BeyondTrust

SOLUTION BRIEF

Strategically Securing Federal Data in the Next Normal

Mapping BeyondTrust Solutions to the Continuous Diagnostics and Mitigation (CDM) Phases

CONTENTS

Introduction to CDM 1

Breaking Down the CDM Phases 3

BeyondTrust and CDM 4

The Attack Chain 10

The BeyondTrust Privileged Access Management Platform 12

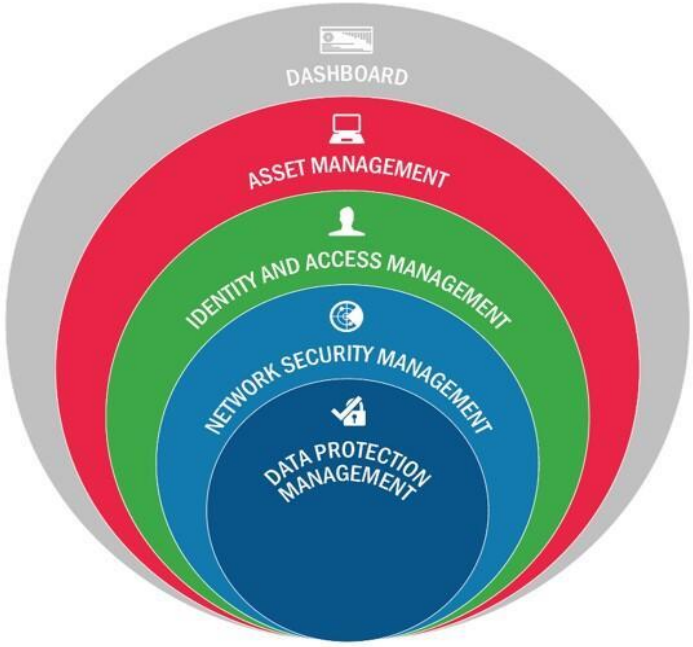
Introduction to CDM

According to The Cybersecurity and Infrastructure Security Agency (CISA), The Continuous Diagnostics and Mitigation (CDM) Program provides a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture by:

- Reducing the agency threat surface
- Increasing visibility into the federal cybersecurity posture
- Improving federal cybersecurity response capabilities
- Streamlining Federal Information Security Modernization Act (FISMA) reporting

The CDM Program was developed in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational tiers.

The Cybersecurity & Infrastructure Security Agency breaks down the CDM phases in the diagram opposite.



Breaking Down the CDM Phases

Phase 0: Foundational - Dashboards:

CDM Agency Dashboards receive, aggregate, and display information from CDM tools on agency networks and then push summarized information for display on the CDM Federal Dashboard.

- The CDM Agency Dashboard displays data about devices, users, privileges, and vulnerabilities. This dashboard collects and arranges detailed information on vulnerabilities gathered and provides an object-level view of an agency's cybersecurity posture.

- The CDM Federal Dashboard gives CISA and the Office of Management and Budget (OMB) visibility across all federal networks to better understand how participating agencies are managing their cyber risk and to ultimately improve cybersecurity across the Federal Government. The information retrieved through this dashboard helps determine if additional resources, guidance, policies, or directives are needed to improve risk management at the agency level.

The BeyondTrust solution set, through the BeyondTrust BeyondInsight management console integrates with any CDM dashboard via the use of Structured Query Language (SQL) queries.

Phase 1: Asset Management | What is on the network?

Managing "what is on the network?" helps agencies monitor devices on their network.

Phase 2: Identity and Access Management | Who is on the network?

Managing "who is on the network?" helps agencies monitor who uses their networks and what kind of access and privileges those users have.

Phase 3: Network Security Management | What is happening on the network? How is the network protected?
Managing "what is happening on the network?" and “how the network is protected” helps agencies protect against hacking, misuse, and unauthorized changes to internal and external boundary defenses.

Phase 4: Data Protection Management | How is data protected?
Managing “how is data protected?” helps agencies protect highly sensitive data (especially data with personally identifiable information) on their networks.

CDM DEFEND

The scope of CDM DEFEND encompasses all activities that support CDM capabilities, including:

- Deploying CDM capabilities across the .gov domain
- Deploying the capabilities within groups of agencies to achieve volume discounts and other cost efficiencies
- Providing flexibility for different requirements in terms of agency readiness, complexity, location of data (on premise/mobile/cloud), and mission objectives
- Supporting the use of innovative products
- Offering “shared service” options for agencies where sharing costs and skilled support yield the most benefit

BeyondTrust and CDM

We have a unique set of integrated solutions to address a wide range of architectures, including CDM, enabling agencies to achieve Zero Trust security goals. BeyondTrust provides full multi-tenant support, where agencies can have their own views and control their own environments. We support the following use cases: PIV Card Enablement, FIPs 140-2, and IPV6 compliant.

Our solutions have a low total cost of ownership as BeyondTrust can architect with less appliances (virtual or physical) and manage several licenses with a single product, while lowering maintenance costs over time. Our implementation and configuration services have a quick time to value with our all-inclusive model of features and functionality.

Ultimately, BeyondTrust provides your agency with the ability to do more with less manpower, not eliminating jobs, but allowing employees to tackle additional mission critical projects.

Phase 0: Foundational – Dashboard and Simplified Management

BeyondInsight (BI) - Centralized management, reporting and threat analytics for Privileged Access Management (PAM).

- BeyondInsight is BeyondTrust's platform for centralized management, reporting, and threat analytics for Privilege Access Management (PAM). It delivers unmatched visibility and control over privileged access activity, simplifies deployment, automates tasks, improves security, and reduces privilege related risks.
- Deep reporting and advanced privileged threat analytics correlate data from a variety of BeyondTrust and third-party solutions to uncover critical privilege related threats and identify weak points for hackers to exploit. BeyondInsight also allows for endpoint policy management, granular control, and flexible assignment process with smart rules.
- BeyondInsight allows your security team to maintain complete and ongoing visibility over all privileges in your environment.

Phase 1: Asset Management | What is on the network?

BeyondInsight (BI) Asset Discovery - centralized management reporting, delivering unmatched visibility and control over privileged access activity, automating tasks, improving security, and reducing privilege related risks.

- Operates within the BeyondInsight platform
- Integrated component with the Unified Vulnerability Management (UVM) appliances
- Provides endpoint scanning and usage details
- Configurable to function in a variety of networking infrastructure environments

Phase 2: Identity and Access Management | Who is on the network?

(PPM) Privilege Password Management- Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities. This solution includes Password Safe (PWS).

- Operates within the BeyondInsight platform
- Managed Service Provider capable for management of distinct and secure operating groups
- Single console for management of assets and privileged accounts
- Allows for a consistent user experience for managed privileged account usage with RDP, SSH, Telnet and application injection

Privilege Management for Unix/Linux (PMUL) - Achieve compliance, control privileged access, prevent and contain breaches on Unix or Linux systems.

- Integrates with the BeyondInsight platform
- Implements a true least privilege delegation model allowing users to run commands at a higher privilege level according to policy
- Integrates with Password Safe for management of privileged account access and use

Active Directory (AD) Bridge - Extend Microsoft® Active Directory authentication, single sign-on capabilities and Group Policy configuration management to Unix and Linux systems.

- Integrates with the BeyondInsight platform
- Centralizes authentication for Unix, Linux and Mac hosts by extending Active Directory and Kerberos authentication
- Allows for consistent configuration of hosts by extending Active Directory group policy to Unix/Linux hosts
- Provides ability to consolidate credentials which reduces the overall attack footprint of the Unix/Linux hosts

Phase 3: Network Security Management | What is happening on the network? How is the network protected?

BeyondInsight Asset Discovery (BI) – centralized management reporting, delivering unmatched visibility and control over privileged access activity, automating tasks, improving security, and reducing privilege related risks.

- Robust analytics and reporting engine allows for current state reporting, activity history reporting and trend analysis
- Single collection point for audit information from most BeyondTrust solution sets

(PPM) Privilege Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities. This solution includes Password Safe (PWS).

- Operates within the BeyondInsight platform
- Provides comprehensive audit history of all privileged activity completed through the product
- Ability to control what access is allowed under differing circumstances

Privilege Management for Unix/Linux (PMUL) - Achieve compliance, control privileged access, prevent and contain breaches on Unix or Linux systems.

- Integrates with the BeyondInsight platform
- Provides comprehensive audit history of all privileged activity completed through the product
- Command history indexed for easier audit history investigation

Secure Remote Access (SRA) - Apply least privilege and robust audit controls to all remote access required by employees, vendors, contractors, and service desks.

- Encrypted point-to-point access capabilities
- Session recording and auditing

Phase 4: Data Protection Management | How is data protected?

(PPM) Privilege Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities. This solution includes Password Safe (PWS).

- Operates within the BeyondInsight platform
- Continuous auto-discovery to safeguard new assets and privileged accounts
- Ability to dynamically end individual sessions

- Roles based access enforced at the managed asset and managed privileged account level

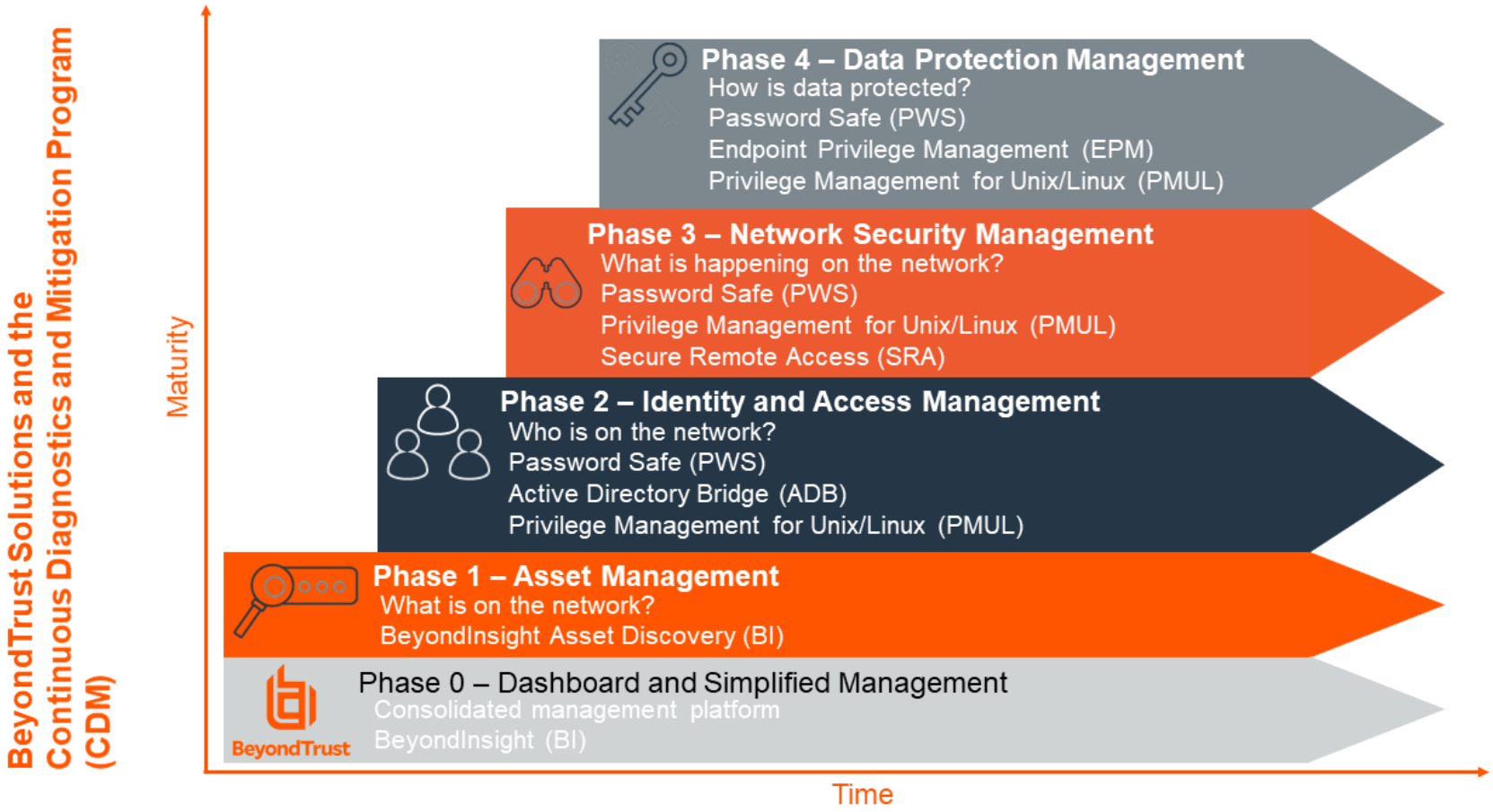
Endpoint Privilege Management (EPM) - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

- Integrates with the BeyondInsight platform
- Enforce least privilege and eliminate admin rights at the operating system level to ensure access to data is appropriately managed
- Comprehensive support including:
  - Windows (desktop and server)
  - Apple macOS
  - Network devices
  - Unix and Linux systems
- Built-in logic to detect and stop common malware introduction paths and processes

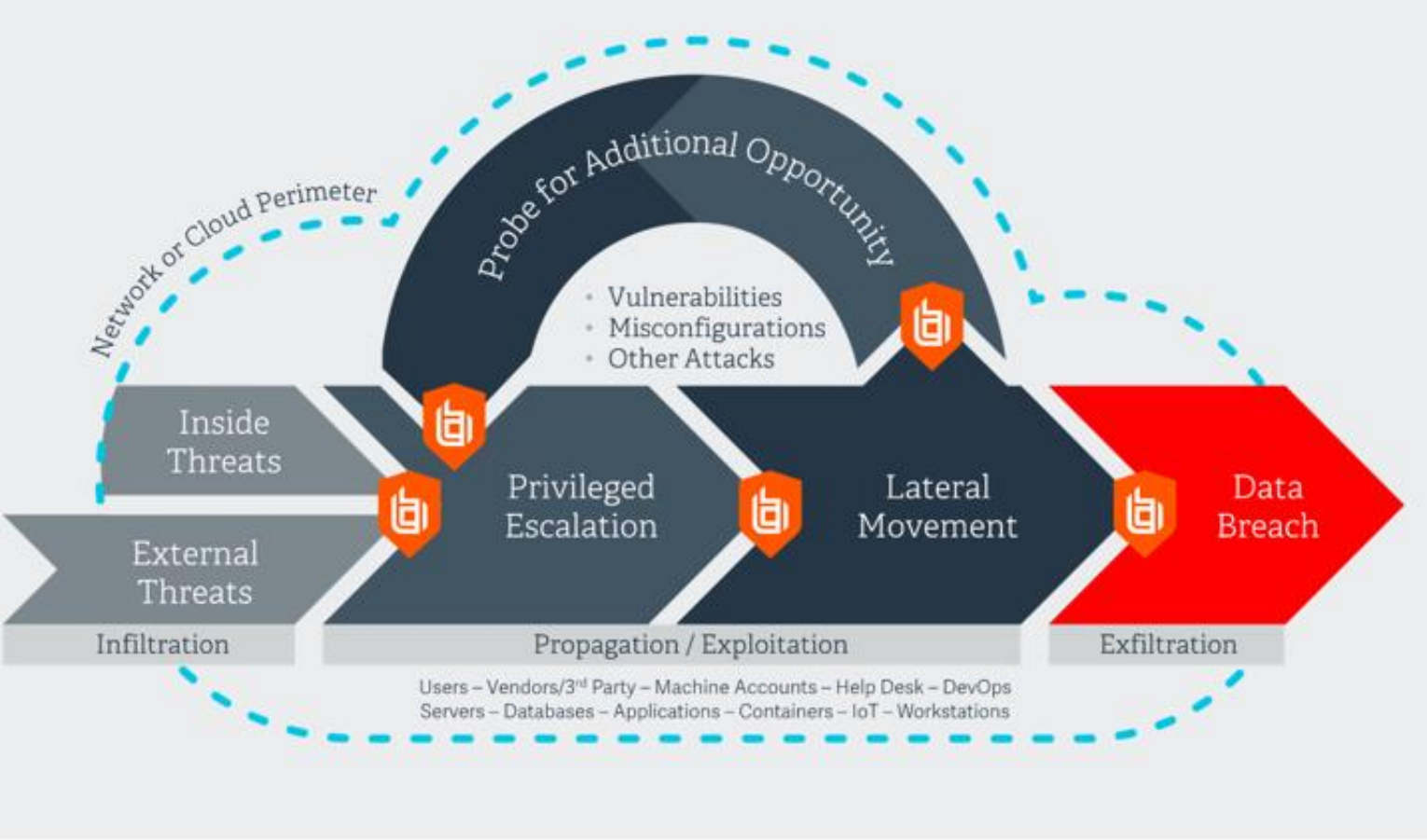
Privilege Management for Unix/Linux (PMUL) - Achieve compliance, control privileged access, prevent and contain breaches on Unix or Linux systems.

- Integrates with the BeyondInsight platform
- Robust policy engine allows for the granular assignment of privilege elevation ensuring access to data is appropriately managed

The following is a visual graph highlighting where BeyondTrust solutions map to each CDM Phase:



The Attack Chain



The BeyondTrust solution set helps agencies stop the attack chain at multiple points.

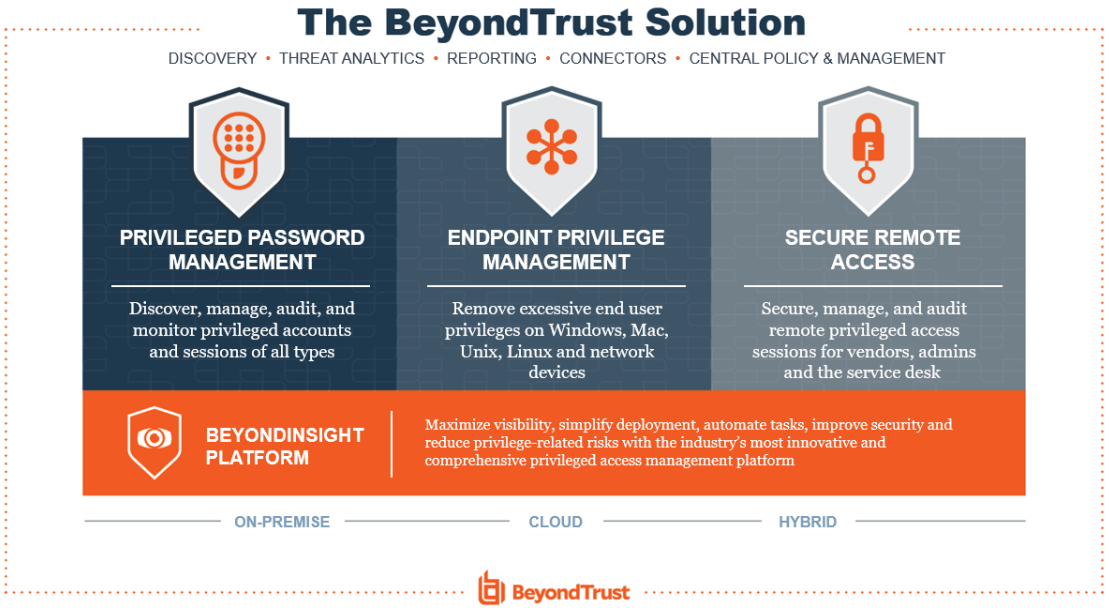
Whether an insider or external threat, once an attacker gains admin-level privileges they can move laterally around your network often unnoticed. BeyondTrust solutions break the attack chain at multiple points to quickly stop threats and mitigate damage.

Each BeyondTrust Stop Sign:

1) **External Threats:** Our Secure Remote Access solutions will protect the pathways into your network.
2) **Privileged Escalation:** Our entire solution set will prevent the misuse of privileges within your environment.
3) **Lateral Movement:** Command and application whitelisting/blacklisting (entire BeyondTrust solution set).
4) **Vulnerabilities/Exploits/Privileged Attacks:** Advanced capabilities of Endpoint Privilege Management (verifying caller application and source).
5) **Probing for Additional Opportunity:** Protection of "always on" accounts with Just-in-Time access.
6) **Data Breach:** File integrity monitoring built into Endpoint Privilege Management to secure sensitive files.

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions. BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace. By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.