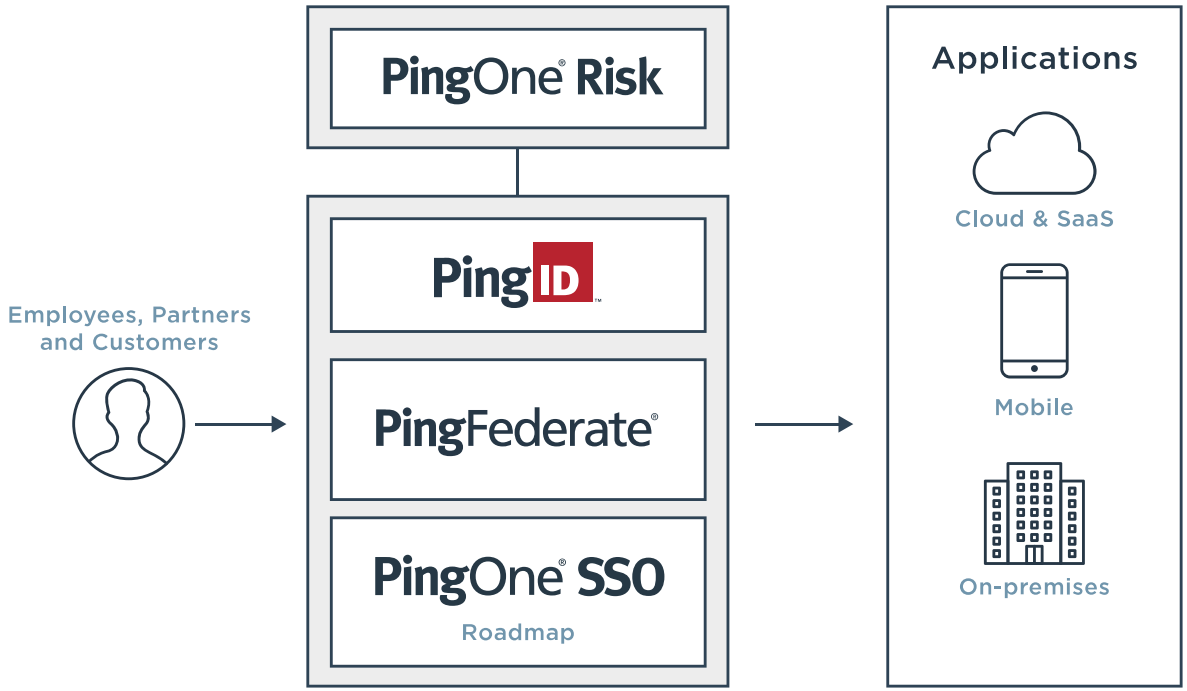
ProofID PingIdentity

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.



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

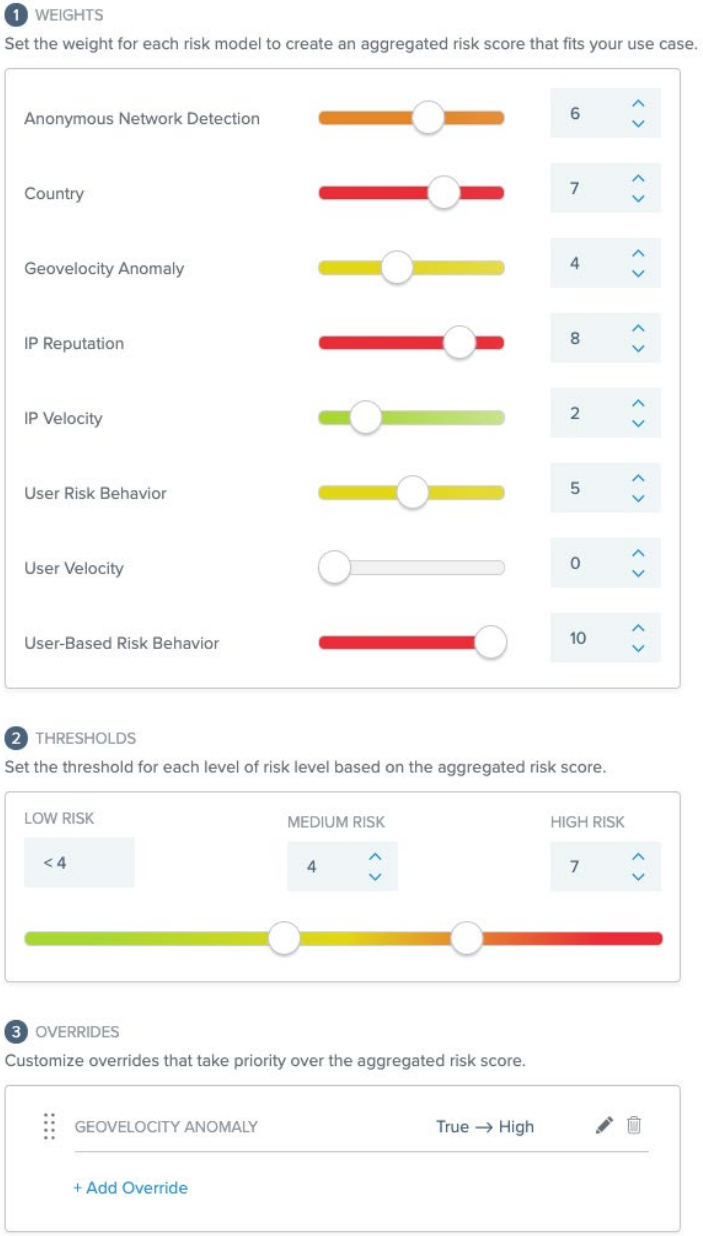
If the number of users or IP addresses is determined to be anomalous, the user will be prompted with step-up authentication or denied access.

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.



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 proofid.com

ABOUT PROOFID ProofID is a global identity security partner, integrator and service provider. Proven specialists, ProofID is committed to delivering pain-free, secure and seamless access and authentication experiences. Trusted by Tier 1 enterprises around the world to design, deliver and manage identity services, ProofID has successfully deployed their technology into regulated financial institutions with dynamic workforce needs, high street retailers that require seamless customer engagement, leading universities and worldwide charities. Their highly skilled team has been awarded more technical accreditations than any other Ping partner and earned Ping's Delivery Partner of the Year Award for three consecutive years. For more information, please visit www.proofid.com.

ABOUT PING IDENTITY Ping Identity delivers intelligent identity solutions for the enterprise. We enable companies to achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The PingOne Cloud Platform provides customers, workforce, and partners with access to cloud, mobile, SaaS and on-premises applications across the hybrid enterprise. Over 60% of the Fortune 100 choose us for our identity expertise, open standards, and partnerships with companies including Microsoft and Amazon. We provide flexible identity solutions that accelerate digital business initiatives, delight customers, and secure the enterprise through multi-factor authentication, single sign-on, access management, intelligent API security, directory, and data governance capabilities. For more information, please visit www.pingidentity.com.