

István Paráda¹

Cybersecurity Failures in Enterprise MDM Platforms

An Analytical Study of the Ivanti Case

Abstract

Mobile Device Management (MDM) platforms have evolved into critical components of enterprise security architectures, influencing device governance, access control and policy enforcement across corporate networks. As these systems increasingly operate as centralised control planes, they have become attractive targets for adversaries seeking scalable organisational compromise. The study develops a comprehensive analytical framework that integrates public Ivanti security incident data with vulnerability assessment documents and current MDM system design materials. Through qualitative incident analysis and architectural interpretation, the research identifies three primary factors that amplify the systemic impact of MDM compromise: excessive privilege concentration, identity adjacency and update trust dependencies. The findings demonstrate that the security significance of MDM systems extends beyond conventional endpoint management, as these platforms increasingly influence authentication processes, trust relationships and enterprise-wide security decisions. The study argues that MDM platforms should be governed as high-value control-plane assets requiring architectural risk management rather than solely operational security maintenance. The results contribute to the broader understanding of centralised management infrastructures and highlight the need for stronger segmentation, authentication controls, and trust-boundary protection mechanisms within modern enterprise environments.

Keywords: Mobile Device Management, MDM security, Ivanti, enterprise security architecture, identity management

¹ Ludovika University of Public Service, e-mail: paradaistvan@gmail.com

Introduction

The introduction of mobile work solutions and remote work solutions has completely transformed how businesses establish their computer systems. The Mobile Device Management (MDM) system serves as the primary tool organisations use to enforce security regulations, manage device settings and ensure safe access to corporate networks.² MDM systems, which started as tools for inventory control and configuration enforcement, now manage devices and control user access while maintaining security.³ This expanded operational role has simultaneously increased the strategic value of MDM platforms as attack targets. Security breaches that target MDM systems have more harmful consequences because they enable attackers to access all parts of an organisation, whereas breaches targeting endpoint devices affect only specific devices. Control of an MDM system enables attackers to leverage centralised security systems to manipulate authentication processes and install harmful security settings, thereby disable protective controls across the organisation.⁴ The academic security literature fails to recognise MDM platforms as essential security elements because, according to researchers, they are secondary management tools. The recent series of high-impact vulnerabilities disclosed in Ivanti⁵ MDM products challenge this perception. Using the Ivanti incidents as an empirical case study, the paper seeks to extract generalisable insights into the architectural and governance factors that shape MDM security outcomes.

Research questions and methodology

The security risks associated with centralised administrative infrastructure have been studied extensively in the context of directory services and identity management systems. Researchers and practitioners have long recognised that Active Directory⁶ and similar directory services constitute high-value targets whose compromise yields organisation-wide consequences disproportionate to the effort required for initial access.⁷ The concept of "Tier 0" assets – systems whose compromise directly enables control over an entire identity domain – has become a foundational principle in enterprise security architecture and is reflected in Microsoft's widely adopted Enterprise Access Model.⁸

Within the MDM-specific literature, prior work has predominantly addressed device management from operational and compliance perspectives, with limited emphasis

² ENISA 2025.

³ SINGER–FRIEDMAN 2014.

⁴ CIPOLLA et al. 2025.

⁵ Ivanti is an IT software company that provides security, endpoint management and IT service management (ITSM) solutions.

⁶ Active Directory (AD) is a Microsoft-developed directory service that acts as a centralised database for managing users, computers, and security permissions within a Windows domain network.

⁷ ANDERSON 2020.

⁸ Microsoft 2023.

on architectural security implications.⁹ More recent studies emphasise the increasing complexity of identity architectures, particularly in distributed and cloud-based environments, where identity services act as central coordination mechanisms across multiple system layers.¹⁰ In this context, such systems are increasingly understood as components of the enterprise control plane rather than as isolated authentication services. Despite these developments, the existing literature has not systematically conceptualised Mobile Device Management platforms as identity-adjacent control planes. While prior work has addressed MDM technologies and vulnerability management practices, these analyses typically focus on operational implementation rather than on the structural mechanisms through which MDM architectures amplify systemic security risk.

This study builds on these foundations by specifically analysing how MDM architectures amplify security risks through privilege concentration, identity adjacency and update trust dependencies.

In light of the systemic nature of MDM-related risks and to evaluate the broader implications of the Ivanti breaches, this paper addresses three primary questions:

- RQ1: Why do MDM vulnerabilities consistently yield such a disproportionate impact on organisations?
- RQ2: Which specific architectural traits in modern MDM systems are responsible for magnifying these compromises?
- RQ3: What broader governance lessons can be extracted from the Ivanti case?

To address these questions, I use a qualitative methodology centred on structured document analysis. The empirical dataset consists of publicly available vulnerability disclosures, CVE records,¹¹ CISA alerts¹² and forensic incident reports published between 2023 and 2026. Rather than focusing on quantitative exploit frequency, the analysis examines how vulnerabilities interact with architectural trust relationships embedded within MDM platforms. I treat the Ivanti incidents as empirical points – not as isolated bugs, but as evidence of systemic privilege relationships that are inherently embedded in MDM platform designs.¹³ This approach is appropriate, given that the security impact of MDM compromise is driven less by exploit frequency than by systemic privilege relationships embedded in platform design. Vulnerabilities were selected based on the following criteria:

- relevance to MDM control plane components
- confirmed exploitability or documented real-world impact
- availability of technical documentation

⁹ YAMIN-KATT 2019.

¹⁰ KOVACEVIC et al. 2024.

¹¹ CVE Common Vulnerabilities and Exposures Records are standardised, unique identifiers and associated descriptions for publicly known cybersecurity vulnerabilities, designed to facilitate secure, consistent communication and tracking.

¹² CISA alerts are official, timely notifications from the Cybersecurity and Infrastructure Security Agency warning of new, high-impact cyber threats, vulnerabilities, or exploitation campaigns.

¹³ ISO/IEC 2022.

I categorised the vulnerabilities into three primary classes: authentication bypass, remote code execution and privilege escalation. I derived these categories inductively from the dataset and validated against established vulnerability taxonomies.

Fundamentals of Mobile Device Management security

Assessing the security implications of Mobile Device Management (MDM) platforms requires viewing them as centralised control infrastructures positioned between enterprise networks, managed devices and identity systems. An MDM system typically maintains persistent trust relationships with enrolled devices, possesses elevated administrative privileges, and exercises remote control capabilities over device configuration and software state. From a security perspective, this positioning creates a unique convergence of roles. MDM platforms simultaneously operate as policy enforcement points, configuration control systems, and, in many deployments, as intermediaries in authentication and access control workflows.¹⁴ As enterprises increasingly integrate MDM solutions with identity providers, conditional access engines and cloud services, the MDM layer becomes tightly coupled with identity assurance mechanisms. This architectural convergence introduces a critical dependency: device trust is commonly inferred from the device's MDM enrolment status. The MDM platform security breach results in two main consequences that impact both device management capabilities and subsequent security operations. Endpoint malware needs to evade detection on each device, but an MDM compromise enables attackers to use trusted administrative pathways while bypassing most standard endpoint security mechanisms. These characteristics indicate that MDM security cannot be adequately assessed through traditional endpoint threat models. Instead, MDM platforms should be understood as high-privilege control planes whose failure modes resemble those of directory services or identity providers rather than those of managed endpoints.¹⁵

The Ivanti MDM incidents as an empirical case study

The Ivanti Mobile Device Management system provides a representative empirical case for examining the systemic security risks associated with centralised device management infrastructures. Between 2023 and January 2026, multiple high-severity vulnerabilities were disclosed across Ivanti MDM products,¹⁶ which include Endpoint Manager Mobile Sentry¹⁷ and Avalanche.¹⁸ The disclosures encompass multiple types of security vulnerabilities, including authentication bypass, privilege escalation and

¹⁴ HOWELL et al. 2023.

¹⁵ AZODOLMOLKY 2013.

¹⁶ CISA 2024.

¹⁷ Ivanti Endpoint Manager Mobile Sentry (formerly part of MobileIron) is a secure, in-line gateway designed to manage and protect data traffic between mobile devices and corporate systems.

¹⁸ Ivanti Avalanche is a specialised mobile device management (MDM) system designed to manage, secure and update large fleets of rugged mobile computers, scanners and smart devices, frequently in logistics and supply chain environments.

pre-authentication remote code execution (in the following RCE)¹⁹ to demonstrate how MDM systems have developed over time.

Table 1 summarises the publicly disclosed Ivanti MDM vulnerabilities identified during this period, including their CVE identifiers, affected components and assessed severity levels. The dataset demonstrates that all authentication flaws, management interface weaknesses, and update system flaws produce excessive effects because MDM platforms function as central trust systems.

The first table shows that security vulnerabilities that allow remote attacks without authentication have become more common.²⁰ The initial security reports focused on post-authentication vulnerabilities and configuration-dependent weaknesses, whereas current reports indicate that organisations face security threats stemming from pre-authentication attack methods.

Table 1: Chronological overview of high-impact Ivanti MDM vulnerabilities (2023–2026)

Year	CVE ID(s)	Product / component	Type of vulnerability	CVSS ²¹
2023	CVE-2023-39335, CVE-2023-3933722	Ivanti Endpoint Manager Mobile (EPMM)	Enrolment impersonation/access misuse	CVSS 8.5 CVSS 6.8
2023	CVE-2023-3803523	Ivanti sentry	API24 authentication bypass	CVSS 9.8
2024	CVE-2024-2202625	EPMM	Local privilege escalation via crafted package	CVSS 6.7
2024	CVE-2023-46806, CVE-2023-4680726	EPMM	SQL injection ²⁷	CVSS 6.7
2024	CVE-2024-24996, CVE-2024-2920428	Ivanti Avalanche MDM	Heap overflow → possible RCE	CVSS 9.8
2025	CVE-2025-4427, CVE-2025-442829	EPMM	Auth bypass / RCE chain	CVSS 7.5 CVSS 8.8
2025	CVE-2025-2246230	Ivanti neurons for ITSM	Authentication bypass	CVSS 9.8
2026	CVE-2026-1281, CVE-2026-134031	EPMM	Pre-auth remote code execution (zero day)	CVSS 9.8

Source: compiled by the author based on NVD, CISA KEV Catalog and CVE Details (2023–2026)

¹⁹ Remote Code Execution (RCE) is a critical cybersecurity vulnerability that allows attackers to remotely run malicious code, commands, or software on a target computer or network, often resulting in a full system takeover.
²⁰ CVE Details 2026.
²¹ CVSS stands for Common Vulnerability Scoring System. It is an open industry standard used to assess and rate the severity of software and hardware security vulnerabilities, assigning them a numerical score from 0.0 to 10.0 based on factors like attack complexity, impact and exploitability.
²² Ivanti CVE-2023-39335, CVE-2023-39337 2026.
²³ NARANG 2023.
²⁴ An API (Application Programming Interface) is a set of rules and protocols that allow different software applications to communicate, share data and securely exchange functionality.
²⁵ NIST 2024.
²⁶ Computer Incident Response Center Luxembourg 2023.
²⁷ SQL injection (SQLi) is a security vulnerability in which attackers inject malicious SQL code into input fields to manipulate backend databases.
²⁸ ANDERSON 2025.
²⁹ SMITH 2025.
³⁰ Center for Cybersecurity Belgium 2025.
³¹ MOORE 2025.

The MDM platform has become more complex to operate, while its value as a target for attackers has increased due to its ability to deliver extensive attack paths.³² Importantly, the Ivanti incidents should not be interpreted solely as vendor-specific implementation failures. Instead, they reflect broader structural characteristics inherent in centralised enterprise mobility and endpoint management architectures. Similar security weaknesses exist across different enterprise mobile management systems, including both MDM and unified endpoint management platforms.³³ Ivanti, therefore, serves as a representative empirical example through which broader architectural characteristics of modern MDM platforms can be examined.

The empirical observations presented in this section establishes the foundation for the analytical findings discussed in the subsequent sections. By situating individual vulnerabilities within a temporal and architectural context, the analysis moves beyond incident reporting toward a systematic understanding of why MDM compromises produce organisation-wide security consequences.

Systematic analysis of the 2026 EPMM pre-authentication RCE incident (CVE-2026-1281) case

The practical validity of the proposed MDM threat model can be demonstrated through analysing the 2026 Ivanti Endpoint Manager Mobile (EPMM) zero day vulnerability chain (CVE-2026-1281). The analysed vulnerabilities were disclosed contemporaneously with the preparation of this manuscript. Accordingly, the study is based on publicly available information and should be interpreted as a contemporaneous analytical case study rather than a fully retrospective forensic analysis – the technical failure cascaded system-wide, affecting all services because it originated in the core MDM management plane. Public threat intelligence reports indicate that CVE-2026-1281 was actively exploited in combination with a second vulnerability (CVE-2026-1340), which enabled unauthenticated adversaries to execute arbitrary code on EPMM servers without the need of valid credentials or user interaction. The compromise provided attackers with administrative control over the centralised MDM infrastructure, thereby exposing enterprise-wide mobile device management functions to systemic manipulation. According to incident investigations published by the Palo Alto Networks Unit 42,³⁴ exploitation activities included the establishment of reverse shells, deployment of web shells, reconnaissance operations, and the downloading of additional malware payloads.

The attack sequence originated at the internet-facing management interface, which served as the most vulnerable trust boundary in the system architecture. By exploiting a pre-authentication remote code execution vulnerability, adversaries bypassed perimeter authentication mechanisms and obtained control over the management server. This effectively transformed the MDM platform from a defensive

³² SYYNIMAA 2022.

³³ CELIK 2025.

³⁴ Palo Alto Networks Unit 42 is a renowned global team of threat researchers, incident responders, and security consultants that provides proactive cyber risk management and emergency incident response.

management component into an entry point for the broader enterprise network. Following the initial breach, the attackers advanced to the second stage of the attack model by gaining administrative control of the MDM management server. At this stage, the adversary transitioned from an external attacker to an internally trusted administrative actor, inheriting the extensive privileges of a centralised MDM control plane. In the third phase of the attack chain, the adversaries used authorised MDM push-management functions to spread harmful configuration profiles across all devices in the enrolled device fleet. The enrolled devices executed the commands automatically because they had already established a trust connection with the management server. The compromised endpoints subsequently functioned as trusted proxies within the enterprise environment. The attackers used their ability to control device status, their access to valid session tokens, and their knowledge of enterprise network protocols to navigate the organisation's internal identity systems, including the VPN,³⁵ gateways, directory services and authentication systems.³⁶

The threat intelligence telemetry indicates that the exploitation campaign affected organisations across various sectors, including state and local government, healthcare, manufacturing, professional services and high-technology industries in the United States, Germany, Australia and Canada. The U.S. CISA³⁷ included CVE-2026-1281 in its KEV.³⁸ The catalogue was updated because attackers were currently exploiting the vulnerability, which had become a major security risk. The scale of potential exposure was also significant. Security telemetry identified more than 4,400 internet-accessible EPMM instances worldwide, demonstrating the platform's extensive deployment footprint and the large attack surface available to threat actors.

This case demonstrates that the organisational impact of MDM compromise is disproportionately high, not merely because of the underlying software vulnerability, but also because of the concentrated privilege structure and implicit trust relationships embedded in MDM platform architectures.³⁹ While the Ivanti case provides the empirical foundation for this analysis, the structural implications identified here apply broadly to modern enterprise MDM deployments and centralised endpoint management systems.

Vulnerability pattern analysis and threat modelling of MDM platforms

For analytical clarity, I introduce three core concepts that serve as the foundation for interpreting the security implications of Mobile Device Management (MDM) platforms. These concepts – privilege concentration, identity adjacency and update trust dependency – are not presented as entirely novel theoretical constructs, but

³⁵ A Virtual Private Network (VPN) is a service that creates a secure, encrypted "tunnel" between your device (computer, phone) and the internet.

³⁶ HOGAN-BURNEY – TSYGANSKIY 2025.

³⁷ Cybersecurity and Infrastructure Security Agency.

³⁸ Known Exploited Vulnerabilities.

³⁹ ROSE et al. 2020.

rather as an integrated framework tailored to the specific architectural characteristics of MDM systems.⁴⁰

Privilege concentration refers to the extent to which administrative authority and security-relevant control functions are centralised within a single system component. In the context of MDM platforms, this manifests as the aggregation of device management, policy enforcement, and configuration control within a unified management plane. Such concentration creates a structural condition in which the compromise of a single system element yields disproportionately high impact across the managed environment.

Identity adjacency describes the extent to which a system influences authentication processes or access control decisions without being formally classified as an identity provider. MDM systems increasingly operate in this intermediate space, as device compliance status, enrolment state, and configuration integrity are frequently used as implicit inputs into access control mechanisms. As a result, these systems acquire indirect authority over identity-related decisions, thereby expanding their security relevance beyond traditional device management roles.⁴¹

Update trust dependency captures the reliance of managed endpoints on a centralised authority for the delivery and execution of configuration changes, software updates and policy enforcement actions. This dependency is typically implemented through implicit trust relationships, where endpoints accept and execute instructions from the management server without independent validation. While this model enables efficient large-scale administration, it also creates a high-risk propagation channel in the event of control-plane compromise.⁴²

Using a consistent framework for interpretation helped me to make sense of the entire dataset. This structured approach enabled me to move from simply documenting incidents to generating more meaningful insights and analysis. During my analysis, I adopted an active stance, analysing vulnerabilities along with their impact on the MDM architecture. I found specific vulnerabilities, which included possible administrative takeover and granting unlimited control of the MDM system, as evidence of privilege centralisation. Moreover, I analysed vulnerabilities associated with authentication, device compliance validation, and access control using the notion of identity adjacency. Also, I classified vulnerabilities allowing unauthorised access to system configurations and updates as a sign of user trust in the system's update mechanisms. Adopting an interpretive model was critical in allowing me to analyse the whole dataset. The interpretive approach provided me with the opportunity to transition from mere documentation to deeper analysis.

While Table 1 presents a chronological overview of disclosed Ivanti vulnerabilities, the dataset also reveals several recurring structural patterns that are highly relevant for understanding systemic risk in Mobile Device Management architectures. Rather than representing isolated implementation defects, the vulnerabilities cluster around a limited number of architectural trust boundaries within MDM systems.⁴³

⁴⁰ TUHIN 2025.

⁴¹ ALPÁR et al. 2011.

⁴² CAPPOS et al. 2008.

⁴³ SALTZER-SCHROEDER 1975.

A qualitative classification of the vulnerabilities summarised in Table 1 identifies three dominant categories, as illustrated in Figure 1.

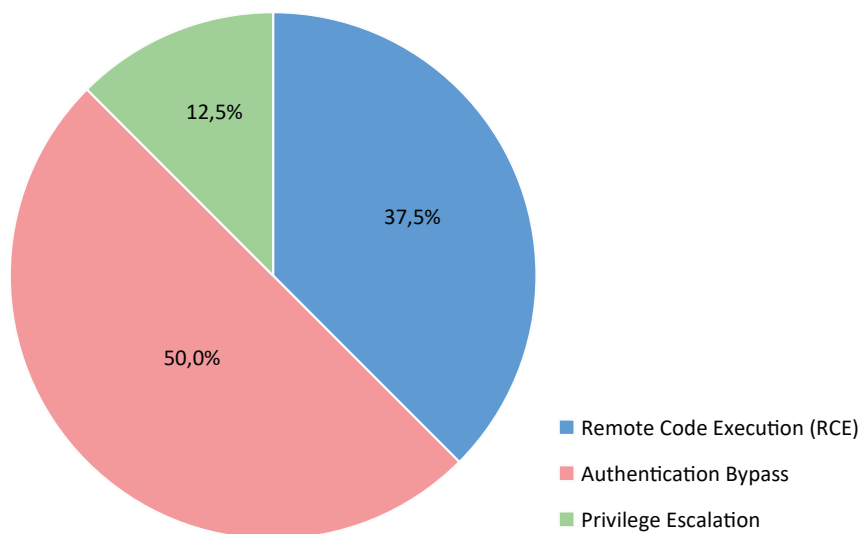


Figure 1: Distribution of incidents by vulnerability types in Ivanti MDM incidents (2023–2026)

Source: compiled by the author based on vulnerability data collected from MDM–Ivanti (2023–2026)

Authentication bypass vulnerabilities are among the most critical categories, as they allow attackers to circumvent the primary security boundary protecting administrative management functions. When such flaws occur in externally accessible interfaces, attackers may obtain control over the MDM platform without prior credentials. The process of exploiting privilege escalation vulnerabilities begins when attackers use their restricted access to elevate their privileges to full administrative rights. The RCE vulnerabilities in MDM systems pose major security risks because management servers handle privileged access while maintaining secure connections to all connected devices. Attackers who exploit these vulnerabilities gain complete access to the management server, including the ability to control device settings and network security protocols.⁴⁴

The distribution of vulnerabilities across MDM components highlights the concentration of risk within a small number of architectural interfaces.⁴⁵ The most frequently affected elements include:

- API management
- enrolment and device registration services
- administrative web interfaces
- update and package deployment mechanisms

⁴⁴ ELYASSA 2024.

⁴⁵ ANDERSON 2020.

These components represent the primary trust boundaries between external entities and the MDM control plane. Because many of these interfaces must remain accessible to devices across enterprise networks or the public internet, they inherently expand the platform's attack surface. An important trend in the dataset is the growing prevalence of pre-authentication vulnerabilities that enable attackers to exploit management interfaces without valid credentials. This shift significantly lowers the barrier to compromise and transforms the MDM platform into a viable initial access target rather than merely a post-compromise privilege escalation opportunity.

The architectural role of MDM platforms creates greater security risks because their system design enables common software vulnerabilities to have more severe effects than they do in standard enterprise environments.⁴⁶ While standard vulnerabilities usually affect a limited number of services or specific hosts, flaws in MDM control planes can have a cascading effect across the entire organisational infrastructure. The amplification effect affects all managed devices that experience operational failure due to a specific security vulnerability.⁴⁷ The system vulnerabilities turn off all authentication mechanisms that determine user access to protected resources in accordance with established security protocols. The adversary obtains access to software distribution pathways and compliance monitoring systems because the organisation's security system for system protection is compromised. Consequently, even moderately complex vulnerabilities can produce disproportionate organisational consequences when they occur within centralised device management systems.⁴⁸

Conclusion

The Ivanti incident research shows that organisations now protect their systems through centralised device control together with zero-trust security systems. Organisations now use MDM platforms as security systems to protect their devices, as they authenticate user identities through these platforms. The security standards that protect organisations through device management, along with identity management, now fail because attackers who breach MDM systems can gain complete control over device security and user authentication.⁴⁹ Through this analytical synthesis, I provide direct answers to the core research questions of this study:

- RQ1: Why do MDM vulnerabilities consistently yield such a disproportionate impact on organisations? The "Force Multiplier" effect in MDM systems results in all systems experiencing their most severe impact. Because the MDM server maintains an automated, pre-established trust relationship with the entire device fleet, a single compromise at the control plane level allows the

⁴⁶ BÁLINT-PETŐ 2025.

⁴⁷ ENISA Cyber Threats 2026.

⁴⁸ HAYES et al. 2020.

⁴⁹ WINDLEY 2005.

instantaneous propagation of malicious configurations without requiring the exploitation of individual devices.

- RQ2: Which specific architectural traits in modern MDM systems are responsible for magnifying these compromises? The magnification is primarily driven by privilege concentration and identity adjacency. Modern MDM systems are no longer peripheral tools; they are deeply integrated into the identity assurance chain. Using device enrolment status as a trust indicator creates a security vulnerability for the MDM platform, as it becomes the only security assessment method.
- RQ3: What broader governance lessons can be extracted from the Ivanti case? The Ivanti case demonstrates that MDM security must shift from a “patch management” focus to an architectural trust model. Governance must treat MDM platforms as Tier 0 assets⁵⁰ – equivalent to Active Directory or Identity Providers – consistent with findings in centralised command and control architectures where trusted information flows determine decision-making integrity⁵¹ requiring strict network segmentation, multi-factor authentication for all administrative interfaces, and the assumption that the management plane itself is a high-value target for pre-authentication attacks.
- The primary scientific contribution of this study lies in the analytical reframing of MDM platforms as identity-adjacent control planes. This research demonstrates that modern MDM systems operate across device, identity and policy layers concurrently, creating a concentration of privilege that traditional endpoint threat models fail to predict. By bridging the conceptual gap between identity-centric security and endpoint management, this study argues for applying high-assurance frameworks to all centralised management architectures.

The security of MDM systems will become increasingly important for organisations as they extend their mobile and remote work capabilities, according to the conclusion of this study. The Ivanti case study demonstrates that structural properties, including the exploitation of secure management pathways, determine the depth of security breaches in systems, not just software flaws. Future security approaches must adapt to view MDM platforms as essential, high-risk elements of the identity framework, and researchers need to explore multi-vendor resilience to develop systemic insights across different deployment models, particularly in the context of increasingly integrated, multi-domain system architectures.⁵²

⁵⁰ Tier 0 assets are the most critical IT systems, identities and components in an organisation – often called the “crown jewels” – that provide direct administrative control over Active Directory (AD) or cloud identity environments.

⁵¹ TÓTH 2025.

⁵² TÓTH-FARKAS 2023.

References

- ALPÁR, Gergely – HOEPMAN, Jaap-Henk – SILJEE, Johanneke (2011): The Identity Crisis: Security, Privacy and Usability Issues in Identity Management. *arXiv*. Online: <https://arxiv.org/abs/1101.0427>
- ANDERSON, Ross (2020): *Security Engineering. A Guide to Building Dependable Distributed Systems*. Cambridge: Cambridge University Press. Online: <https://doi.org/10.1002/9781119644682>
- ANDERSON, Elliot (2025): CVE-2024-24996, CVE-2024-29204 Ivanti Avalanche Buffer Overflow Vulnerabilities. Online: www.lumifycyber.com/threat-library/cve-2024-24996-cve-2024-29204-ivanti-avalanche-buffer-overflow-vulnerabilities/
- AZODOLMOLKY, Siamak (2013): *Software Defined Networking with OpenFlow*. Online: https://speetis.fei.tuke.sk/KomunikacnaTechnika1/prednasky/7_11_2016/kniha_sietovanie.pdf
- BÁLINT, Ferenc – PETŐ, Richárd (2025): Sustainable and Safe Cities Through Computer Applications 2025. *Interdisciplinary Description of Complex Systems*, 23(3), 207–216. Online: <https://hrcak.srce.hr/file/481559>
- CAPPOS, Justin – SAMUEL, Justin – BAKER, Scott M. – HARTMAN, John H. (2008): *A Look in the Mirror: Attacks on Package Managers*. CCS '08: Proceedings of the 15th ACM Conference on Computer and Communications Security. New York: Association for Computing Machinery, 565–574. Online: <https://doi.org/10.1145/1455770.1455841>
- CELIK, Osman (2025): *Attack Surface Management Report*. Online: www.wisdominterface.com/wp-content/uploads/2025/07/Report2025KuppingerColeLeadershipCompassAttackSurfaceManagement-1.pdf
- Center for Cybersecurity Belgium (2025): *Warning: CVE-2025-22462, Authentication Bypass Vulnerability in Ivanti Neurons for ITSM Leading to Remote Unauthenticated Administrative Access, Patch Immediately!* Online: <https://ccb.belgium.be/advisories/warning-cve-2025-22462-authentication-bypass-vulnerability-ivanti-neurons-itsm-leading>
- CIPOLLA, Tom – AL DANA, Lina – KUMAR, Sunil (2025): *Market Guide for Endpoint Management Tools*. Gartner Research. Online: www.gartner.com/en/documents/4018596
- CISA (2024): *Known Exploited Vulnerabilities Catalog. Ivanti*. Online: www.cisa.gov/known-exploited-vulnerabilities-catalog
- Computer Incident Response Center Luxembourg (2023): CVE-2023-46806 (GCVE-0-2023-46806). Online: <https://cvepremium.circl.lu/vuln/CVE-2023-46806>
- CVE Details (2026): *Ivanti: Vulnerability Statistics*. Online: www.cvedetails.com/vendor/17398/ivanti.html
- ELYASSA, Mehdi (2024): *Red Teaming Like an APT, a MobileIron 0-day Exploit Chain*. Online: www.sstic.org/media/SSTIC2024/SSTIC-actes/simulation_dun_apt_en_red_team__recherche_et_dcouv/SSTIC2024-Article-simulation_dun_apt_en_red_team__recherche_et_dcouverte_de_0-day_sur_mobileiron-elyassa.pdf

- ENISA (2025): *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity. Online: www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
- ENISA Cyber Threats (2026): *Single Points of Failure in Critical ICT Systems*. Online: www.enisa.europa.eu/topics/cyber-threats
- HAYES, Darren – CAPPA, Francesco – LE-KHAC, Nhien An (2020): An Effective Approach to Mobile Device Management. *Digital Business*, 1(1). Online: <https://doi.org/10.1016/j.digbus.2020.100001>
- HOGAN-BURNEY, Amy – TSYGANSKIY, Igor (2025): *Microsoft Digital Defense Report 2025*. Online: www.microsoft.com/security/blog
- HOWELL, Gema et al. (2023): *NIST SP 800-124 Rev.2. Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Online: <https://doi.org/10.6028/NIST.SP.800-124r2>
- ISO/IEC (2022): *ISO/IEC 27001:2022. Risk-based Security Methodology*. Online: www.iso.org/standard/27001
- KOVACEVIC, Ivana – RANKOVIC, TAMARA – STOJKOV, MILAN – SIMIC, Milos (2024): Token-Based Identity Management in Distributed Cloud Systems. *arXiv*. Online: <https://arxiv.org/abs/2410.21865>
- Microsoft (2023): *Enterprise Access Model. Microsoft Security Documentation 2023*. Online: <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model>
- MOORE, Justin (2025): *Critical Vulnerabilities in Ivanti EPMM Exploited*. Online: <https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/>
- NARANG, Satnam (2023): *CVE-2023-38035: Ivanti Sentry API Authentication Bypass Zero-Day Exploited in the Wild*. Online: <https://fr.tenable.com/blog/cve-2023-38035-ivanti-sentry-api-authentication-bypass-zero-day-exploited-in-the-wild>
- NIST (2024): *CVE-2024-22026 Detail*. National Vulnerability Database. Online: <https://nvd.nist.gov/vuln/detail/CVE-2024-22026>
- ROSE, Scott – BORCHERT, Oliver – MITCHELL, Stu – CONNELLY, Sean (2020): *Zero Trust Architecture. NIST SP 800-207*. Online: <https://doi.org/10.6028/NIST.SP.800-207>
- SALTZER, Jerome H. – SCHROEDER, Michael D. (1975): The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9), 1278–1308. Online: <https://doi.org/10.1109/PROC.1975.9939>
- SINGER, Peter W. – FRIEDMAN, Allan (2014): *Cybersecurity and Cyberwar. What Everyone Needs to Know*. Oxford: Oxford University Press. Online: <https://doi.org/10.1093/wentk/9780199918096.001.0001>
- SMITH, Ben (2025): *CVE-2025-4427, CVE-2025-4428: Ivanti Endpoint Manager Mobile (EPMM) Remote Code Execution*. Online: www.tenable.com/blog/cve-2025-4427-cve-2025-4428-ivanti-endpoint-manager-mobile-epmm-remote-code-execution
- SYNNIMAA, Nestori (2022): *Exploring Azure Active Directory Attack Surface: Enumerating Authentication Methods with Open-Source Intelligence Tools*. Proceedings of the 24th International Conference on Enterprise Information Systems, Volume 2, ICEIS, 142–147. Online: <https://doi.org/10.5220/0011077100003179>

- TÓTH, András (2025): Enhancing Situational Awareness and Decision-Making: The Impact of Advanced ISR Solutions on Command and Control Systems. *Hadmérnök*, 20(2), 143–160. Online: <https://doi.org/10.32567/hm.2025.2.9>
- TÓTH, András – FARKAS, Tibor (2023): Opportunities and Directions for the Evolution of Command and Control Systems in the Context of Multi-domain Operations. *Vojenské Reflexie*, 18(3), 59–73. Online: <https://doi.org/10.52651/vr.a.2023.3.59-73>
- WINDLEY, Phillip (2005): *Digital Identity*. Sebastopol, CA: O'Reilly. Online: <https://dl.acm.org/doi/abs/10.5555/1098715>
- YAMIN, Muhammad – KATT, Basel (2019): *Mobile Device Management (MDM): Technologies, Issues, and Challenges*. ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. New York: Association for Computing Machinery, 143–147. Online: <https://doi.org/10.1145/3309074.3309103>