelligent adversary.

Six AI-Posed Threats to Dynamics AX (and Other On-Premises Solutions) and Cloud Mitigation Strategies

The advent of Artificial Intelligence has fundamentally reshaped the cybersecurity landscape, introducing a new generation of threats that are more adaptive, personalized, and potent than ever before. For organizations still relying on on-premises ERP systems like AX, these AI-driven attacks represent an escalating challenge to their security posture. The inherent limitations of legacy systems – including slower update cycles, limited scalability, and reliance on internal IT resources – make them particularly vulnerable.

We're now going to detail six critical AI-posed threats and outline how a strategic migration to cloud-native solutions, specifically Microsoft Dynamics 365, offers robust and proactive mitigation strategies.

> The dangers of artificial intelligence (AI) are real. There are many benefits with AI, but also plenty of threats... I think these are all scary. **Sam Altman, CEO: OpenAI**

Threat 1 Sophisticated Phishing and Social Engineering Attacks

Description: The traditional phishing email, often riddled with grammatical errors and generic appeals, is rapidly becoming a relic of the past.

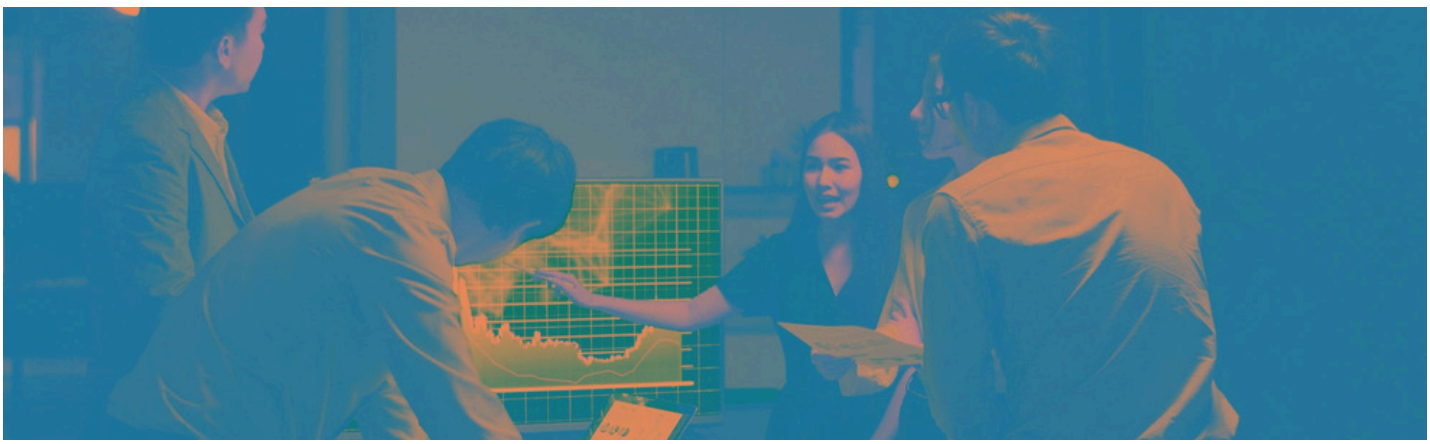
AI-powered tools have revolutionized phishing and social engineering, enabling attackers to generate highly personalized, context-aware communications that are almost indistinguishable from legitimate interactions. These advanced tools can scour publicly available information (from social media to corporate websites) to craft emails that mimic the tone, style, and specific details of an individual's colleagues, superiors, or trusted vendors.

Beyond text, AI can generate deepfake voice and video, allowing attackers to convincingly impersonate individuals in real-time, bypassing traditional authentication methods and exploiting human trust.

Impact on On-Premises: The direct consequence of these advanced social engineering tactics on on-premises environments is a significant increase in the risk of credential t heft.

Once an employee is tricked into divulging login details, attackers gain unauthorized access to the internal network and sensitive data within the on-premises ERP system. This can lead to malware infiltration, as compromised credentials can be used to deploy ransomware or other malicious software directly onto the network.

Furthermore, unauthorized access can result in data exfiltration, intellectual property theft, or even direct manipulation of critical business data within Dynamics AX, leading to financial losses, reputational damage, and operational disruption. The static nature of on-premises defenses is typically no match for the dynamic and highly personalized nature of AI-driven social engineering.



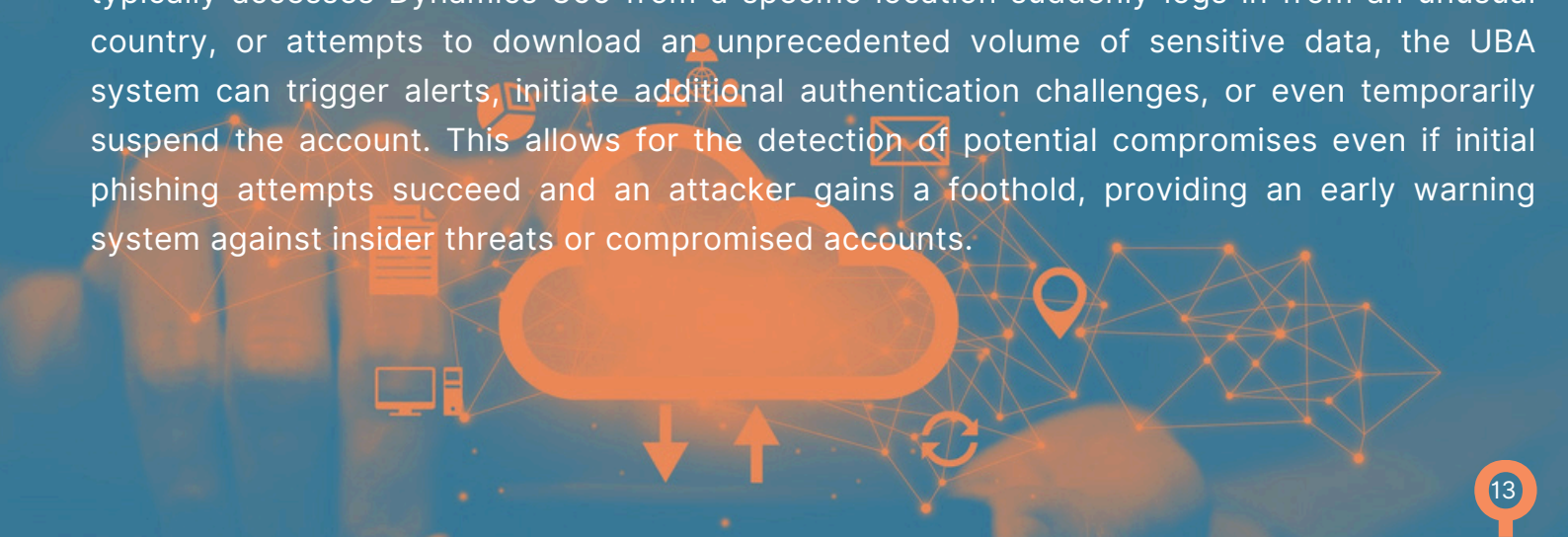
Cloud Mitigation Strategy: Cloud-native ERP solutions like Dynamics 365, built on the Azure platform, offer a multi-layered defense against these sophisticated AI-powered attacks:

Advanced Threat Protection (ATP): Integrated ATP services, such as Microsoft Defender, leverage AI and machine learning to detect and neutralize AI-generated phishing emails, malicious attachments, and deceptive links before they ever reach end-users' inboxes. These systems analyze vast quantities of email traffic, identify subtle anomalies in sender behavior, content, and links, and can even detonate suspicious attachments in a safe sandbox environment to identify zero-day threats. This proactive filtering significantly reduces the attack sur face.

Conditional Access and Multi-Factor Authentication (MFA): Cloud-native identity management solutions like Azure Active Directory (Azure AD) are foundational. They enforce robust multi-factor authentication (MFA), requiring users to provide two or more verification factors (e.g., password plus a code from a mobile app or biometric scan). This drastically reduces the success rate of stolen credentials, as even if an AI-powered phishing attack compromises a password, the attacker cannot gain access without the second factor.

Furthermore, Azure AD's Conditional Access policies can dynamically assess risk factors (e.g., unusual location, unfamiliar device, impossible travel scenarios) and enforce additional authentication requirements or block access entirely, significantly reducing the impact of successful social engineering attempts.

User Behavior Analytics (UBA): AI-driven UBA tools, often integrated within cloud security platforms like Azure Sentinel and Microsoft Defender for Cloud Apps, continuously monitor user activity patterns. These systems establish a baseline of normal behavior for each user and then flag any anomalous activities that deviate from this norm. For example, if a user who typically accesses Dynamics 365 from a specific location suddenly logs in from an unusual country, or attempts to download an unprecedented volume of sensitive data, the UBA system can trigger alerts, initiate additional authentication challenges, or even temporarily suspend the account. This allows for the detection of potential compromises even if initial phishing attempts succeed and an attacker gains a foothold, providing an early warning system against insider threats or compromised accounts.



Threat 2 Automated Exploitation of Software Vulnerabilities

Description: The speed at which new software vulnerabilities are discovered and exploited has dramatically increased. AI accelerates this process exponentially.

AI-powered tools can rapidly scan vast networks and software environments to identify known vulnerabilities (e.g., unpatched systems, misconfigurations, weak protocols) and even infer the presence of zero-day exploits (previously unknown vulnerabilities).

More alarmingly, advanced AI can automatically generate exploit code tailored to specific vulnerabilities, accelerating the attack timeline from discovery to exploitation from weeks or months to mere hours or even minutes. This means that as soon as a vulnerability is publicly disclosed, or even before, AI can weaponize it.

Impact on On-Premises: For on-premises Dynamics AX deployments, the impact of AI-driven automated exploitation is severe.

The time window for patching vulnerabilities before they are exploited shrinks dramatically, often to an unmanageable degree. This leads to faster breach times, as attackers can quickly identify and compromise systems before internal IT teams have a chance to deploy necessary updates.

The difficulty in patching before exploitation increases the likelihood of widespread system compromise, as a single unpatched vulnerability can serve as an entry point for an attacker to gain control over the entire on-premises environment, leading to data theft, system disruption, or the deployment of further malicious payloads. The manual and often cumbersome nature of on-premises patch management simply cannot keep pace with AI's rapid exploitation capabilities.

Cloud Mitigation Strategies: Cloud-native environments, particularly those managed by hyperscale providers like Microsoft, are designed to counter this threat through continuous, proactive security measures such as:

Continuous Patching & Updates: One of the most significant advantages of Dynamics 365 on Azure is Microsoft's commitment to continuous and automated patching and updates. Microsoft manages the underlying infrastructure, operating systems, and core application components. Patches are applied seamlessly, often without requiring any downtime for the end-user, and frequently before vulnerabilities are widely known or exploited by malicious actors.

Secure Development Lifecycle (SDL): Dynamics 365 is not merely patched after vulnerabilities are found; it is built with a rigorous Secure Development Lifecycle (SDL).

This means security is incorporated at every stage of the software development process, from initial design and threat modeling to coding, testing, and deployment. By integrating security from the ground up, Microsoft significantly reduces the inherent vulnerabilities in the software itself.

This proactive approach to security by design makes Dynamics 365 inherently more resilient to automated exploitation attempts compared to legacy systems that may have been developed before modern security best practices were widely adopted.

Proactive Security Monitoring: Microsoft operates global security operations centers (SOCs) that work 24/7, leveraging advanced AI and machine learning to monitor for emerging threats and vulnerabilities across their entire cloud infrastructure, including Dynamics 365 services. These SOCs analyze petabytes of telemetry data from millions of devices and applications worldwide, allowing them to identify new attack patterns, zero-day exploits, and suspicious activities in real-time. This collective intelligence and proactive monitoring enable Microsoft to develop and deploy countermeasures rapidly, often before individual customers are even aware of a potential threat.

> With the cybersecurity landscape more complex than ever, it's never been clearer that every organization will need to deploy and maintain a Zero Trust security architecture... This is driving accelerated demand for our integrated, end-to-end solutions spanning identity, security, compliance, and device management, across all clouds and all platforms.
>
> **Satya Nadella, CEO: Microsoft**

Threat 3 AI-Driven Ransomware and Malware Evolution

Description: Ransomware has evolved from simple, indiscriminate attacks to highly sophisticated, targeted campaigns.

AI is now enabling ransomware to adapt its attack vectors, evade detection by traditional signature-based antivirus software, and intelligently target high-value data within an organization. AI-powered ransomware can learn from its environment, identify critical systems and sensitive data, and then encrypt them in a way that maximizes disruption and extortion potential.

It can also employ polymorphic code generation, constantly changing its signature to bypass traditional detection mechanisms, making it incredibly difficult for static, signature-based antivirus solutions common in on-premises environments to identify and block.

Furthermore, AI can assist ransomware in identifying and disabling backup systems, ensuring that victims have no recourse but to pay the ransom.

Ransomware attacks were reported by nearly twice as many organizations with on-premises environments (37%) compared to those with cloud environments (19%).

Impact on On-Premises: The impact of AI-driven ransomware on on-premises Dynamics AX systems is devastating. There is an increased likelihood of successful ransomware attacks due to the malware's ability to evade traditional defenses and intelligently target critical ERP data. If successful, recovery times are significantly longer, as the sophisticated encryption and evasion techniques make decryption and system restoration more complex.

This often leads to greater data loss, as backups may be compromised or outdated, and the cost of recovery (including potential ransom payments, forensic investigations, and business interruption) can be crippling. On-premises systems often lack the advanced behavioral detection capabilities and immutable backup solutions necessary to effectively counter these evolving threats.

Cloud Mitigation Strategy: Cloud-native solutions like Dynamics 365 leverage advanced security capabilities to combat AI-driven ransomware including:

Behavioral AI Detection: Cloud security services, such as Microsoft Defender for Endpoint and Azure Sentinel, employ sophisticated AI and machine learning models to detect anomalous behavior indicative of ransomware, rather than relying solely on signatures. These systems monitor file access patterns, process behavior, network communications, and system changes in real-time.

For example, if a process suddenly starts encrypting a large number of files or attempting to delete shadow copies, the behavioral AI can flag it as ransomware, even if its signature is unknown, and automatically isolate the affected system or terminate the malicious process. These services integrate natively with Dynamics 365's cloud environment when managed through Microsoft 365 Defender, Azure Security Center, and Sentinel.

Immutable Backups and Point-in-Time Restore: Dynamics 365 offers robust backup and recovery capabilities that are designed for resilience against ransomware.

Backups are often immutable, meaning once created, they cannot be altered or deleted by malicious actors, even if they gain administrative access. This ensures that a clean, uncorrupted copy of the data is always available.

Furthermore, point-in-time restore capabilities allow organizations to rapidly revert their Dynamics 365 environment to a state just prior to an attack, minimizing downtime and data loss. This capability is far more advanced than typical on-premises backup solutions, which can often be targeted and encrypted by sophisticated ransomware.

Network Segmentation and Micro-segmentation: The cloud environment is designed with advanced network segmentation and micro-segmentation principles. This means that even if a part of the network is breached, the malware's ability to move laterally and infect other systems is severely limited.

Dynamics 365 components and customer data are isolated within their own secure segments, preventing a single point of compromise from leading to a widespread infection. This containment strategy significantly reduces the "blast radius" of a ransomware attack, protecting critical ERP data.

Threat 4 Data Exfiltration and Corporate Espionage via AI-Powered Bots

Description: Traditional data exfiltration attempts often involve large, sudden transfers of data that are relatively easy to detect. However, AI-driven bots have changed the game.

These sophisticated bots can mimic legitimate user behavior, moving undetected within a network for extended periods. They can systematically identify, categorize, and exfiltrate sensitive data in small, incremental chunks over long durations, making their activities incredibly difficult to detect using traditional security tools that look for sudden spikes or large transfers.

These bots can adapt their communication methods, use encrypted channels, and blend in with normal network traffic, making them ideal for long-term espionage campaigns aimed at intellectual property theft, competitive intelligence gathering, or financial data compromise.

> It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.
> **Stéphane Nappo, Global Chief Information Security Officer: Société Générale International Banking**

Impact on On-Premises: For on-premises Dynamics AX systems, the impact of AI-powered data exfiltration and espionage can be catastrophic and often goes undetected for extended periods.

This can lead to significant intellectual property theft, as proprietary designs, algorithms, or customer lists are siphoned off without immediate detection. Sensitive financial and operational data, crucial for business continuity and competitive advantage, can be compromised over the long term, leading to severe financial losses, erosion of market position, and regulatory penalties.

The lack of advanced, AI-driven analytics and comprehensive data loss prevention (DLP) capabilities in many on-premises environments means these subtle, persistent exfiltration attempts can remain hidden until it's too late.

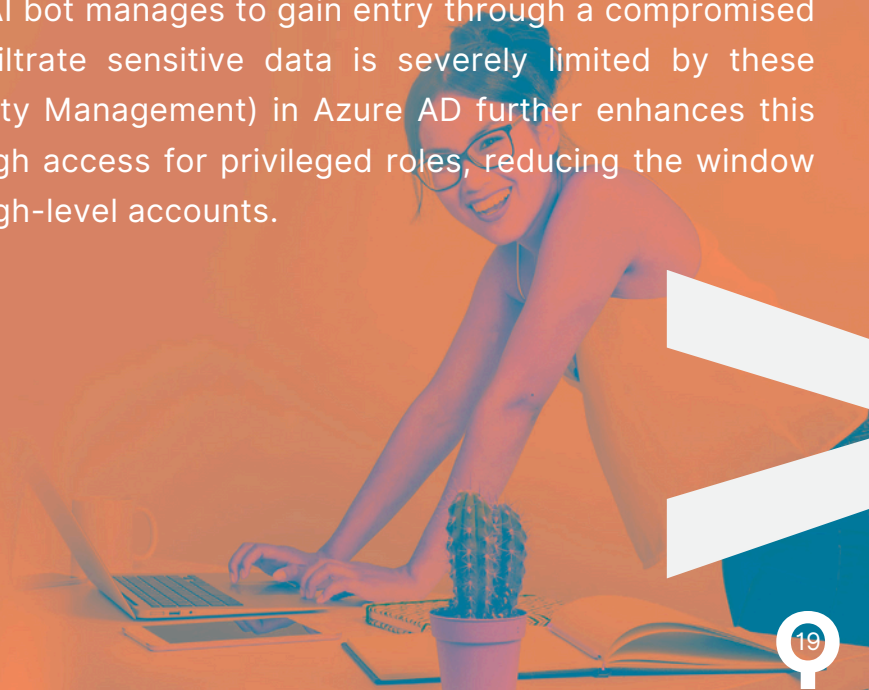
Cloud Mitigation Strategy: Cloud-native platforms offer advanced capabilities to detect and prevent subtle data exfiltration attempts:

Advanced Analytics And Anomaly Detection: Cloud security services like Azure Security Center and Azure Sentinel leverage AI and machine learning to analyze vast amounts of log data, network traffic, and user activity. They can identify subtle patterns of data exfiltration or unusual access that traditional tools might miss.

For instance, if an employee who normally accesses only a few customer records suddenly starts querying thousands of records, or if data is being sent to an unusual external IP address in small, consistent increments, these systems can flag the anomaly and trigger alerts. This proactive monitoring allows for early detection of espionage attempts.

Data Loss Prevention: Integrated DLP policies are a core component of cloud security. These policies can be configured to automatically identify, monitor, and protect sensitive information across various data stores and communication channels within the controlled cloud environment. DLP can prevent sensitive data (e.g., credit card numbers, social security numbers, proprietary designs) from leaving the Dynamics 365 environment, regardless of the method an AI bot might employ. It can block uploads to unauthorized cloud storage, prevent emails containing sensitive data from being sent externally, or even encrypt data at rest based on its content.

Granular Access Controls (RBAC and Least Privilege): Role-Based Access Control (RBAC) and the principle of least privilege are enforced at a granular level within Dynamics 365. This means that users and applications are granted only the minimum necessary permissions to perform their specific tasks. Even if an AI bot manages to gain entry through a compromised account, its ability to access and exfiltrate sensitive data is severely limited by these granular controls. PIM (Privileged Identity Management) in Azure AD further enhances this by providing just-in-time and just-enough access for privileged roles, reducing the window of opportunity for attackers to exploit high-level accounts.



Threat 5 AI-Enhanced Denial-Of-Service (DoS/DDoS) Attacks

Description: Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks aim to overwhelm a system's resources, making it unavailable to legitimate users. AI significantly enhances the sophistication and effectiveness of these attacks.

AI can orchestrate more complex and adaptive DDoS attacks by intelligently varying attack vectors (e.g., SYN floods, UDP floods, HTTP floods), sources (using botnets with geographically dispersed IP addresses), and traffic patterns in real-time. This adaptive nature makes traditional, static mitigation strategies challenging, as the attack can quickly shift tactics to bypass defenses.

AI can also identify weaknesses in network infrastructure and target specific components, leading to more efficient and devastating disruptions.

Impact on On-Premises: For on-premises Dynamics AX deployments, the impact of AI-enhanced DoS/DDoS attacks can be severe and immediate.

Fixed on-premises infrastructure has finite bandwidth and processing capacity. An AI-orchestrated DDoS attack can rapidly overwhelm these resources, leading to system downtime and complete service unavailability for legitimate users.

This disruption can result in significant revenue loss due to halted operations, inability to process transactions, and damage to customer trust. Recovering from such an attack can also be time-consuming and costly, requiring manual intervention to restore services and analyze the attack vector.

Cloud Mitigation Strategy: Cloud-native platforms, particularly infrastructures like Azure, are inherently designed to mitigate large-scale DoS/DDoS attacks:

Scalability and Redundancy: Azure's global infrastructure provides immense bandwidth and distributed resources across numerous data centers worldwide.

Its inherent scalability allows the platform to absorb and mitigate even massive-scale DDoS attacks by distributing the incoming malicious traffic across a vast network. Instead of overwhelming a single on-premises server, the attack traffic is spread across multiple geographically dispersed data centers, effectively diluting its impact.

This built-in redundancy ensures that even if one region experiences an issue, services can seamlessly failover to another, maintaining availability.

Azure DDoS Protection: Microsoft offers dedicated Azure DDoS Protection services that automatically detect and mitigate attacks at the network edge, preventing them from ever reaching the application layer where Dynamics 365 resides.

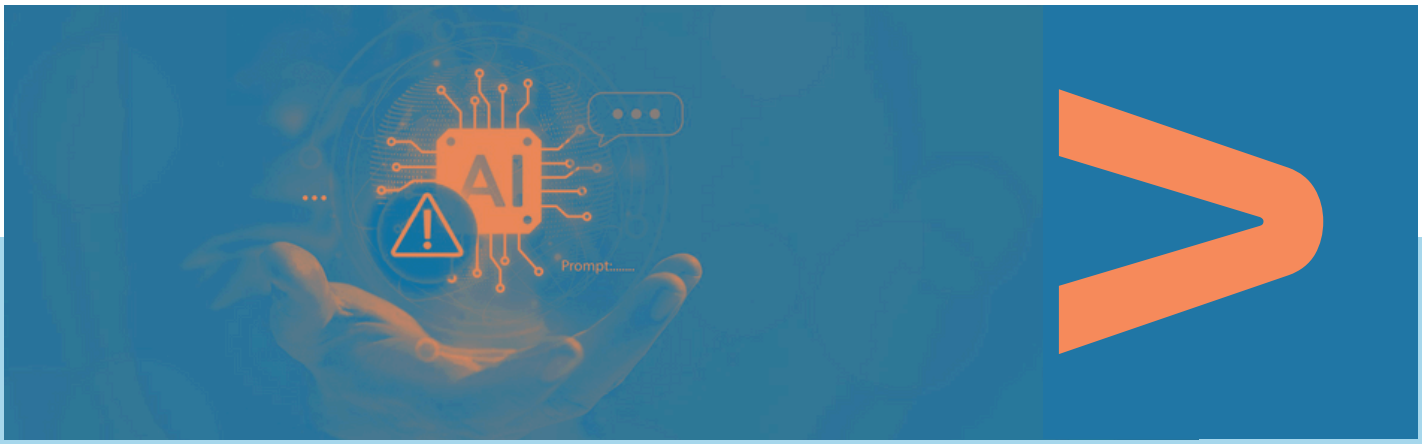
This service uses advanced traffic analysis, machine learning algorithms, and real-time threat intelligence to identify and block malicious traffic while allowing legitimate traffic to pass t hrough.

It offers both Basic (automatically enabled for all Azure services) and Standard tiers, with the Standard tier providing enhanced telemetry, alerting, and tuning capabilities for more critical workloads. This proactive, automated mitigation is a stark contrast to the often reactive and resource-intensive efforts required for on-premises DDoS defense.

Threat 6 AI-Driven Supply Chain Attacks

Description: Supply chain attacks, where malicious code is injected into software components or updates from trusted third-party vendors, have become increasingly prevalent. AI significantly enhances these attacks by enabling attackers to more effectively identify and exploit weaknesses in the software supply chain.

AI can rapidly scan vast repositories of open-source libraries, third-party components, and vendor software for vulnerabilities, misconfigurations, or even subtle backdoors. It can then intelligently craft malicious code that blends seamlessly into legitimate components, making detection difficult during development and deployment. This allows attackers to compromise systems through trusted channels, bypassing traditional perimeter defenses and impacting a wide range of organizations that use the compromised software.



Impact on On-Premises: For on-premises systems, the impact of AI-driven supply chain attacks is particularly insidious. Compromise occurs through trusted channels, meaning that the malicious code comes from a seemingly legitimate source (e.g., a software update, a third-party integration module). This makes it incredibly difficult for internal IT teams to identify the source of the breach, as the attack doesn't originate from an external, obvious threat.

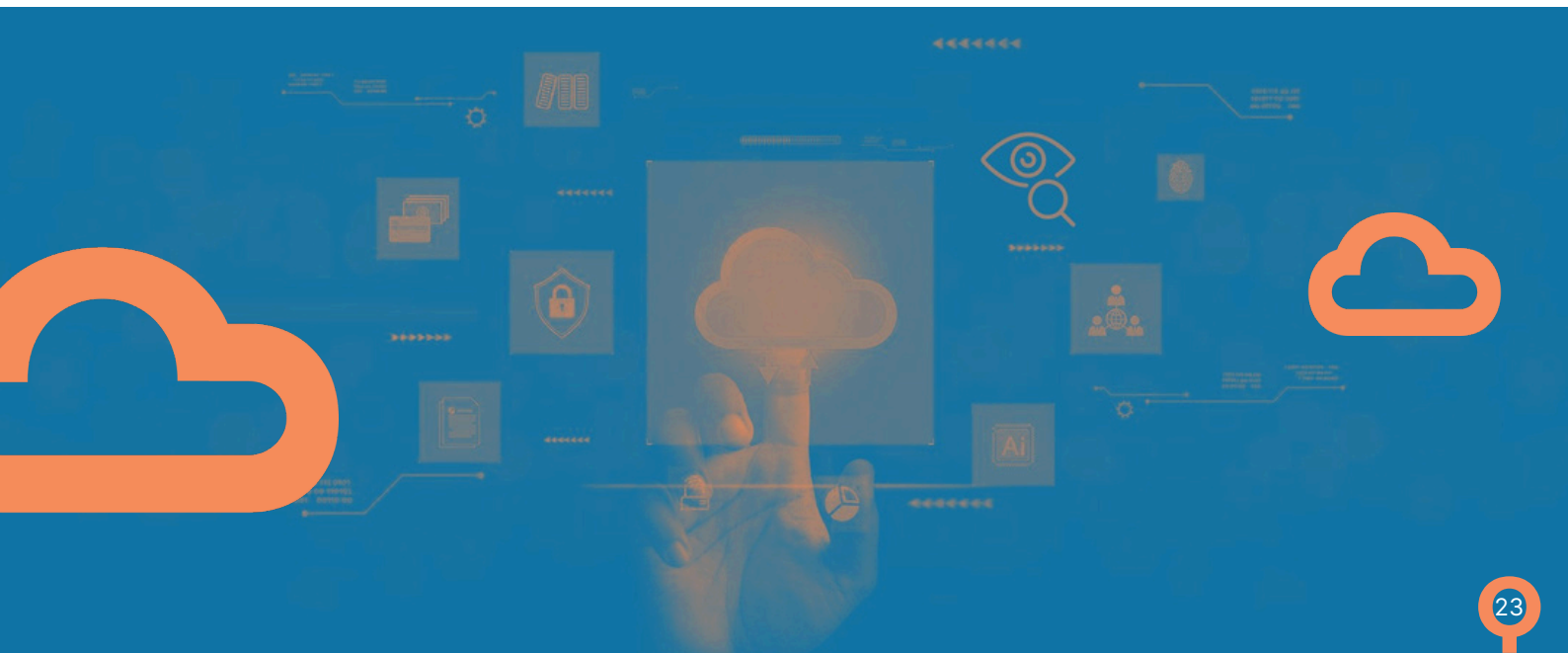
The widespread impact across integrated systems is also a major concern, as a single compromised component can propagate malicious code across the entire on-premises environment, affecting not only Dynamics AX but also connected applications and databases. Manual vetting of every software component and update is impractical, leaving on-premises environments exposed.

Cloud Mitigation Strategy: Microsoft's cloud-native approach incorporates multiple methods of defense, including:

Rigorous Supply Chain Security: Microsoft maintains strict security controls over its own development and supply chain for Dynamics 365. This includes extensive vetting of all third-party components, open-source libraries, and internal development processes. Microsoft employs a "shift left" security approach, embedding security checks and reviews throughout the entire software development lifecycle to prevent the introduction of vulnerabilities or malicious code at the earliest stages. This commitment to a secure supply chain is a fundamental aspect of delivering a trustworthy cloud service.

Continuous Vulnerability Scanning: Automated tools continuously scan Dynamics and its underlying components for known vulnerabilities, misconfigurations, and potential security weaknesses. These scans are integrated into the development and deployment pipelines, ensuring that any newly discovered vulnerabilities in third-party libraries or internal code are identified and remediated rapidly. This proactive and continuous scanning significantly reduces the risk of a compromised component making its way into the production environment.

Isolation & Sandboxing: Cloud environments often employ advanced isolation techniques and sandboxing to limit the "blast radius" of a compromised component. Even if a vulnerability were to slip through and a component were compromised, the cloud architecture ensures that it operates within a highly isolated environment, preventing it from affecting other parts of Dynamics 365 or other customer environments. This containment strategy is crucial for mitigating the widespread impact that a supply chain attack could have in a less segmented on-premises environment.



Beyond Threat Mitigation: Additional Benefits Intwo Provides as You Move to the Cloud.

Whilethe primary focusof migrating from Dynamics AX to Dynamics 365 in the age of AI is undoubtedly enhanced security, the benefits extend far beyond threat mitigation. Intwo's expertise in this transition unlocks a multitude of operational, strategic, and financial advantages that position enterprises for future resilience and growth.

Scalability And Performance

On-premises Dynamics AX deployments often struggle with rigid infrastructure that cannot easily adapt to fluctuating business needs. Scaling up requires significant capital expenditure, procurement delays, and complex implementation. Scaling down leads to underutilized resources.

Dynamics 365, built on Azure, offers unparalleled on-demand scalability. Whether a sudden surge in transactions during peak season, rapid business expansion, or the need to process vast datasets for AI-driven analytics, the cloud dynamically allocates resources, ensuring consistent performance without over-provisioning.

This elastic scalability means businesses pay only for what they consume, optimizing resource utilization and ensuring that performance never becomes a bottleneck.

> The real benefits of the cloud are slightly different than we originally predicted; they are less about pure cost efficiency, and more about speeding up time to market (aka agility). Every CIO and IT decision maker should be thinking about how they can use cloud and hosting to accelerate time to market, which means turning IT from a cost center into a revenue center.
>
> **Toby Owen,**
> **Group Product Manager: Google**

Reduced Operational Overhead

Managing on-premises ERP infrastructure is a resource-intensive endeavor. It involves significant capital expenditure on hardware, ongoing maintenance, power consumption, cooling, and the need for a dedicated IT team to handle patching, updates, backups, and troubleshooting.

By helping organizations migrate to Dynamics 365, Intwo enables you to offload the burden of managing infrastructure, security, and maintenance to Microsoft. The operational overhead associated with infrastructure management is drastically reduced, freeing up internal IT resources to focus on strategic initiatives, innovation, and business-specific applications rather than routine maintenance tasks. This allows IT to become a business enabler rather than just a cost center.

Enhanced Business Continuity and Disaster Recovery

For on-premises systems, achieving robust business continuity and disaster recovery (BC/DR) can be complex, costly, and often involves maintaining redundant infrastructure in a separate location. This is a significant investment that many organizations struggle to justify.

But with Intwo, Dynamics 365, and Azure's global infrastructure, your solutions come with built-in redundancy, automatic failover capabilities, and comprehensive disaster recovery mechanisms. Data is replicated across multiple data centers, ensuring high availability and resilience against regional outages or catastrophic events. In the event of a disaster, operations can failover to a healthy region, minimizing downtime and ensuring continuous business operations.

This level of BC/DR is virtually unattainable for most on-premises deployments without prohibitive costs.

Innovation and Integration

The cloud environment is a hub of continuous innovation. Dynamics 365 receives regular updates and new features, often incorporating the latest advancements in AI, machine learning, and business intelligence. This means organizations always have access to cutting-edge capabilities without manual upgrades.

Furthermore, Dynamics 365 is designed for seamless integration with other Microsoft services, including Power Platform (Power BI, Power Apps, Power Automate), Microsoft 365, and Azure's vast array of AI and analytics services (Copilot, autonomous agents, Fabric, and more).

Intwo's expertise ensures that these integrations are optimized and strategically deployed to fit your business goals, allowing businesses to create a truly connected and intelligent enterprise ecosystem.

Cost Efficiency

While initial migration costs exist, the long-term cost efficiency of cloud migration is compelling. The shift from a capital expenditure model (buying hardware, software licenses upfront) to an operational expenditure model (subscription-based services) provides greater financial flexibility. Reduced hardware and maintenance costs, lower energy consumption, and the elimination of the need for large, dedicated IT infrastructure teams contribute to significant overall savings.

Furthermore, the ability to scale resources on demand means organizations only pay for the computing power and storage they actually use, avoiding the waste associated with over-provisioned on-premises environments. Intwo helps organizations analyze their total cost of ownership to demonstrate the long-term financial benefits of cloud adoption.

What's next...?

The "Alage,"whileofferingunprecedented opportunities, has also ushered in a new era of threats.

As this playbook has detailed, AI-driven adversaries are no longer reliant on brute force or simplistic tactics; they are capable of orchestrating sophisticated phishing campaigns, rapidly exploiting software vulnerabilities, evolving ransomware to evade detection, conducting stealthy data exfiltration, launching adaptive denial-of-service attacks, and injecting malicious code through compromised supply chains.

For organizations still operating on-premises enterprise software like Microsoft Dynamics AX, these evolving threats pose inherent and escalating challenges that traditional security postures are increasingly ill-equipped to handle. The slower update cycles, limited scalability, and reliance on internal IT resources inherent in legacy systems create critical vulnerabilities that AI can exploit with devastating efficiency.

Conversely, a strategic migration to cloud-native solutions, exemplified by Microsoft Dynamics 365, provides a robust, proactive, and continuously evolving defense against these intelligent threats.

> Security underpins every layer of our tech stack, and it's our number one priority...We are doubling down on this very important work, putting security above all else - before all other features and investments.
>
> **Satya Nadella, CEO: Microsoft**

Built on the secure and scalable foundation of Microsoft Azure, Dynamics 365 inherently leverages advanced threat protection, continuous patching, behavioral AI detection, immutable backups, granular access controls, and a rigorous secure development lifecycle. These capabilities are not merely incremental improvements; they represent a fundamental paradigm shift in enterprise security, transforming an organization's defensive posture from reactive and vulnerable to resilient and adaptive in the face of an increasingly intelligent adversary.

Cloud migration is no longer just about achieving cost savings or gaining operational agility; it has become a critical strategic imperative for enterprise security in the age of AI. It is an investment in future resilience, ensuring that an organization's most vital business processes and data are protected by the most advanced, continuously updated, and globally monitored security infrastructure available.

To assess the specific conditions and potential vulnerabilities of your existing Dynamics AX or any on-premises system, and to explore a strategic migration pathway to Dynamics 365 for enhanced security and future resilience, we urge you to consult with Intwo.

Our deep expertise in Microsoft technologies, coupled with our specialized cybersecurity advisory and implementation services, positions us as your ideal partner in navigating this evolving threat landscape and securing your enterprise for the future.

Stay Ahead of Emerging Threats with Smarter AI-Powered Tools in Dynamics 365. Connect with Us Today to Secure Your Future!

AMSTERDAM
Polarisavenue 51
C4 - 3rd floor 2132 JH Hoofddorp,
Netherlands
Main phone number:
+31 20 547 8060

AUSTRALIA
Unit 104, 109 Oxford
Street Bondi Junction NSW 2022,
Australia
Main phone number:
+61 2 8310 5568

BANGALORE
Office 621, 2nd Floor,
NMH Complex 80ft Road, 4th Block,
Koramangala Bangalore – 560 034,
India
Main phone number:
+91 80 4122 9072/73

CANADA
800 Steeles Ave.
W. #B10182 Thornhill,
ON L4J 7L2,
Canada
Main phone number:
+1 416 988 0366

CARIBBEAN & LATIN AMERICA
Parq Ind Quebrada
Arenas 2010 Carr 1 San Juan,
PR 00926-9206,
Puerto Rico
Main phone number:
+1 787 273 0000

DUBAI
Office 1005, BB1 Mazaya Business
Avenue, Jumeirah Lakes Towers
P.O. Box 122492,
Dubai, UAE
Main phone number:
+971 4 583 6802

KSA
5th Floor, Al Shablan Tower Al Khobar
31952– Dammam Highway
P.O. Box 3140,
Saudi Arabia
Main phone number:
+966 50 919 9872

SEATTLE
8531 154th Avenue NE,
Suite 110 Redmond, WA 98052,
United States
Main phone number:
+1 425 820 6120

Q ATA R
P.O. Box 55991 ,
Office 102 1st Floor
Sheikh Jabor Bin Yousef Bin Jassem
Al Thani Building Old Airport Road,
Doha, Qatar
Main phone number:
+974 4 444 2150

SAN DIEGO
5963 La Place Court,
Suite 302 Carlsbad, CA 92008,
United States
Main phone number:
+1 858 385 8900

SINGAPORE
70 Shenton Way #21-12
Eon Shenton Singapore 079118,
Singapore
Main phone number:
+65 6222 6591