Insight

Identity Security:
A Strategic Buyer's Guide

Contents Page

Identity Security: A Strategic Buyer's Guide

In modern enterprises, every user login, service account, and third-party connection is a potential risk. As hybrid work, cloud apps, and AI reshape the enterprise, attackers increasingly go after identities - not firewalls. As an attacker, why hack in – when you can steal an identity and login? Protecting digital identities has become one of the most effective ways to prevent breaches, control access, and maintain trust.

In fact, identity has become the primary attack vector for enterprises, with **93%** of organisations experiencing at least **two identity-related attacks** in the past year.*

For security leaders, this means that protecting identities is now mission critical. This guide demystifies key identity security concepts – IAM, IGA, PAM, ITDR, multi-factor authentication, etc. – and explains why each matters to your organisation. It also highlights how Insight, as a leading solutions provider with deep Microsoft partnerships, can help build a comprehensive identity security program.

*https://investors.cyberark.com/news/news-details/2024/Report-93-Of-Organizations-Had-Two-or-More-Identity-Related-Breaches-in-the-Past-Year/)

Why Identity Security Matters

Modern enterprises are grappling with an explosion of digital identities – from employees and customers to software bots and cloud services. Each identity represents a potential entry point for attackers, especially as hybrid work and cloud adoption dissolve the traditional network perimeter. Techniques like social engineering and credential theft target not just users but also machine accounts and application identities. Weak or stolen credentials are a factor in the majority of breaches underscoring the urgency of strong identity safeguards.

an estimated 86% of breaches involve stolen credentials**

Beyond the immediate threat of breaches, poor identity practices carry business risks: unauthorised access to sensitive data, non-compliance with regulations, operational downtime, and loss of customer trust. By contrast, a robust identity security programme enables "zero trust" principles ("never trust, always verify"), ensuring that only the right people (or systems) get the right access, under the right conditions. It also improves user experience by replacing chaos (multiple logins, manual access processes) with streamlined, secure access – allowing productivity without sacrificing security. In short, focusing on identity security helps organisations reduce risk, meet compliance mandates, and empower the business with confident access to technology resources.

**https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Key Pillars of Identity Security

To protect the organisation, identity security must span multiple domains. It's not a single product, but an interconnected set of capabilities that together answer fundamental questions: Who (or what) can access what, when, and how? The diagram below illustrates the full landscape of identity security capabilities – from managing identities and privileges to monitoring for threats.

Insight Identity Strategy Framework

Identity & Access
Who can access what?

Identity Foundations
- Directory services
- Federation / B2B
- Provisioning and de-provisioning
- Customer identity / B2C

Authentication
including MFA, phishing resistant MFA, and passwordless

Authorisation

Single-sign-on

User self-service

Identity Governance & Administration (IGA)
Should they still have access?

Identity Governance
- Access reviews & certifications
- Compliance management
- Auditing

Identity Admin
- Workflow management

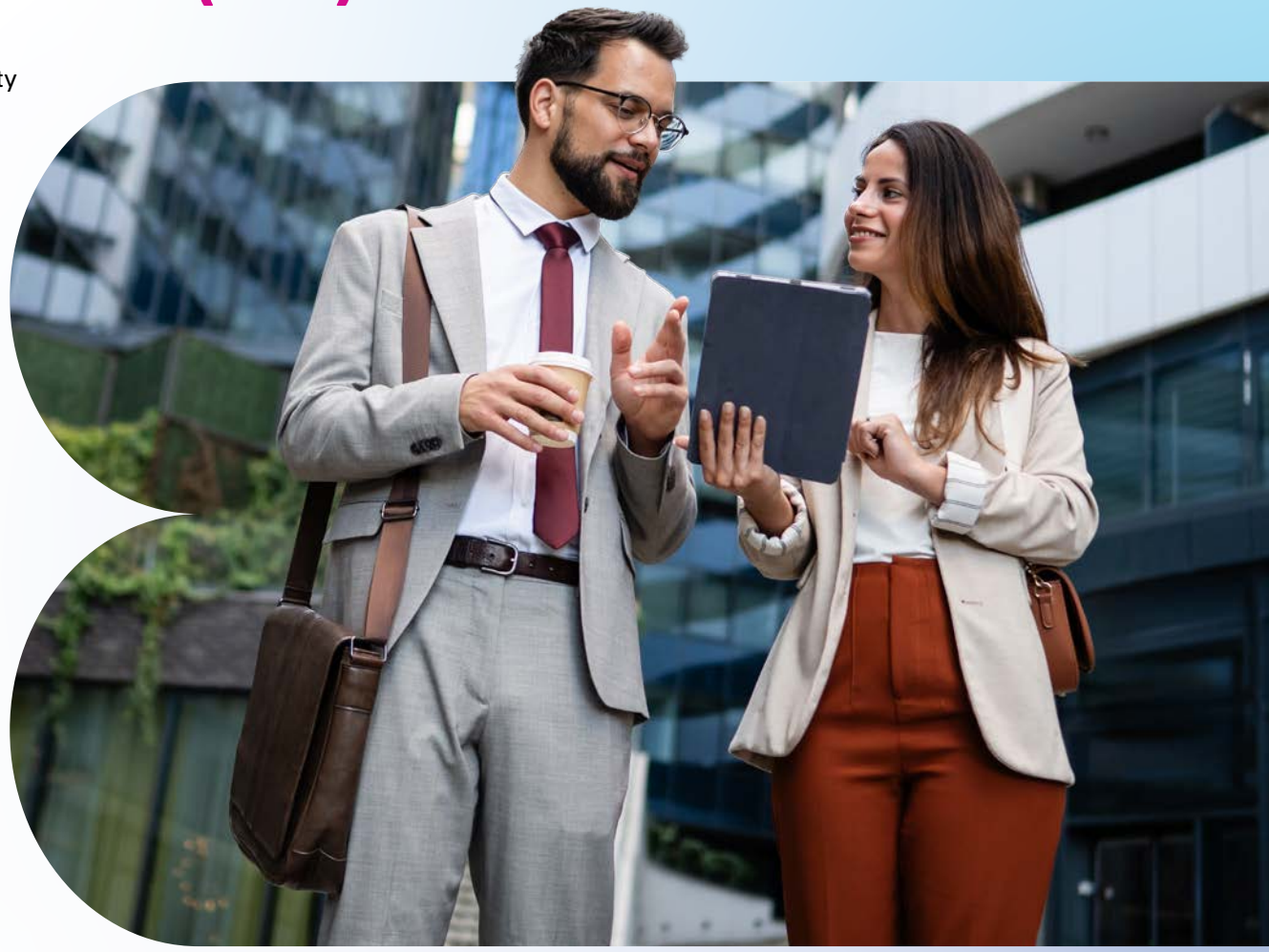
Privileged Access
- Account discovery
- Credential management
- Session recording
- Privileged elevation and delegation management

Identity Threat Detection & Response (ITDR)
Are we under attack?

Threat Detection
- Anomaly detection & user and entity behaviour analytics (UEBA)

Threat Response
- Suspend account or force password reset
- Force reauthorisation, or "step-up" authorisation

Identity and Access Management (IAM)



Identity and Access Management (IAM) is the foundation of an identity security strategy. It focuses on establishing and managing digital identities (for employees, partners, customers, and even software accounts) and controlling their access to resources. IAM covers the creation of user identities in directory systems, provisioning of accounts to applications, and authentication services like single sign-on. It "establishes the baseline for who or what should have access to what" in the organisation. In practice, IAM solutions (such as Microsoft Entra ID, formerly Azure AD) allow users to log in securely and conveniently, enforce password policies or passwordless login, and centrally manage access to various systems.

Why it matters: A strong IAM foundation ensures that only authenticated, authorised users can reach sensitive assets, reducing the risk of unauthorised access. Centralised IAM improves security and user experience by eliminating password proliferation and enabling business users with the access they need (for example, through single sign-on to cloud apps). It also lays the groundwork for enforcing security policies like multifactor authentication and conditional access across the enterprise. Without effective IAM, organisations often struggle with inconsistent access controls and identity "silos," leading to security gaps, frustrated users, and audit findings. In summary, IAM is crucial for both productivity and security, providing the first line of defence against identity misuse.

Key IAM capabilities typically include: directory services to store and verify user identities, authentication mechanisms (from passwords to biometrics and MFA), federation for partner or customer logins (B2B/B2C), and provisioning/de-provisioning processes to grant and revoke access as people join, move, or leave. Modern IAM emphasises strong authentication and context-aware access (discussed more below) as attackers increasingly target login credentials.

Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) builds on IAM by governing who should have access to what over time. While IAM sets up identities and access, IGA ensures those access rights remain appropriate and compliant as the organisation and roles change. It "ensures that access is appropriate over time by managing entitlements, conducting access reviews, and enforcing policy-based controls". In practical terms, IGA involves processes like periodic certification of users' access by managers, approval workflows for access requests, segregation-of-duties policies to prevent toxic permission combinations, and auditing of identity data.

Why it matters: IGA is critical for compliance, security, and efficiency. Without governance, users accumulate excessive privileges or retain access to systems they no longer need (for example, when moving to a new role or after termination). This "privilege creep" creates security vulnerabilities and can lead to audit and compliance failures. IGA helps organisations enforce the principle of least privilege – each identity having the minimum access required – and provides evidence for regulations (like GDPR and NIS2) that access to sensitive data is being properly controlled and reviewed. By automating access reviews and approvals, IGA also reduces the manual burden on IT and managers, making access management more scalable. In short, IGA answers the question "Should this identity still have this access?" on an ongoing basis, thereby mitigating insider threats and errors while ensuring the organisation remains audit-ready and secure.

Privileged Access Management (PAM)

Privileged Access Management (PAM) is a specialised area of identity security focused on high-impact accounts – the "keys to the kingdom." Privileged accounts (such as system administrators, domain admins, cloud platform owners, or service accounts with broad permissions) have capabilities that, if misused or compromised, could be devastating. PAM focuses on protecting high-risk credentials and admin-level permissions, whether they belong to a human administrator or a service account controlling production systems. Key PAM controls include secure storage of privileged credentials (e.g., in encrypted vaults), just-in-time access (granting elevated privileges only when needed and for a limited time), multifactor authentication for privileged actions, session monitoring and recording, and automated logout or credential rotation after use.

Why it matters: Privileged accounts are a common target in cyberattacks – attackers seek them out because they confer the highest level of access. Without PAM, a single stolen admin password can unleash a catastrophic breach, allowing an intruder to disrupt systems or exfiltrate vast amounts of data. PAM solutions significantly reduce this risk by preventing the unchecked use of powerful accounts. They ensure that administrators use unique, strong credentials (often checked out just for the duration of a task) and that all privileged activities are traceable. This not only thwarts external attackers but also mitigates insider threats or accidental misuse by IT staff. For the organisation, implementing PAM means critical systems and data are far better protected from abuse. Moreover, many compliance regimes explicitly require controls around administrative access – PAM helps satisfy those requirements through enforced oversight and audit trails. In essence, PAM adds an essential safety layer around your most sensitive access, dramatically limiting the damage that can be done if an identity is hijacked or misused.

Strong Authentication and Access Control

Effective authentication underpins all the above identity domains. Authentication is the process of verifying that a user or system is who they claim to be. Weak authentication (like sole reliance on passwords) is a known weak link – passwords can be guessed, stolen, or phished. Strong authentication means requiring multiple factors (MFA) or modern methods that attackers can't easily subvert. For human users, this could include one-time passcodes, smartphone authenticator apps, physical security keys, or biometrics, in addition to, or instead of a password. For system identities (like APIs or service accounts), strong authentication involves eliminating static passwords and using certificates or token-based methods with secure key management.

Why it matters: According to Microsoft, multifactor authentication can prevent 99.9% of account compromise attacks on user accounts. By implementing MFA across the organisation, the risk of unauthorised access drops dramatically – even if a password is stolen, the attacker cannot easily provide the second factor. In business terms, strong authentication is one of the highest ROI security measures available: it directly defends against common attacks like phishing and credential stuffing, which in turn prevents costly breaches. Additionally, techniques like conditional access (an access policy that adapts based on context/risk) further strengthen authentication. For example, if a login attempt comes from an unusual location or a device in poor health, the system can require extra verification or block access. This ensures security without unduly hindering legitimate users.
By "never trusting" by default and always verifying identity continuously (a core tenet of Zero Trust), organisations can confidently enable remote work and cloud adoption. Strong authentication and adaptive access controls thus protect the business while enabling flexibility – employees, partners, and customers can connect from anywhere, but on IT's terms and with minimal friction.

Identity Threat Detection and Response (ITDR)

Even with preventive measures in place, organisations should assume some identity breaches will occur (e.g. a phishing email fools an employee, or a legacy account gets compromised). Identity Threat Detection and Response (ITDR) is an emerging pillar focused on detecting and mitigating identity-centric attacks in real time. It "monitors for identity misuse and compromise", watching for abnormal patterns that indicate an impersonation or unauthorised use of credentials. This can include tools that analyse login behaviour for anomalies (impossible travel, unusual times, changes in device or IP patterns), detect attacks on directory infrastructure (like privilege escalation in Active Directory or abuse of SSO tokens), and integrate with broader security operations to respond to threats targeting identities.

Why it matters: Traditional security monitoring has focused on endpoints and networks, but modern attackers often bypass those by exploiting identity weaknesses – for instance, using valid credentials to log in and then silently elevating privileges. ITDR solutions fill this gap by providing purpose-built detection for identity attacks, which might not trigger alarms in endpoint or network tools. Gartner and industry leaders emphasise ITDR as a crucial component in a Zero Trust strategy, ensuring that suspicious behaviour by or against an identity is caught early. For example, if an attacker gains access to a dormant account and starts accessing sensitive data, ITDR can flag this unusual activity and automate a response (such as revoking tokens or demanding re-authentication). Microsoft's approach to ITDR highlights unifying identity protection with security operations – sharing signals between identity systems and the Security Operations Centre (SOC) so that attacks can be stopped quickly. In business terms, ITDR capabilities reduce the likelihood that an identity breach turns into a full-scale incident. They help limit the "blast radius" of an identity compromise by detecting it fast and responding (often automatically) before an attacker can pivot deeper into systems. As part of a mature identity security program, ITDR gives CISOs and CIOs greater confidence that even if preventive controls falter, there is a safety net to catch and contain identity-based threats.

Building a Comprehensive Identity Security Programme

Understanding the components is a start – but how do you bring them together strategically? Successful identity security is as much about people and process as technology. Here are key steps and best practices for implementing a holistic program:

Assess and Inventory all Identities and Access: You can't protect what you don't know you have. Begin with a thorough discovery of human and non-human identities across your organisation (workforce accounts, service accounts, cloud roles, etc.) and what they have access to. Identify high-risk identities (like domain admins or third-party vendor accounts) and any "orphan" accounts not tied to a current owner. This assessment will reveal gaps, such as users with excessive permissions or applications without MFA, and guide your priorities. Using the right tooling can turn this from a manual labour of spreadsheet wrangling into a repeatable process.

Enforce Strong Authentication Everywhere: Make multi-factor authentication mandatory for all users, especially privileged and remote access. Consider phasing in advanced methods like passwordless authentication (e.g. biometric or FIDO2 security keys) for better security and usability. Use conditional access policies to adapt to risk – for instance, require MFA only for sensitive applications or when risk indicators (unusual login locations, impossible travel) are detected. This ensures security measures remain effective without creating user fatigue.

Adopt Least Privilege Through IAM & IGA Processes: Leverage your IAM and IGA tools to enforce the principle that each identity gets the minimum access required. Establish role-based access controls (RBAC) so that standard roles have preset access, reducing ad-hoc privilege grants. Implement an identity lifecycle process: when people join, change roles, or leave, their access should be promptly updated or removed. Regularly perform access reviews (attestations) for critical systems – using IGA solutions to have managers or system owners certify who should still have access. This governance cycle will prevent privilege creep and ensure compliance over time.

Secure and Monitor Privileged Access: If you haven't already, consider investing in a PAM solution or leverage cloud privileged management features (such as Microsoft Entra Privileged Identity Management for Azure AD roles). Vault all administrative passwords and use check-out processes with approvals for anyone obtaining elevated access. Enable just-in-time elevation so that admin rights expire automatically when not in use. Monitor all administrative sessions (record keystrokes or commands for critical servers, if feasible) and set up alerts for any unusual privileged activities (e.g., a new user being added to a domain admins group unexpectedly). Treat your directory infrastructure (e.g., Active Directory or Entra ID) as a Tier 0 asset – lock it down with the highest security controls, since all other access depends on its integrity.

Integrate Identity Signals Into Threat Detection: Feed identity activity logs (from IAM systems, Active Directory, cloud directories, SSO, etc.) into your Security Operations (SIEM/SOC) workflows. Deploy identity threat detection tools – for example, Microsoft Entra ID Protection and Microsoft Defender for Identity – that specialise in spotting things like credential attacks or anomalous usage. Ensure that when a potential compromise is detected, there are playbooks to respond quickly: automate account disablement or password resets for suspected breached accounts, and leverage conditional access to dynamically block or step-up authenticate risky sessions. Regularly simulate identity breach scenarios to test your detection and response (for instance, run a phishing drill and see if the SOC catches the use of a leaked test credential).

Foster a Security-Aware Culture: Technology alone is not enough. Educate employees about good identity hygiene – such as recognising phishing attempts, using approved password managers, and never sharing credentials. Institute policies and training so that everyone understands that protecting their login is part of their responsibility (for example, reporting lost devices immediately, or not ignoring MFA prompts). Build a partnership between your identity administrators and security team: they should work hand-in-hand, since identity is now a frontline of defence. When IT and security teams collaborate (as encouraged in Microsoft's reference architecture), threats can be addressed faster and policies refined continuously.

By following these practices, organisations create multiple layers of defence around identities while keeping access agile. The goal is an adaptive, resilient identity security posture – one that not only guards against today's credential attacks but also can adjust to new threats and business needs over time. This comprehensive approach turns identity security from a daunting challenge into a business enabler: allowing the right people to connect to the right things confidently and stopping attackers at the gate.

Identity Maturity

Managed
Automated provisioning, SSO across major apps, privileged access controls, routine access reviews

Baseline
Centralised directories, MFA for some users, basic role-based access, occasional audits

Optimised
Conditional access policies, identity-based threat detection, strong governance processes

Adhoc
Disconnected systems, weak password hygiene, manual user provisioning, little or no MFA

Adaptive
Risk-driven access, passwordless, AI-powered detection, aligned with zero trust & business outcomes

Threat Detection & Response

Identity security is no longer just about controlling access to systems. It is becoming a dynamic, intelligence-driven foundation that enables secure collaboration, decentralised access, and automation at scale. As cloud adoption, hybrid work, and AI-driven operations expand, the role of identity is evolving from reactive gatekeeping to proactive defence and business enablement. Forward-looking organisations are already laying the groundwork for this shift.

Here are the trends shaping the future of identity security – and what they mean for your organisation.

Decentralised Identity and Verifiable Credentials

Decentralised Identity (DID) allows users to manage and control their own identity data without relying on a central authority. Identities are built around verifiable credentials, stored off-chain in secure digital wallets, and validated using public key cryptography or distributed ledgers. Microsoft is investing in this space through Entra Verified ID, supporting a shift toward self-sovereign identity.

Why it matters:
This model reduces reliance on identity providers and allows organisations to validate identity attributes (e.g. employment status, certifications, health status) without storing personal data. In sectors like education, government, and healthcare, it enhances privacy, prevents identity fraud, and simplifies compliance with regulations like GDPR. As adoption grows, organisations will need strategies to issue, verify, and consume decentralised credentials securely and at scale.

Identity-as-Code and Policy-Driven Access

Inspired by infrastructure-as-code, identity-as-code treats identity configurations (roles, policies, permissions) as version-controlled code, integrated into CI/CD pipelines. Tools like Microsoft Entra Permissions Management and Terraform-based governance frameworks are bringing this concept into mainstream enterprise environments.

Why it matters:
Defining identity policies as code enables faster, more consistent deployments and better auditability. It allows security and platform teams to collaborate through DevSecOps workflows, reducing misconfigurations and human error. As organisations scale into multi-cloud and hybrid environments, identity-as-code ensures that access controls evolve alongside infrastructure, not after it.

Machine Identity Explosion

Non-human identities – APIs, containers, IoT devices, microservices – now outnumber human users in most enterprises. Each of these identities requires credentials (tokens, secrets, certificates) and access controls. Yet many organisations still treat them as an afterthought, with hardcoded credentials, poor rotation, or no lifecycle management.

Why it matters:
Machine identities are a major target for attackers seeking persistent, covert access. Managing them effectively requires dedicated controls – including automated secret rotation, visibility into unused or overprivileged service accounts, and integration with secrets management tools (e.g. Azure Key Vault, HashiCorp Vault). In future-ready identity programmes, human and machine identities are governed with equal rigour.

AI-Augmented Identity Protection

AI and machine learning are becoming critical tools in defending identities. Microsoft Entra ID Protection and Defender for Identity already use AI to detect anomalies in login behaviour, such as impossible travel, token replay, or MFA fatigue attacks. These capabilities are evolving to provide more context-aware, autonomous decision-making.

Why it matters:
Static rules can't keep up with the speed or creativity of modern attackers. AI-driven protection enables real-time risk scoring, adaptive policies, and automated remediation – all of which reduce response time and limit the impact of compromise. As AI models improve, expect identity platforms to handle more of the detect-decide-act loop autonomously, escalating only the most serious or ambiguous incidents to human analysts.

Insight & Microsoft: Your Partners in Identity Security Excellence

Implementing the full spectrum of identity security can be complex. This is where the right partner can make all the difference. Insight is positioned as a leader in identity security services, backed by an exceptionally strong partnership with Microsoft. Insight's team of experts has deep, hands-on experience with Microsoft's identity and security technologies – from Azure Active Directory (now Microsoft Entra ID) to the latest in identity governance and threat protection tools. In fact, Insight is one of Microsoft's top global partners in security: we hold all four Microsoft Security Advanced Specialisations, including the specialisation for Identity and Access Management, as well as specialisations in Cloud Security, Information Protection, and Threat Protection. Insight is also a member of the Microsoft Intelligent Security Association (MISA), collaborating closely with Microsoft's security product teams.

What do these credentials mean for a client? Simply put, Insight brings proven expertise to design and implement an identity security strategy tailored to your organisation – leveraging the best of Microsoft's technologies. Whether you are strengthening on-premises identity infrastructure or adopting the full Microsoft Entra suite for cloud-based identity, Insight has 1,500+ Microsoft-certified architects and security engineers ready to assist. Our experts have helped enterprises worldwide to deploy multifactor authentication, enable single sign-on across thousands of apps, automate identity lifecycle with tools like Microsoft Entra ID Governance, and integrate identity signals into threat detection platforms. We align these solutions with your business objectives, ensuring security improvements also support productivity and user experience.

Insight's close partnership with Microsoft keeps us at the forefront of new identity security advancements. For example, as Microsoft introduced Identity Threat Detection & Response capabilities and AI-driven security insights, Insight has been early to incorporate these into our managed services. (Insight was among the first to achieve Microsoft's verified Managed XDR status, showing our ability to integrate identity threat detection with 24/7 response operations. We also follow Microsoft's Security Reference Architecture, a best-practice blueprint, to ensure all identity security pieces fit together in your environment. The result is a cohesive solution rather than siloed tools.

Most importantly, Insight approaches identity security as a strategic enabler for your business. We don't just deploy technology – we partner with your stakeholders to develop policies, governance models, and user adoption strategies that make the solutions effective. According to Insight's UK security team, "digital identity is the key to accessing the heart of any organisation and therefore must be protected with the same priority as data or infrastructure... Microsoft offers a comprehensive architecture, but real impact is achieved when combined with culture, processes, and organisational commitment". Insight helps bring that full picture together. We offer services ranging from initial assessments and workshops to hands-on implementation, to managed identity security operations. No matter where you are on your identity security maturity curve, Insight has the expertise to guide you forward.

By choosing Insight as your partner, you gain a team that is not only technically skilled, but also deeply invested in your success. We measure our success by your ability to prevent breaches, meet compliance goals, and confidently adopt new technologies – all under the watch of a robust identity security framework. With Insight and Microsoft by your side, you can turn identity security from a worry into a business strength.

Microsoft

Conclusion

Identity Security is more than a checklist item – it's a strategic imperative in the modern threat landscape. By understanding and integrating the key pillars (IAM, IGA, ITDR), organisations can protect their critical assets and empower their people to work efficiently and safely. The journey may seem complex, but you don't have to navigate it alone. With a trusted partner like Insight – armed with industry-leading Microsoft solutions and unmatched expertise – you can build an identity security programme that protects your business today while staying ready for what comes next.

Glossary

Term	Definition
Access Control	Policies and technologies that determine who can access specific systems, data, or services, and under what conditions.
Authentication	The process of verifying the identity of a user, device, or system using factors such as passwords, biometrics, or security keys.
Authorisation	The process of determining what an authenticated identity is allowed to do or access.
Conditional Access	Dynamic access policies that evaluate risk signals (like device status or location) before allowing access.
Decentralised Identity (DID)	An identity model where individuals control their own identity data and credentials, verified using distributed technologies.
Directory Services	Centralised systems for managing identity information, such as Microsoft Entra ID or Active Directory.
Identity and Access Management (IAM)	Foundational systems and policies for managing digital identities and controlling access to resources.
Identity-as-Code	Treating identity configurations (roles, policies) as code for automation, auditability, and integration into DevOps pipelines.
Identity Governance and Administration (IGA)	Tools and processes to manage the lifecycle of identity access, including reviews, approvals, and policy enforcement.
Identity Lifecycle	The full process of onboarding, changing, and offboarding identities across their time with the organisation.
Identity Threat Detection and Response (ITDR)	Capabilities that monitor for and respond to identity-based threats like misuse, escalation, or anomaly detection.

Term	Definition
Just-in-Time (JIT) Access	Granting privileged access temporarily and only when needed, to minimise standing risk.
Least Privilege	A principle ensuring users and systems have only the access necessary to do their job – nothing more.
Machine Identity	Non-human accounts used by software, APIs, services, or devices, which require identity controls and governance.
Multifactor Authentication (MFA)	An authentication approach requiring two or more forms of verification, improving resistance to account compromise.
Passwordless Authentication	Login methods that eliminate the need for passwords, using biometrics, device trust, or cryptographic keys.
Privileged Access Management (PAM)	Controls and tools that secure administrator and other sensitive accounts through vaulting, monitoring, and JIT access.
Role-Based Access Control (RBAC)	A method of assigning access rights based on a user's job function or role.
Self-Sovereign Identity (SSI)	A model where users own and manage their digital identities independently of central authorities.
Service Account	A digital identity used by systems or software to perform automated tasks, often requiring elevated privileges.
Single Sign-On (SSO)	A system that allows users to log in once and gain access to multiple systems or applications.
Token-Based Authentication	Authentication that relies on secure tokens (e.g. JWTs) rather than re-entering usernames and passwords.
Zero Trust	A modern security philosophy where access is never assumed and always verified, based on context and continuous assessment.

Next Steps

Contact Insight to build your comprehensive identity security programme. With identity now the primary attack vector for enterprises, securing every user, service account, and connection is mission-critical. Our holistic approach protects your digital identities, reduces risk, and enables Zero Trust principles. We help you ensure only the right people get the right access, whilst streamlining productivity. Trust Insight's deep expertise and Microsoft partnership to turn your identity security from a complex challenge into a business enabler.

- **se.insight.com**
- **0852210010**