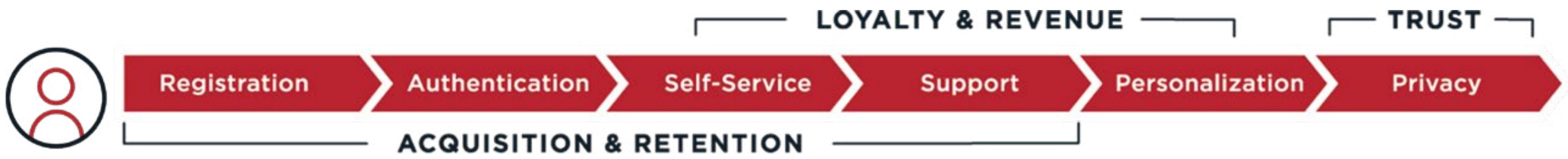
PingOne for Customers

DATASHEET



Customers expect every digital interaction to be seamless, secure and personalized. PingOne for Customers combines a no-code orchestration engine with authentication, user management and multi-factor authentication services to build, test and optimize digital customer experiences.

Increase Agility to Evolving Business Needs

Keep ahead of the competition and drive business with no-code identity orchestration that reduces the time to create and deliver seamless and secure customer experiences.

Acquire More Customers

By streamlining your registration with single sign-on (SSO) capabilities, you can reduce abandonment and acquire more customers.

Increase Customer Interactions

Once customers are registered, authentication services enable consistent sign-on experiences so you can drive increased engagement and revenue.

Deliver Consistent Multi-channel Experiences

Ensure that all applications have a consistent view of customer data so you can deliver personalized, multi-channel experiences to your customers following sign-on.

Key Features

- No-code identity orchestration to rapidly build, test and optimize customer experiences
- No-code identity orchestration to rapidly build, test and optimize customer experiences
- SSO and adaptive authentication across all apps
- Embed customer-friendly multi-factor authentication (MFA) in custom apps or use SMS or email OTPs
- Self-Service SSO integrations and delegated administration for application teams
- A single view of your customers across all applications

Capabilities & Benefits

No-Code Identity Orchestration

- Orchestration for frictionless, personalized and secure digital experiences
- Optimize and deliver customer journeys that balance security and convenience with identity proofing, account recovery, passwordless authentication, progressive profiling and more
- No-code flows with a drag-and-drop interface, workflow templates and A/B testing
- Out-of-the-box connectors to hundreds of third-party applications, including other identity and access management vendors
- Open RESTful APIs, identity standards and embeddable JavaScript widgets

Convenient Single Sign-On to All Apps

- Consistent credentials across all apps, including custom apps
- Social login, registration and account linking
- Eliminate passwords with passwordless authentication
- Standards support (OAuth, OpenID Connect, SAML)
- Developer-friendly APIs
- Customizable templates and UIs
- Robust authentication policies
- IdP discovery

Adaptive Multi-factor Authentication

- Comprehensive authentication policies that apply MFA based on risk
- Embed MFA (push and soft tokens) in custom iOS or Android apps
- SMS, email and voice OTPs
- Customer service identity verification with MFA
- Identity verification for high-risk transactions
- Admin portal to manage user devices
- Customers can create and manage trusted devices

Unified Customer Profile Across All Apps

- Unify disparate identity silos and datastores to create a single view of the customer
- Consolidate unified profiles with bi-directional sync, migration and coexistence
- Meet data residency requirements with logic to store data in local regions
- End-to-end data encryption
- Admin activity alerts and limitations
- Meet the most stringent enterprise security requirements
- Handle peak usage with ease when scaling without compromising performance

Cloud-based Solutions to Meet Your Needs

Select the PingOne for Customers solution package that enables you to meet business goals:

Essential

Rapidly build identity experiences using a no-code orchestration engine alongside authentication and user management capabilities

Plus

All Essential capabilities + MFA to remove friction and reduce the need for passwords all while enhancing customer security and improving user experience

Premium

All Plus capabilities + advanced user management and authentication to support complex architectures, custom application integration and the most extreme security and scale requirements

Visit www.pingidentity.com/en/platform/pricing.html for solution package details and pricing.

Integrations

Integration kits, adapters and connectors make deployment easy:

- Hundreds of connectors to third-party applications for orchestration of identity services
- Social identity connectors (Facebook, Google, Twitter and more)
- Risk, identity verification and online fraud detection service integrations
- RESTful agentless kits for any language
- Server kits

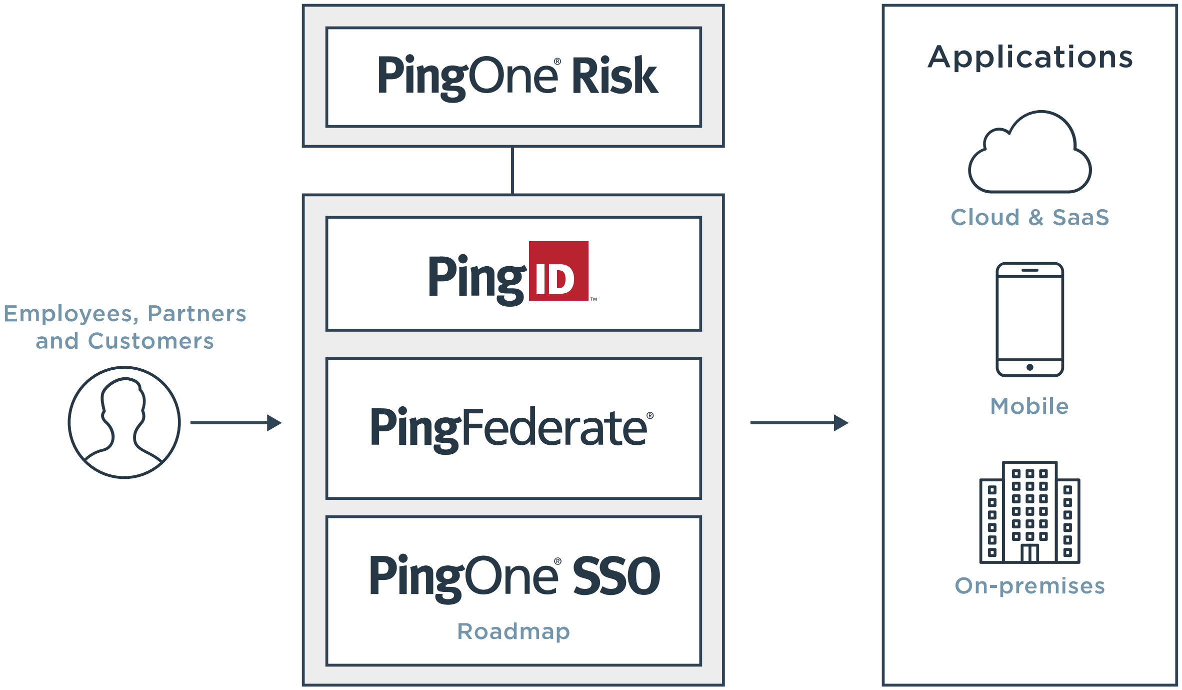
DATASHEET

PingOne® Risk

PingOne Risk is a cloud-based service that leverages machine learning and intelligent, configurable policies to secure authentication by evaluating multiple risk signals to verify user identity and detect potential threats.

Combine the PingOne Risk service with a variety of Ping products to continuously analyze contextual user information in order to understand the risk of granting access to an application. This allows you to make real-time decisions about the level of authentication required or if access should be denied. PingOne Risk detects potentially risky behavior through the use of machine-learning models and advanced analytics to evaluate different signals, including user behavior and entity analytics, anonymous network detection, IP reputation and impossible travel.

By understanding the level of risk, organizations can create intelligence-based, configurable policies that apply appropriate strong authentication for resources and provide trusted users with a passwordless experience. Organizations can increase security by accessing PingOne Risk dashboards to view reports on high-risk events and get in-depth insights on the authentication behavior of their users.



Employees, Partners and Customers

PingOne® Risk

PingID

PingFederate®

PingOne® SSO

Roadmap

Applications

Cloud & SaaS

Mobile

On-premises

EVALUATE RISK PREDICTORS TO DETECT MALICIOUS ACTIVITY

PingOne Risk leverages multiple risk predictors to learn user behavior and detect anomalies, thereby helping organizations make intelligent authentication decisions.

User and Entity Behavior Analytics

Legitimate users access applications and resources in predictable patterns, but bad actors don't adhere to these patterns when attempting to access enterprise systems. PingOne Risk leverages user and entity behavior analytics (UEBA) and machine learning in two ways to understand the behavior patterns of workforce users and detect potentially anomalous activity:

1. **User Risk Behavior** - PingOne Risk continuously learns the behaviors of users inside a workforce organization to determine what behavior is potentially abnormal for that organization.
2. **User-based Risk Behavior** - PingOne Risk compares activity of a specific user to the transaction history of that user to determine if the activity is abnormal for them.

The machine-learning models in PingOne Risk leverage a variety of data points to learn and detect anomalous behavior, including:

- Device type, operating system and version
- Browser type and version
- Time and day
- IP range
- User location

Using this behavior data, the machine-learning model will characterize abnormal activity as low, medium or high risk and prompt the user for the appropriate strong authentication.

Additionally, administrators can evaluate the UEBA functionality in PingOne Risk before deployment by viewing the output of the machine-learning model without affecting the authentication flow. This allows organizations to adjust rule settings to ensure only the right users gain access to resources.

Features & Benefits

- Cloud-based risk management
- User behavior insights for smarter authentication decisions
- Increased level of assurance in user identity
- Machine learning and advanced analytics to learn behaviors that are unique to users and organizations
- Differentiation of normal and abnormal authentication requests
- Aggregated risk policies that incorporate multiple risk signals
- Dashboards to provide security insights and reporting on high-risk events
- Multiple external data feeds that leverage a variety of threat indicators
- Integration with PingID and PingFederate along with an API for third-party services

Risk Signals Evaluated

- User and Entity Behavior Analytics
  - On a per organizational basis
  - On a per-user basis
- Anonymous Networks
- IP Reputation
- Impossible Travel
- IP Velocity
- User Velocity
- Custom Predictors

Anonymous Network Detection

Bad actors will typically use unknown VPNs, Tor and proxies to mask their IP address in order to sneak access to resources and applications. PingOne Risk analyzes IP address data from a user's device to determine if the address is originating from any type of anonymous network. If so, the user can then be prompted for step-up authentication or denied access. Additionally, PingOne Risk supports creating a whitelist to include an enterprise's VPN networks, ensuring that legitimate VPN users can access authorized resources.

IP Reputation

IP addresses are frequently reused in malicious activities such as DDoS attacks or spamming activity. If a user attempts to access an application that is associated with an IP address previously involved with suspicious activity, the probability of potentially risky behavior increases—and stronger authentication is then required. PingOne Risk analyzes data from different intelligence sources to determine the probability an IP address is associated with malicious activity and to request stronger authentication to verify the user's identity.

Impossible Travel

Users frequently log in to the same application from multiple locations throughout the day. However, a time lapse between the current login location and the previous location that is shorter than the time it would take to travel between the two points could indicate potentially suspicious activity. PingOne Risk analyzes location data to calculate if travel time between two login locations is physically possible. If the elapsed time is determined to be impossible, the user can be prompted with step-up authentication or denied access.

IP Velocity and User Velocity

Compromised user accounts are increasingly used by bad actors to gain access to resources and data. PingOne Risk detects anomalies by evaluating the following:

- IP Velocity - Detects the number of IP addresses a user is leveraging
- User Velocity - Detects the number of users originating from the same IP address

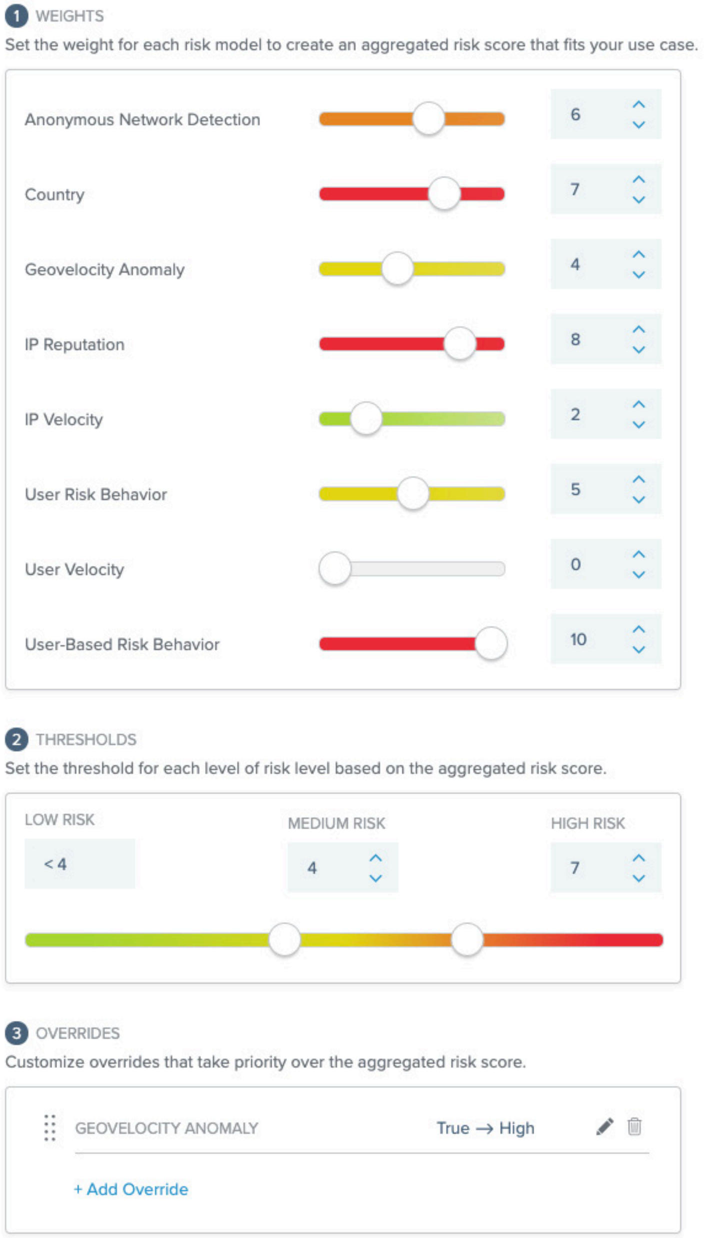
If the number of users or IP addresses is determined to be anomalous, the user will be prompted with step-up authentication or denied access.

Custom Predictors

Organizations leverage multiple risk signals from different sources to detect fraudulent activities across multiple scenarios. Combining all risk signal feeds into a single view can increase the security posture of the organization with an overall risk score that provides in-depth insight specific to the organization. PingOne Risk can be used to manage risk feeds by aggregating all vendors' signals into an overall risk score which allows organizations to take action depending on the level of risk calculated.

USE RISK AGGREGATION TO STRENGTHEN POLICIES

PingOne Risk enables administrators to configure intelligence-based policies by combining the results of multiple risk predictors to calculate a single risk score. Each risk predictor is assigned different weights to determine if a user poses low, medium or high risk to the organization and the level of authentication required. The thresholds for each risk level based on the aggregated risk score can be optimized to align with the organization's needs. Additionally, administrators can create multiple risk policies to apply in different use cases to meet business requirements.



1 WEIGHTS

Set the weight for each risk model to create an aggregated risk score that fits your use case.

Anonymous Network Detection	6
Country	7
Geovelocity Anomaly	4
IP Reputation	8
IP Velocity	2
User Risk Behavior	5
User Velocity	0
User-Based Risk Behavior	10

2 THRESHOLDS

Set the threshold for each level of risk level based on the aggregated risk score.

LOW RISK	MEDIUM RISK	HIGH RISK
< 4	4	7

3 OVERRIDES

Customize overrides that take priority over the aggregated risk score.

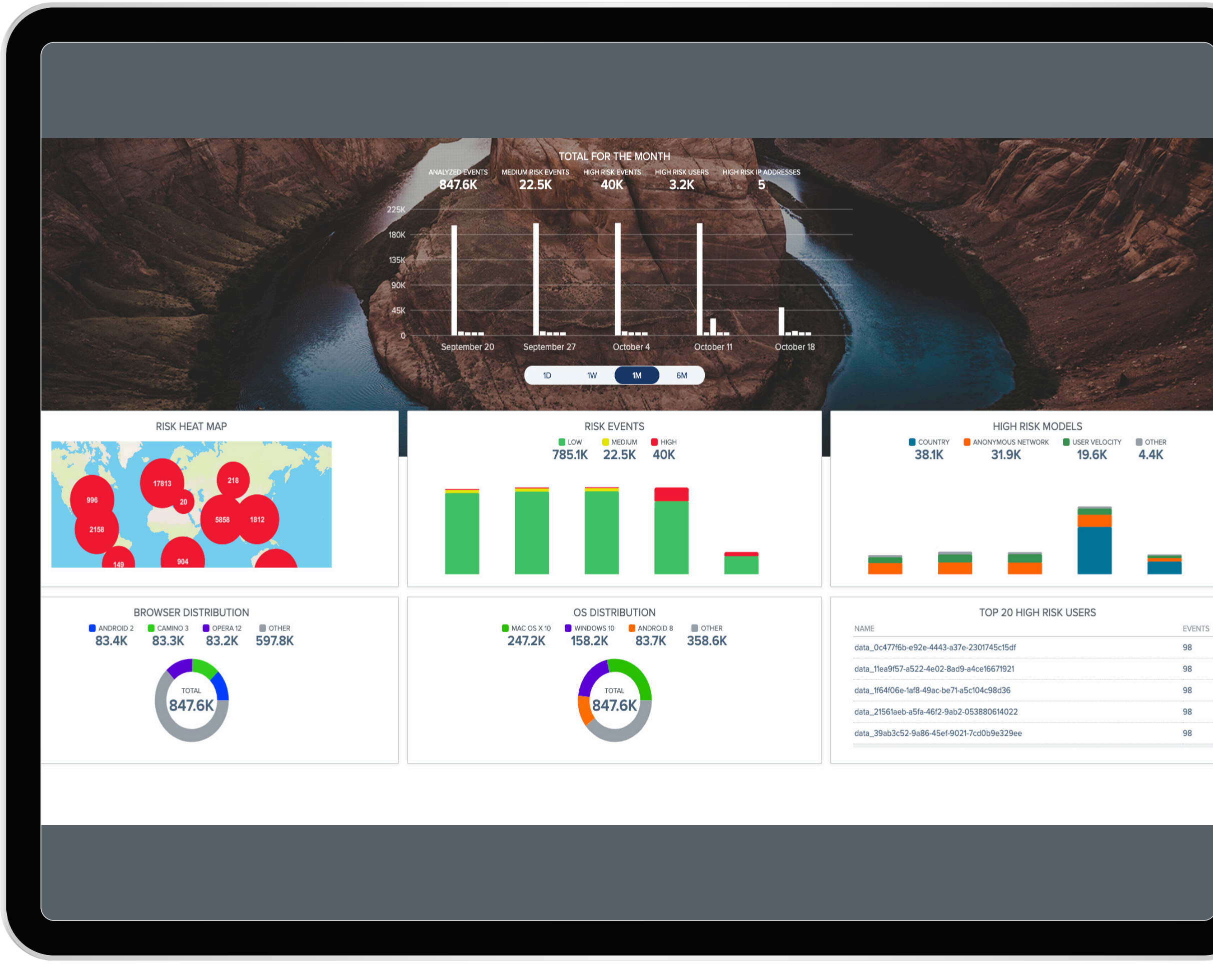
GEOVELOCITY ANOMALY True → High

GAIN INSIGHTS TO INCREASE SECURITY POSTURE

PingOne Risk provides a risk dashboard to give organizations in-depth insights into authentication behaviors to help make decisions that can strengthen security. Administrators can view reports on detected malicious activity and data on risky activity within an organization:

- Number of abnormal activities discovered
- Types of abnormal activities discovered
- A list of high-risk users
- Distribution of levels of risk
- High-risk locations

To learn more about PingOne Risk, visit pingidentity.com.



TOP 20 HIGH RISK USERS

NAME	EVENTS
data_0c477f6b-e92e-4443-a37e-2301745c15df	98
data_11ea9f57-a522-4e02-8ad9-a4ce16671921	98
data_1f64f06e-1af8-49ac-be71-a5c104c98d36	98
data_21561aeb-a5fa-46f2-9ab2-053880614022	98
data_39ab3c52-9a86-45ef-9021-7cd0b9e329ee	98

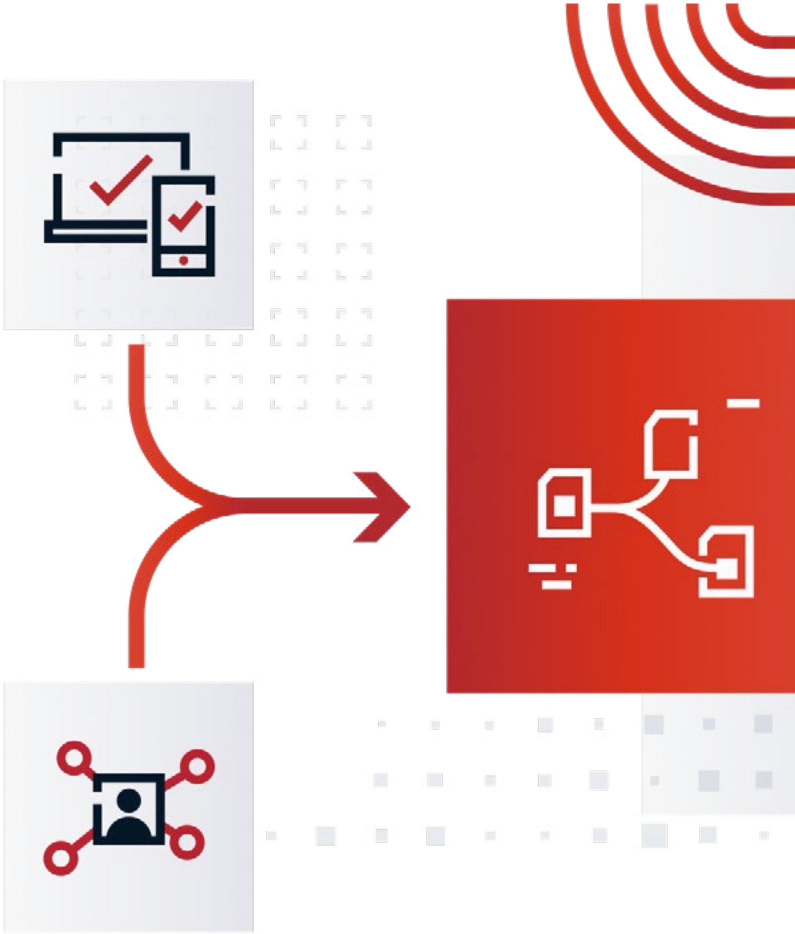
DaVinci

DATASHEET

Organizations constantly want to improve their digital experiences to gain a competitive advantage. However, identity systems are often a roadblock that are slow and inflexible to change. PingOne DaVinci solves that by providing no-code identity orchestration capabilities to integrate applications and create workflows, which ultimately provide seamless and secure user experiences across your entire technology stack.

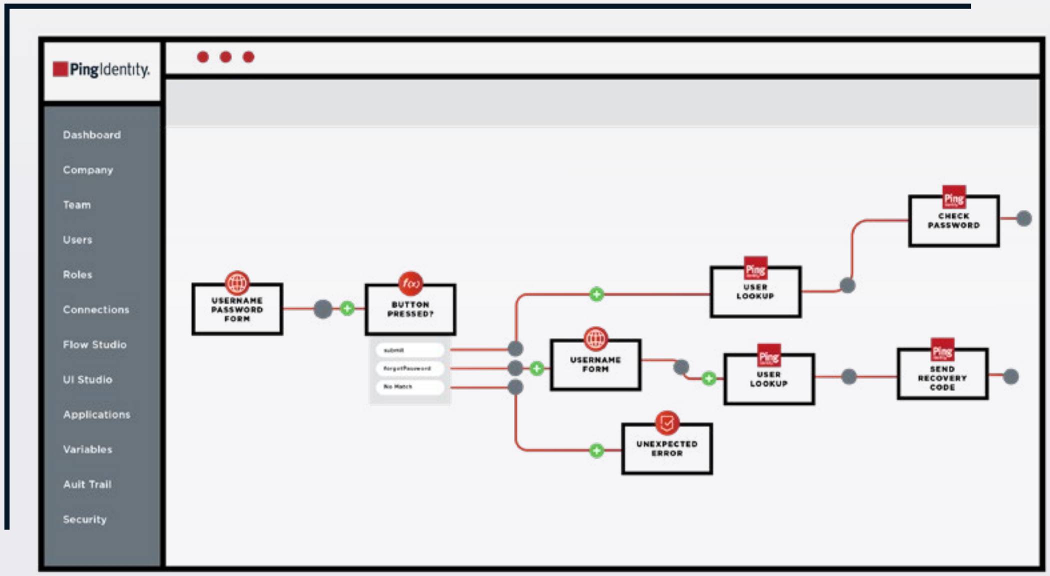
Features

- Identity orchestration for secure, frictionless and personalized user experiences
- Manage all identity use cases and journeys (fraud detection, verification, authentication, authorization, etc.)
- Out-of-the-box connectors to hundreds of third-party applications
- No-code flows with a drag-and-drop interface, workflow templates and rapid A/B testing
- Quick deployment with a single API call and an embeddable widget



How It Works

DaVinci is a cloud-based orchestration platform that allows you to stitch together applications and policies across the entire user journey via a no-code, drag-and-drop interface. It's deployed with a single API with an embedded widget that lets you design, test and push changes to your site in quick succession. DaVinci works across multiple applications and identity ecosystems to ensure easy adoption for all your use cases.



No-Code Orchestration

DaVinci enables organizations to design user-centric experiences without having to worry about long development timelines. You can connect applications, define the business logic and set policies through a drag-and-drop interface across your entire ecosystem. We also make it easy to implement, by collapsing what previously took thousands of lines of code into a single API call.

User Journey Optimization

Organizations need to run tests quickly and efficiently in order to provide the best user experiences possible. DaVinci empowers you to run identity experiments—for example, it could be subtle improvements to your registration experiences, adding a new or different passwordless option or trying out a new identity verification application. With DaVinci, you can run A/B tests with different user groups with speed and push these changes out in no time—without heavy developer resources or integration delays.

Frictionless Security

DaVinci is the lens into your entire user journey, across various facets of your identity ecosystem and use cases. With the visibility to see what various applications and security tools are embedded and triggered throughout a flow, you can begin to optimize and remove unnecessary friction. As a result, you can confidently take on new projects that will make your users happy, from self-service and "BYOD" policies to fraud detection, passwordless authentication and more.

Benefits

Business & IT Agility

Identity has become a mission-critical technology for all businesses. Previously, it was limited to identity experts or developers; but, orchestration changes all of that. With DaVinci, you no longer have to worry about integration delays or technology limitations. Instead, the conversation can be about the business and building better user experiences

Omnichannel

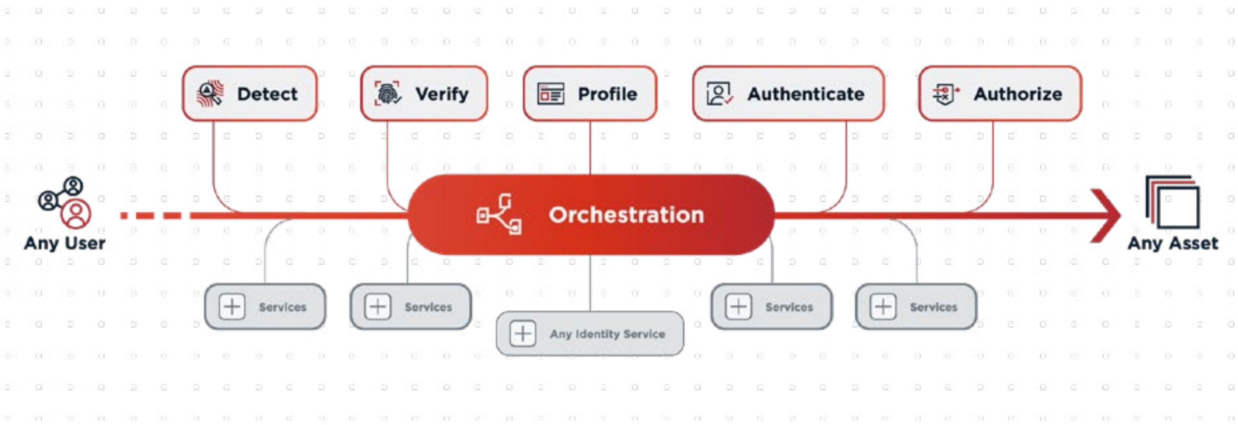
As the world goes increasingly digital, the way users interact with your brand must be consistent throughout all channels or you will risk losing customers and revenue to your competitors. DaVinci makes it easy to optimize experiences across multiple applications, devices and scenarios to deliver the types of experiences your customers are craving—and you can do this in rapid succession to keep up with your business growth.

Identity Independence

Whether you're all-in on a few vendors or prefer a best-of-breed approach to your technology stack, when it comes to orchestration, you need to be able to leverage your existing investments and keep your options open in the future. With DaVinci, we support hundreds of applications including other identity vendors—unlike our competitors. After all, you can only realize the benefits of orchestration if it provides coverage for your entire enterprise ecosystem.

DaVinci Provides:

- Control and visibility of the entire identity lifecycle, including fraud detection, registration, verification, authentication, authorization, risk monitoring and more
- Integrations to hundreds of enterprise applications and all facets of the identity security ecosystem, including—but not limited to—IGA, IAM, PAM and SIEM
- A library of template flows to implement across various identity use cases and scenarios.
- Support for open identity standards, such as SAML, OIDC, SCIM and FIDO2
- No-code drag & drop interface to easily implement and A/B test business logic
- Rapid cloud deployment via a JavaScript embeddable widget


Detect
Verify
Profile
Authenticate
Authorize
Any User
Orchestration
Any Asset
Services
Services
Any Identity Service
Services
Services