

Idira Identity Security Blueprint Rapid Risk Reduction Playbook

Rapid Risk Mitigation for Mission-Critical Identities

In today's AI-powered, multcloud, and SaaS world, identity is the new perimeter. Physical and network barriers have dissolved, and all identities can be an attack path to an organization's most valuable assets. Organizations must strengthen identity security to reduce risks. However, implementing an effective identity security program—including identifying weaknesses, evaluating potential exposure, and introducing new security controls—can be a daunting proposition for many organizations.

Idira™ Identity Security Blueprint (Idira Blueprint), by Palo Alto Networks, is specifically designed to help organizations improve their security posture and mitigate risk in a methodical and efficient manner using field-proven measures. Idira Blueprint Rapid Risk Reduction Playbook helps organizations quickly implement the most critical elements of their blueprint to rapidly strengthen security and reduce risk. This paper highlights how Idira Identity Security Blueprint helps reduce identity security risk. It also explains how Rapid Risk Reduction Playbook can help jump-start your identity security implementation and accelerate risk reduction.

Idira Blueprint Rapid Risk Reduction Playbook helps organizations quickly implement the most critical elements of the blueprint to rapidly strengthen security and reduce risk.

Reducing Identity Security Risks with Idira Identity Security Blueprint

Identity security is front and center for today's information technology and security leaders. It's also at the core of a strong zero trust strategy. External attackers and malicious insiders can gain unauthorized access to identities and traverse networks to steal confidential information, disrupt critical systems and applications, and impair business operations. Nearly 90% of Unit 42® investigations over the past year showed that identity weaknesses played a material role.¹

We have developed a prescriptive blueprint to help businesses establish and maintain an effective program to strengthen identity security. Idira Blueprint is designed to defend against three common moves every perpetrator makes to steal data and disrupt systems. This thinking-like-an-attacker approach yields a prioritized, phased implementation plan that closely aligns actions with potential risk reduction.

The Identity Attack Chain

1. **Malicious actors:** Bad actors can exist either internally or externally to the organization. External actors use various techniques to gain entry, while internal actors tend to use existing knowledge and access. In both cases, their ability to execute has become supercharged by AI tools.
2. **Identity compromise:** Actors use techniques, such as social engineering, keystroke logging, and credential repository scraping, to harvest passwords, hashes, SSH keys, or hard-coded credentials. They prey on low authenticator assurance levels (AALs) to bypass authentication controls, such as SMS or the lack of a device posture-based multifactor authentication (MFA).
3. **Lateral and vertical movement:** Actors will leverage their initial access to navigate across an organization's resources, whether laterally from within a risk tier (e.g., workstation-to-workstation) or crossing vertically into another risk tier or environment (e.g., workstation-to-cloud, DevOps tool, or a SaaS app).
4. **Privilege escalation and abuse:** Once a bad actor has discovered the access they desire, they elevate their privileges to then carry out malicious actions against the organization, abusing those privileges.
5. **Actions on objectives:** Those malicious actions are typically predefined objectives such as data theft, ransomware distribution, service disruption, supply chain spread, and brand damage.

1. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

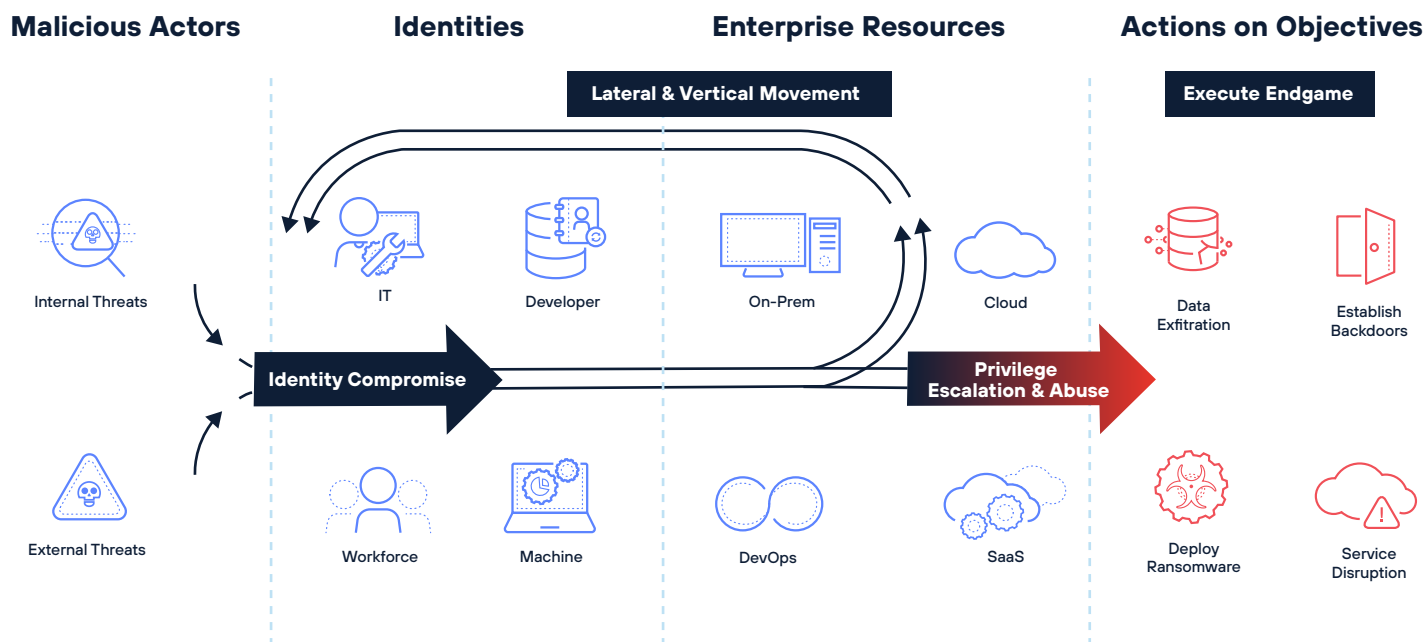


Figure 1. Identity attack chain

Idira Blueprint provides security control recommendations, which are framed around [mitigating these core attack patterns](#). They are based on three guiding principles:

- Prevent identity compromise.
- Stop lateral and vertical movement.
- Limit privilege escalation and abuse.

Idira Blueprint uses these guiding principles to align Idira Identity Security Platform controls with the mitigation of attack chain risks.

Targeting the Greatest Risk with Rapid Risk Reduction Playbook

Idira Blueprint Rapid Risk Reduction Playbook focuses on the highest-priority elements of your organization's Idira Blueprint identity security success plan, helping you address the most urgent requirements in the shortest possible time. Later, you can implement more elements of Idira Blueprint for less-urgent use cases.

The playbook adheres to incident response best practices recommended by leading authorities including:

- US National Institute of Standards and Technology in [Incident Response Recommendations and Considerations for Cybersecurity Risk Management](#).
- European Union Agency for Network and Information Security in [ENISA NIS2 Technical Implementation Guidance](#).
- Australian Cyber Security Centre in [Guidelines for cyber security incidents](#).

Incident Response Lifecycle

The playbook addresses the phases of the NIST incident response lifecycle. It helps you improve preparedness by proactively securing access to the most frequently targeted identities and privileged users. It also helps you identify compromised identities, isolate attackers, and establish corrective measures by analyzing privileged activity. For example, if a compromised account was vaulted, you can determine who had access and which systems they accessed so you can mitigate the attack. If it wasn't vaulted, you can examine similar accounts to detect and isolate breaches.

You can also use the playbook to address the containment, eradication, and recovery phases of the incident response lifecycle. Once you identify compromised accounts and privileges, you can vault them with one-time passwords and exclusive account options, preventing the credentials from being used to further the attacker's objectives. You can also remove components the attackers used, such as disabling breached accounts or introducing proxy-based access.

Idira Identity Security Blueprint defines a risk-prioritized framework for an identity security program that aligns program milestones with risk reduction potential. The playbook focuses on the critical and high-risk use cases in the blueprint. It homes in on the most frequently targeted identities, which represent the greatest potential for network, domain, infrastructure, cloud, and identity takeovers, as shown in the following table. The playbook adheres to the blueprint's guiding principles, helping prevent identity compromise, stopping lateral and vertical movement, and limiting privilege escalation.

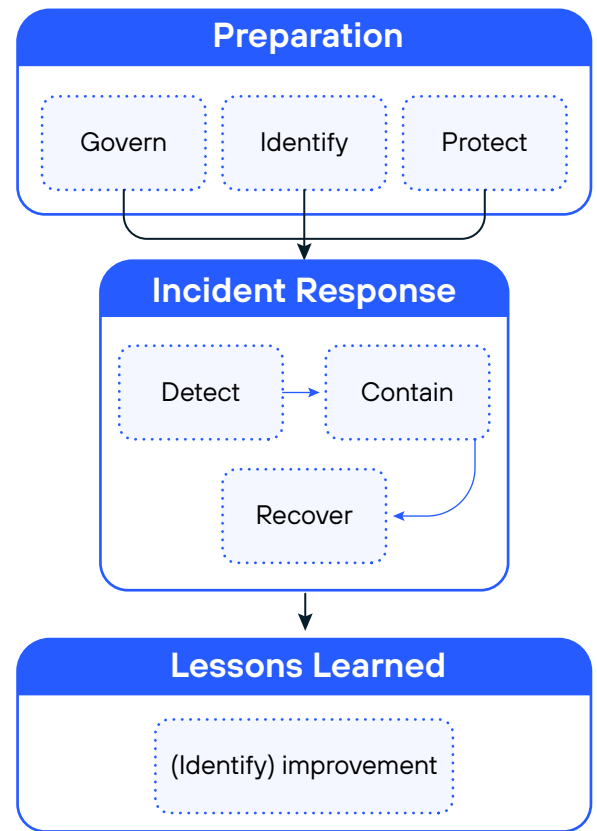


Figure 2. 2025 NIST incident response lifecycle model²

Table 1. Critical Identity Targets and Mitigation Controls for Rapid Risk Reduction

Severity	Control Family	Use Case	Recommended Controls
Critical	Security-first access management	Identity security platform	SSO, adaptive MFA, session protection, and TDR
		IT security tools	
		IT automation tools	
	Zero standing privileges	Cloud service provider admins	SSO, adaptive MFA, ZSP, session protection, and TDR
	Secure standing privileges	Cloud service provider admins	Vaulting, rotating, session management, and TDR
Domain admins			
Hypervisor admins			
High	Zero standing privileges	Windows Server admins (domain)	ZSP, session management, and TDR
	Secure standing privileges	Windows Server admins (local)	Vaulting, rotating, session management, and TDR
		Workstation admins (local & domain)	
	Endpoint privilege management	IT admin workstations	Least privilege enforcement, admin right elevation

2. Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST, April 2025.

Table 1 includes the severity related to the use case, prioritized recommendations, recommendation control family, specific targeted use case, and recommended Idira Identity Security Platform controls to secure the scenario. If you do not have access to one or more of these services, use comparable existing services you have to mitigate the risk related to the use case.

The playbook aims to implement the most critical security controls as quickly as possible. Security best practice and risk mitigation theory dictate that organizations should implement these controls regardless of whether they have suffered a recent breach. Many organizations execute the playbook in 60 days or less. In practice, the playbook duration depends on an organization's size, complexity, maturity, culture, and sense of urgency.

In the aftermath of a breach—or in other instances when business leaders have an urgent desire to strengthen security—organizations often set aside corporate politics and overturn bureaucracy. This dynamic often helps companies accelerate security initiatives and pull some of the later-phase Idira Blueprint recommendations into the playbook objectives.

Playbook Stage One: Secure High-Value Targets

In the first stage of the playbook, focus on securing high-value targets that represent the greatest potential risk to the organization. Identify and secure any identity and related privilege access that can be exploited to control an entire environment. These might include the administrators of your identity security platforms, cybersecurity tools, IT automation services, the domain, and cloud service providers (CSPs) and the access privileges they hold. These assets are typically considered Tier 0 due to their wide scope of influence access and broad blast radius, making their compromise lead to a devastating impact.

Prevent unauthorized access and reduce risk for human users by leveraging adaptive MFA, single sign-on (SSO), session protection, and threat detection and response to any administrators of your identity security platforms, cybersecurity tools, and IT automation tools. Apply adaptive MFA, isolating and protecting privileged sessions, rotating passwords, and intelligently monitoring and analyzing privileged session activity for domain admins, cloud admins, hypervisor admins, and Windows Server admins (local). Extend adaptive MFA, SSO, zero standing privileges (ZSP), session protection, and threat detection and response controls to any user with admin rights to CSPs. Apply continuous discovery for these use cases to prevent drift in the total accounts and identities secured.

Playbook Stage Two: Lock Down Most Common Technology Platforms' Persistent Access

In the second stage of the playbook, lock down the most commonly deployed technology platforms. Secure privileged on-premises, cloud-hosted, and cloud-federated Active Directory (AD) accounts used to administer Windows Servers, ideally with ZSP controls. Protect all local admin accounts (SID-500, other created accounts) on Windows Servers by vaulting and rotating passwords and isolating privileged sessions. Also, secure all Windows and macOS workstation local admin and domain-joined administrative accounts with credential vaulting and password rotation.

Playbook Stage Three: Incorporate Least Privilege into the Endpoint Directly

In the third stage, reduce your privilege escalation risks by implementing OS-level least-privileged access controls for workstations and virtual desktop instances (VDIs) that your IT administrators and cybersecurity engineers use. Endpoint privilege management solutions help you limit exposure by removing local administrative rights from endpoints and tightly controlling user and application permissions based on policy. By enforcing the principle of least privilege—granting users the minimum set of privileges required to perform their jobs—you help prevent vertical movement and improve your security posture. Also, by instituting application controls—preventing ransomware and other malware, as well as restricting the operation of unsanctioned applications—you help reduce risk and uncertainty.

Focus on your IT and security staff before the rest of your workforce to ensure you cover your most critical and risky personas first. This approach generally reduces risk faster, because the number of identities and machines is far greater than the overall workforce population.

Ensuring a Successful Outcome

Implementing a comprehensive, enterprise-wide identity security program is a process, not an event. The playbook is a critical first step in your overall identity security journey. To ensure a successful outcome, properly prepare for the Rapid Risk Reduction initiative, and continuously extend the breadth and depth of your defenses after executing the playbook.

Also, keep in mind that the Idira Identity Security Blueprint is structured to defend against the most common threats posing the highest risk to the business. Every organization's situation is unique.

If you are executing the playbook in response to a cyberattack, you might need to adjust priorities and resequence tasks to address your specific circumstances. For example, you detect that the privileged credentials on a universal technology platform (e.g., a local admin account on a workstation) have been compromised. Then, you might need to isolate, vault, and rotate those credentials while applying the principle of least privilege across all local admin workstations. Over time, you'll need to fully implement all five stages of Idira Identity Security Blueprint for ultimate security.

Before Executing the Playbook

Before carrying out the playbook, identify your stakeholders, project team members, and the hardware and software resources you'll need for the program. Create a project plan that defines the specific Idira Identity Security Platform controls and technologies you plan to implement. Define success criteria and the tools and methods you will use to evaluate progress and measure success.

Understand the current state of your privileged access and identities, which is an important step in remediating the vulnerabilities outlined previously. To assist with this process, you can leverage Idira Identity Security Platform to discover privileged accounts and access across your CSPs, AD domains, Windows, and macOS infrastructure, among other SaaS apps and technology platforms outside the scope of the playbook.

While you might need to perform this playbook in a reactive fashion, we encourage you to perform it proactively. For assistance, [contact our Security Services team](#) for assistance.

At the Conclusion of the Playbook

After you run the playbook, conduct a postmortem. Identify what went well and which processes need improvement going forward. Use lessons learned from the effort to establish ongoing identity security systems and practices. Develop a formal plan to carry out regular identity security enhancements to improve the depth and breadth of your defenses.

Prepare a concluding report for executives and business leaders, explaining how the playbook will help the company improve cybersecurity and reduce risk. Describe additional steps and investments required to further bolster security. Present risk in meaningful, relatable terms like business downtime, lost revenue, or regulatory penalties.

After the Playbook

We encourage you to arrange an Idira Blueprint session to get additional support in designing and structuring a roadmap to extend Idira Identity Security Platform controls across the organization. Now that the most critical and time-sensitive aspects of the Idira Blueprint framework have been addressed, you can expand the scope of your identity security plan to align to your broader business outcomes and objectives.

Consider implementing the outstanding controls and technologies from the Idira Blueprint control families, and continue to strengthen their security posture over time by instituting later phase recommendations. Refer back to this prioritization when developing your own roadmap or plan, combining them with your own business objectives, current security posture, and internal priorities. This way, you can make more informed decisions and determine where you can focus your identity security efforts moving forward.

Continuously assess the effectiveness of your cybersecurity plan and adjust it as needed. Develop a reporting framework and process that showcases your progress and impact to the organization. Execute penetration tests or carry out red team or blue team exercises to test defenses. Use network scanning tools to identify weaknesses and improve your security posture. Revise the plan and reprioritize security measures when appropriate.

Why Palo Alto Networks

Idira Identity Security Blueprint is built on our collective experience, with the Unit 42 team identifying and battling threats in the identity security space. These insights are gathered from lessons learned across our global customer base, postbreach experience, frontline remediators, Red Team, and cutting-edge researchers.

As a recognized leader, we deliver a thorough and effective identity security plan:

- Our security solutions are trusted by over 70,000 customers worldwide, including more than 50% of the Fortune 500, across a wide range of industries, such as financial services, insurance, manufacturing, healthcare, and tech.
- Unit 42, our threat research, incident response, and security consultancy, is front and center in helping companies recover from some of the largest breaches of the 21st century.
- Our Professional Services and Customer Success organizations have real-world implementation and support experience. They also have a detailed, firsthand understanding of the risks that are present within human, machine, and AI identities and best practices.
- Leading research and advisory firms recognize CyberArk, a Palo Alto Networks company, as a leader across multiple identity security categories.³ They include access management, privileged access management, secrets management, nonhuman identity management, enterprise password management, identity threat detection and response, and identity fabrics.

3. *Magic Quadrant for Privileged Access Management*; Abhyuday Data, Paul Mezzera, Shubham Gera, Tarun Rohilla, Michael Kelley, Gartner, October 13, 2025; 2025 Forrester® Wave™: Privileged Identity Management Solutions, Forrester Research, August 7, 2025.

Conclusion

With physical and network barriers dissolved, all identities can be an attack path to an organization's most valuable assets. To secure these identities, turn to the recommendations and guidelines of Idira Identity Security Blueprint. Then, follow Rapid Risk Reduction Playbook to help you identify and mitigate the identity security liabilities that pose the greatest potential risk to your organization as quickly as possible.

Explore all the ways Idira can secure the identities across your organization. [Request a demo.](#)

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42 threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

Gartner® does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner's business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose.

Gartner and Magic Quadrant are a trademark of Gartner, Inc., and/or its affiliates.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
idira_wp_identity-security-blueprint-rapid-risk_050726