Identity-centric Security for the Department of Defense and Intelligence Community

Enable Secure Access in Any Environment

Ping Identity.

FEDERAL GOVERNMENT
SOLUTION BRIEF

Old Technology Can't Support Your New Challenges

As your agency embraces modernization initiatives like telework, cloud computing and identity-centric security, you experience firsthand the limitations of legacy identity and access management (IAM) tools. As you're tasked to secure access for your increasingly remote workforce and support connectivity with mission partners and partner nations, you realize outdated identity security technology wasn't designed for today's threat landscape. Nor can it support the diversity of your hybrid IT environment, with systems holding various levels of sensitive information supported by cloud services and on-prem services, in some cases on low-bandwidth or air-gapped networks.

At the same time, the ever-present threat of bad actors looking to compromise government and private sector networks reveals growing gaps in agencies' Identity, Credential and Access Management (ICAM) programs. To address these new and evolving challenges, many agencies are moving toward a Zero Trust security posture in which you assume a state of breach. There is no implicit network trust and all access requests are verified based on dynamic context and risk. This transformation requires that you establish an identity-centric control plane for access security.

72% of government executives say outdated IT systems hurt their ability to respond to changing demands, and 79% say the age of their IT systems negatively impacts their mission.

Source: Modern Government: Connected. Powered. Trusted. KPMG, Feb 2021

Modern Identity Supports Your Mission-critical Requirements

Secure Access for Every Network

Department of Defense (DoD) and Intelligence Community (IC) agencies have a variety of network types in their environments that hold a range of sensitive information. Whether they are internet-connected, air-gapped, low-side, or high-side networks, agencies must offer secure, dependable access so employees and mission partners can conduct interoperable mission work.

To ensure agencies can support all access needs, Ping offers a variety of deployment options for its workforce identity solutions, including on-premises software, as code, through Docker images to host in private clouds and as a fully managed software-as-a-service (SaaS).

Increase Cloud Adoption

For internet-connected environments, moving services from on-premises data centers to the cloud can lessen time and budget spent on operating and maintaining underlying infrastructure; however, not every cloud solution is viable for DoD and IC agencies. PingOne for Government is In Process at FedRAMP's Moderate impact level — equivalent to DoD Impact Level 2 — to help you and your contractors secure, modernize and future-proof hybrid IT environments according to federal standards and demonstrate compliance with both FedRAMP and the Cybersecurity Maturity Model Certification (CMMC).

If you leverage DevOps practices, Ping delivers cloud-ready containerized software that can be automated to deploy anywhere and everywhere across your multi-cloud, hybrid environment.

Uplevel ICAM Initiatives

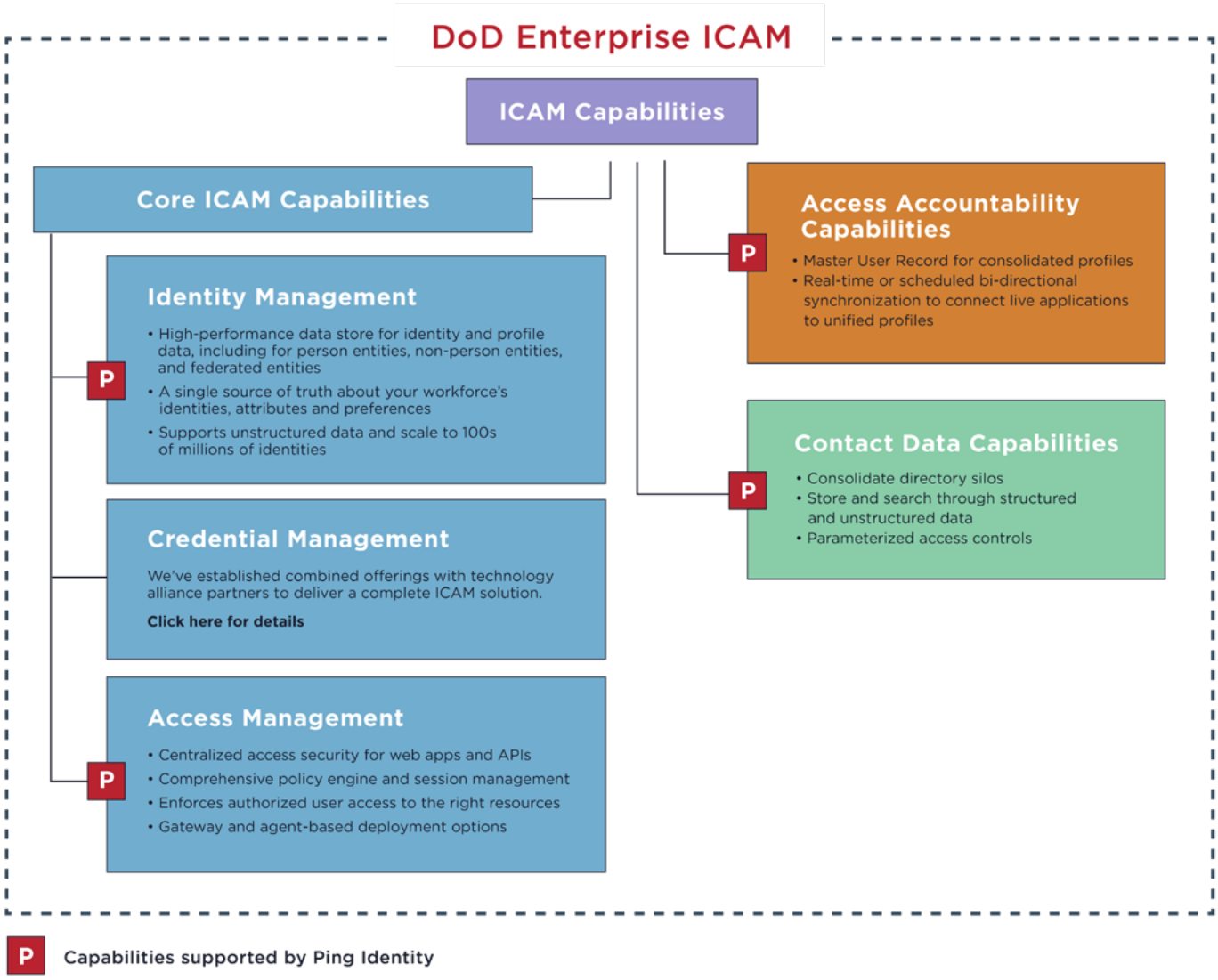
You need a way to both expand the reach of your existing PIV/CAC cards and enable a Bring Your Own Authentication (BYOA) environment to strengthen authentication and secure every digital asset—without forcing your users to re-enroll in yet another MFA silo. Your IT organization can accelerate work-from-anywhere and cloud initiatives by upleveling your enterprise ICAM program with modern federation, identity management and access management from Ping Identity. And since Ping's solutions are standards-based, they easily co-exist with your legacy applications so you can avoid a rip-and-replace situation.

Set the Stage for Zero Trust

Zero Trust requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they're sitting within or outside the network perimeter. Your workforce authentication authority from Ping delivers an identity control plane so you can secure access for every user population, asset, environment and endpoint across your environment.

An Authentication Authority for the DoD/IC

An authentication authority is a powerful combination of federation, identity management and access management components.



DoD Enterprise ICAM is the DoD's implementation of Identity, Credential and Access Management (ICAM). ICAM is the set of tools, policies and systems an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.

Get the latest DoD Enterprise Identity, Credential and Access Management (ICAM) Reference Design at https://dodcio.defense.gov/Library/

Secure and Streamline Access for the Good of the Nation

Secure Remote Access for Everyone

Your ability to provide your workforce secure and seamless access to digital assets from anywhere is mission-critical. With Ping, you can confidently ensure and enforce that the right people have the right access to what they need, when they need it to complete their tasks in support of your goals.

Accelerate Cloud Initiatives

Abandon the notion that "cloud" is separate and requires new cloud identities. Embrace cloud-smart initiatives with an identity platform that keeps you in control. Manage access to all your resources across your hybrid IT environment and meet the federal government's required security controls.

Prevent Identity Silos

You don't need more identity silos; you need a single source of truth that gives you the ability to manage identities and access with a central identity control plane. Ping's workforce authentication authority solution lets you break down the identity silos and overcome hybrid IT challenges.

Protect Every Asset in Every Environment

Ultimately, all assets point back to identity. It's critical to choose an identity security provider that can connect all your multi-generational assets, no matter where they're hosted, using out-of-the-box standards and integration kits.

Lay the Foundation for Zero Trust

An authentication authority provides a solid foundation for an identity-centric security posture, making it easier to transition to a Zero Trust environment as outlined by the DoD's Zero Trust Reference Architecture.

Demonstrate Compliance

Defense and intelligence agencies and federal contractors all have compliance mandates they must meet to demonstrate they are keeping federal data secure when using cloud solutions. Ping's FedRAMP In Process solution will make it easy to demonstrate compliance with DoD Impact Level 2.

To learn more about our solutions for the Federal Government, visit www.pingidentity.com/fedgov