SPONSORED BY

PingIdentity

Identity orchestration: The new foundation of zero trust

SC Media CRA Business Intelligence © 2024 CyberRisk Alliance

ebook
An SC Media publication

Orchestrating true zero trust

Zero trust architecture has become more actionable than ever thanks to evolving NIST and CISA guidance, yet many organizations still have fundamental problems advancing zero trust maturity when it comes to incorporating the right vendors at the right time in their journey to zero trust. Identity orchestration makes it possible for anyone -- not just coding experts -- to create, test, and deploy secure user experiences from registration and sign-on, to identity verification, to ongoing authentication with the right vendor integrations. In this eBook, we look at the key components and processes of identity orchestration using PingOne DaVinci as an example.

Our experts:

- **Max Fathauer**, product marketing manager, Ping Identity
- **Raj Mallempati**, CEO, BlueFlag Security
- **Garrett Bekker**, principal analyst of information security, 451 Research

With the proliferation of mobile devices, the persistence of remote work, and the maturing of cloud computing -- coupled with ever-increasing attacker sophistication, it's never been more challenging or essential to move to a zero-trust security architecture.

Zero trust is a modern security model founded on the principle of "never trust, always verify" users and systems when they attempt to connect to a new resource. Zero trust requires all devices and users, regardless of location, to be authenticated, authorized, and continuously validated before being granted the access they seek. With the risks of implicit trust found in legacy security architectures eliminated in the zero-trust model, the probability of security breaches is reduced dramatically.

Garrett Bekker, principal analyst of information security at 451 Research, part of S&P Global, says that zero-trust architecture assumes threats exist inside and outside the network and assumes a breach is already underway, if not imminent. As a result, users and systems are continuously monitored for potentially malicious activity. By limiting user access to only the resources they need to do their jobs, zero trust heightens the organization's security posture. It limits the mobility attackers typically enjoy moving laterally through a victim's environment.

Of course, zero trust demands the secure management and use of digital identities. Effective identity and access management ensures that only those authenticated and authorized can access resources. This level of control is essential as criminals prove themselves increasingly capable. Because of this, research indicates a significant boost in zero-trust enterprise investment. According to research firm Market and Markets, global demand for zero trust will grow from $31 billion in 2023 to $68 billion in 2028 as enterprises seek these benefits.

© 2024 CyberRisk Alliance

> *"Identity must live at the core of any zero-trust model but getting a firm grip on all the identities within an environment—and the permissions and entitlements granted to those identities—is a difficult, if not impossible, thing to do manually."*
>
> — **Raj Mallempati** | CEO, BlueFlag Security

Forrester contends zero trust can better make security a business enabler by enhancing adaptivity, creativity, and resilience. Forrester argues that zero trust can help accelerate initiatives like new digital customer experiences, new partnership models, anywhere work, geographic expansion, cloud migrations, and edge computing deployments.

The trick, of course, is successfully overcoming the challenges of getting a zero-trust architecture in place. "Identity must live at the core of any zero-trust model but getting a firm grip on all the identities within an environment—and the permissions and entitlements granted to those identities—is a difficult, if not impossible, thing to do manually," says Raj Mallempati, CEO of BlueFog Security.

Foundations and challenges

Enterprises must implement zero trust correctly to gain the benefits of a more secure architecture. This includes the right foundational tools that set organizations on the right path by preventing vendor lock-in.

To help build that foundation, Max Fathauer, product marketing manager at Ping Identity, outlined how Ping Identity helps organizations on their journey to zero-trust architecture in a recent interview. The maturity model is built on several key pillars:

- **Establish an identity foundation with an adaptive authentication authority:** Centralize single sign-on and multi-factor authentication and integrate privileged access management, identity governance and administration, and device posture capabilities.
- **Phase out passwords: Implement passwordless** authentication methods to enhance security and user experience.
- **Dynamic authorization:** Centralize authorization policy to ensure that only the right people have the right post-authentication access to the right apps, APIs, and data within the context of their request.
- **Continuous verification:** Continuously validate the security configuration and posture of all users and network resources before granting access to applications and data.
- **Optimize user journeys:** Integrate the entire security stack and A/B test user journeys to ensure seamless and secure access to resources.

These pillars provide a roadmap for organizations to build a zero-trust architecture, with identity at its core, that will secure all their digital assets. Still, as the industry analysts and maturity models indicate, implementing zero trust is more than enhancing security (although that's compelling enough); it's also about enhancing the user experience while improving security. Yet, security and identity teams face considerable organizational and technical challenges to get there.

© 2024 CyberRisk Alliance

Key challenges to achieving zero trust include:

- **Attaining complete buy-in from other departments**. Scaling zero trust across the enterprise can be difficult due to resistance from other departments.
- **Erosion of traditional control points**. The shift to a "never trust, always verify" principle requires significant changes in managing security.
- **Integrating security silos**. Implementing zero trust requires a comprehensive view of security, which can be challenging when different parts of the organization have their own security policies and procedures.
- **Creating a single source of truth for risk**. Conflicting risk assessments can lead to users being granted or denied access to resources inappropriately.
- **Managing integration complexity**. Zero Trust solutions must integrate with numerous business and collaboration applications, which can significantly challenge organizations.

To meet these challenges, experts advise identity and security teams to focus on gaining visibility across all their assets, identities (user and machine), data flows, and user journeys.

Further, organizations must find a way to gain access across applications with as little friction as possible and foster clear communication regarding the zero trust efforts across departments. This is best achieved through what's known as identity orchestration.

"In our view, identity orchestration helps organizations accelerate their zero-trust journey because it provides visibility and oversight and ensures that your users are compliant with zero trust best practices,"
says 451 Research's Bekker.

Identity Orchestration: Composing the elements of zero trust

Organizations use identity orchestration to unify visibility into user journeys across various systems, including on-premises, cloud systems, applications, and platforms. Identity orchestration platforms provide control and oversight over the entire user journey through the plane of identity and access management — from registration and authentication to authorization, risk monitoring, and fraud detection. More than a mere authentication tool, identity orchestration enables users to create workflows, or user journeys, that establish how staff, partners, and customers securely access services and applications.

> *"Orchestration platforms are fantastic tools for administrators to automate tasks and provide detailed identity and access management to all processes within the network — across the cloud and on-premises. They help management access the rights to systems and ensure that the proper users will be able to obtain the rights to perform interactive functionalities on the systems."*
>
> — **Max Fathauer** | Product marketing manager, Ping Identity

© 2024 CyberRisk Alliance

Because identity orchestration simplifies access to applications, services, and data in a way that makes authentication and authorization events more seamless and secure, it improves both security and a better user experience. This is made possible by integrating multiple vendors and services across disparate cloud and on-premises systems onto the same canvas.

Identity orchestration platforms also allow anyone to create, test, deploy, and maintain identity experiences from registration and sign-on to ongoing authentication. This enables organizations to integrate new products and services quickly, streamline multi-vendor architectures without custom coding, and navigate multi-vendor, multi-cloud technologies.

Through identity orchestration, user and machine identities can be re-authorized at every step of their user journey where appropriate while also enforcing the principle of least privileged access. "When you place an authorization policy enforcement point right before someone gets into an app, you can recheck their risk level to make sure they're still trustworthy: that they are who they say they are and are in fact authorized to access what they're requesting," Fathauer adds.

Once in place, identity orchestration can help enterprises usher in more mature and automated authentication and authorization processes, especially as it relates to deciding when precisely policy is enforced in user journeys. This includes the ability to simplify a complex set of identity and access management processes, such as deciding whether to grant access to resources by vetting if access credentials are correct, the nature of the end users' devices, the geographic and network location, potential anomalies and, based on the totality of the inputs, decide whether to grant access.

© 2024 CyberRisk Alliance

Identity orchestration use cases

Identity orchestration can help organizations overcome challenges in several ways:

A seamless user experience. Identity orchestration allows organizations to integrate all their chosen identity vendors, creating automated workflows for different identity use cases, including authentication, identity proofing, and fraud detection. This eliminates disjointed user experiences caused by multiple, siloed identity systems.

Balancing security and user experience. Identity orchestration helps administrators strike the right balance between security and user experience. It gives admins the power to keep compliant users happy, while also introducing friction in non-compliant user journeys where needed.

Creating personalized user experiences. By making it faster and easier to create and manage secure user journeys by linking multiple services, identity orchestration enables digital teams to deliver more personalized user experiences. This includes creating new journeys tailored to support specific groups of users who might previously have been unable to interact with digital services.

Simplifying workflows. Identity orchestration simplifies identity-based workflows involving multiple systems. For example, setting up a passwordless online banking account for a new customer consists of allowing the customer to sign in and then verifying their identity as required by "know your customer" regulations.

Identity orchestration provides a flexible and adaptive integration framework that allows organizations to easily create identity journeys, automate workflows, and integrate applications and services, improving security and user experience.

© 2024 CyberRisk Alliance

Conclusion: Choosing the right identity platform

Identity orchestration offers a robust new path to zero trust. The first step of many organizations' journey to zero trust will be establishing an identity foundation, including centralizing single sign-on and multi-factor authentication, and integrating privileged access management, identity governance and administration, and device posture capabilities, all of which identity orchestration accelerates.

The orchestration engine should be capable of defining user journeys and integrating the entire security stack in a low-code manner. This includes the ability to orchestrate a secure authentication flow.

"Identity orchestration helps to accelerate your zero-trust journey. You can build out your zero trust program because you don't have to re-architect around the vendors you already use. It gives you visibility and oversight and lets you ensure your users comply with zero-trust best practices," says Fathauer.

The engine should also support the ability to place policy enforcement points to enable dynamic authorization, a needed step in ensuring that only the right people have access to the right resources within the context of their request. This is a crucial zero-trust principle, which requires strict identity verification for every individual or device attempting to access the network or application.

Moreover, the orchestration engine should provide improved visibility and control, enabling organizations to understand better who is accessing their resources and what they are doing with them. This is need for true real-time monitoring and continuous verification, essential components of a zero trust architecture.

Finally, the orchestration engine should enhance the user experience without compromising security. This can be achieved by eliminating the necessity for MFA for routine, low-risk transactions and streamlining access requests and approvals through automated policies and workflows.

Fathauer warns to look for vendor lock-in. "A lot of vendors operate in ways that make it very difficult to leave, and you don't want to choose an identity orchestration vendor that makes it hard to replace later on," he says. Fathauer advises to look especially for vendors that support open standards and have co-authored standards and other third-party guidance, demonstrating their commitment to reducing vendor lock-in.

By addressing this functionality, the right identity orchestration platform helps organizations build a zero-trust architecture with identity at its core, securing their digital assets and enhancing their security posture.

© 2024 CyberRisk Alliance

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. We let enterprises combine our best-in-class identity solutions with third-party services they already use to remove passwords, prevent fraud, support Zero Trust, or anything in between. This can be accomplished through a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect digital interactions for their users while making experiences frictionless. Learn more at www.pingidentity.com.

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications. To learn more, visit CyberRiskAlliance.com.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

© 2024 CyberRisk Alliance

MAKE EVERY CUSTOMER EXPERIENCE EFFORTLESS

Ready to deliver extraordinary experiences that surprise and delight? See why identity is the answer to frictionless customer journeys.

PingIdentity®