BeyondTrust

Mapping BeyondTrust Capabilities to the Digital Operational Resilience Act (DORA)

Regulation (EU) 2022/2554

This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under Digital Operational Resilience Act (DORA). BeyondTrust is not representing that we are subject to or compliant with DORA.

Overview

The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, places significant emphasis on cybersecurity as a component of operational resilience within the financial sector.

Recognising the increasing frequency and sophistication of cyber threats targeting financial institutions, DORA aims to fortify cybersecurity measures to ensure the continuity and stability of financial systems.

The Digital Operational Resilience Act specifically mandates stringent cybersecurity requirements for financial entities operating across the European Union to employ protection, detection, containment, recovery, and repair capabilities against ICT-related incidents. The Act includes risk management frameworks, cybersecurity protocols, secure data storage and transmission practices, as well as comprehensive incident reporting mechanisms to achieve these capabilities. In its execution, DORA seeks to bolster the defense mechanisms of financial institutions against cyberattacks, mitigate potential disruptions, and preserve overall trust in the financial system.

This overview has been prepared so that banks and financial service providers subject to DORA can quickly understand how IT and security teams within these organisations may use this paper to gain a clearer understanding of DORA requirements, learn more about BeyondTrust solutions, and discover how they can be used to support many of their own obligations under the DORA framework.

The Digital Operational Resilience Act has been constructed around 10 chapters, each outlining specific requirements and recommendations related to cybersecurity controls such as threat response, governance, and training. These chapters each contain detailed Articles on requirements ranging from specific cybersecurity architectures to personnel policies.

This paper will be limited to the most relevant articles included in Chapter II: ICT Risk Management of the Digital Operational Resilience Act, listed below.

Chapter II: ICT Risk Management

Article 5: Governance & Organisation
Article 7: ICT Systems, Protocols, and Tools
Article 8: Identification
Article 9: Protection & Prevention
Article 10: Detection
Article 11: Response & Recovery
Article 16: Simplified ICT Risk Management Framework

About BeyondTrust Solutions & DORA

An established leader in identity security and privileged access management (PAM), BeyondTrust has a rich history of helping banks, financial institutions, and other highly regulated organisations align to stringent and complex compliance frameworks across the world. Our customers trust us to help support their compliance with cybersecurity frameworks including SOX, PCI-DSS, SOC2, HIPAA, and more – including DORA.

BeyondTrust solutions support your needs to achieve many of the requirements of the DORA framework across several Articles contained within **CHAPTER II: ICT Risk Management.** The following section directly maps these solutions to the DORA guidelines to which you can use each to help achieve your obligations.

Mapping BeyondTrust PAM to DORA Requirements

CHAPTER II: ICT Risk Management					
Article	**Description of Requirement**	**Identity Security Insights**	**Privileged Remote Access**	**Endpoint Privilege Management**	**Password Safe**
Article 5: Governance and Organisation	This article emphasises the importance of effective governance and organisational structures within financial entities to manage Information and Communication Technology (ICT) risks.	●	●	●	●
Article 7: ICT Systems, Protocols and Tools	To address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols, and tools.	●	●	●	●
Article 8: Identification	2. Financial entities shall, on a continuous basis, identify all sources of ICT risk… and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets.	●	●	●	●

CHAPTER II: ICT Risk Management					
Article	**Description of Requirement**	**Identity Security Insights**	**Privileged Remote Access**	**Endpoint Privilege Management**	**Password Safe**
Article 9: Protection and Prevention	4. As part of the ICT risk management framework financial entities shall: (c) implement policies that limit the physical or logical access to information and ICT assets to what is required for legitimate and approved functions and activities only, and establish of policies, procedures and controls that address access rights and ensure a sound administration thereof.	●	●	●	●
Article 10: Detection	1. Financial entities shall have in place mechanisms to promptly detect anomalous activities 3. Financial entities shall devote sufficient resources and capabilities to monitor user activity and the occurrence of ICT anomalies	●	●	●	●

CHAPTER II: ICT Risk Management					
Article	**Description of Requirement**	**Identity Security Insights**	**Privileged Remote Access**	**Endpoint Privilege Management**	**Password Safe**
Article 11: Response & Recovery	Financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity. (a) Ensure the continuity of the financial entity's critical or important functions. (b) Quickly, appropriately, and effectively respond to, and resolve, all ICT-related incidents. (c) Activate, without delay, dedicated plans that enable containment measures Financial entities shall put in place, maintain, and periodically test appropriate ICT business continuity plans, notably regarding critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	●	●	●	●
Article 16: Simplified ICT Risk Management Framework	Financial entities shall: 1b. Continuously monitor the security and functioning of all ICT systems. 1c. Minimise the impact of ICT risk with sound, resilient, and updated ICT systems, protocols, and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems. 1d. Allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected.	●	●	●	●

Mapping BeyondTrust PAM to DORA Requirements Cont

BeyondTrust's suite of solutions can help your organization strongly align with the Digital Operational Resilience Act (DORA) by enhancing governance frameworks, risk management, and compliance across several key areas. BeyondTrust's tools establish clear governance managing privileged access and enhancing visibility into identities and entitlements, which is critical for Articles 5 and 8 of DORA.

Additionally, BeyondTrust supports regular ICT testing as mandated in Article 7 by securing and controlling access during external testing phases. BeyondTrust's solutions also facilitate robust incident detection and response strategies required by Articles 10 and 11, by offering advanced analytics and real-time monitoring to detect threats early and efficiently manage recovery processes.

Finally, BeyondTrust caters to smaller financial entities through tailored insights and proportional risk management, ensuring compliance without the overhead of complex systems and aligning with Article 16's requirements for a simplified risk management framework. These capabilities ensure that financial institutions can maintain operational resilience and effectively manage ICT risks, thereby adhering to the stringent requirements set forth by DORA.

Based on excerpts from DORA, below are several points and subsections that you can use BeyondTrust solutions to help address. Please note that not all points and subsections are included in this mapping; only the areas that BeyondTrust solutions support are included.

Article 5: Governance & Organisation

This article within the Digital Operational Resilience Act emphasises the importance of effective governance and organisational structures within financial entities to manage Information and Communication Technology (ICT) risks.

All BeyondTrust solutions enable a range of governance, auditing, and policy implementation capabilities, allowing institutions subject to DORA to meet the requirements described in Article 5 and in the following paragraphs.

How BeyondTrust Enables Your Compliance with Article 5

Establishment of Clear Governance Frameworks

Financial entities are required to implement robust governance frameworks that clearly define roles, responsibilities, and accountability for managing ICT risks.

BeyondTrust **Privileged Remote Access** alongside **Password Safe** provides a centralised platform for managing privileged access, aligning with the need for a clear governance framework. It allows for detailed role definitions and enforces accountability by managing and monitoring privileged user activities.

BeyondTrust **Identity Security Insights** discovers and provides visibility into identities, accounts, privileges, entitlements, and paths to privilege across the identity estate – on-premises, cloud, and SaaS. It allows organisations to understand where privileges exist, how they are connected, where controls are lacking, and where they may be abused across their interconnected environment, enabling them to make informed decisions to establish effective policies to enforce least privilege access and controls.

Management Body's Role

The entity's management body should be well-informed about ICT risks and actively oversee the ICT risk management framework.

All BeyondTrust solutions provide comprehensive audit trails and reporting capabilities, facilitating transparency and oversight by the management body. This feature is crucial for demonstrating compliance with DORA requirements.

Resource Allocation

Adequate resources (human, technological, and financial) must be allocated to manage and mitigate ICT risks.

BeyondTrust products are designed to minimise the burden on technical teams to deploy and maintain, allowing your team members to manage a multitude of risks without incurring unnecessary manual overhead.

Though not directly related to the resource allocation as defined in this article, **Endpoint Privilege Management** ensures that users only have the access necessary to perform their job functions (least privilege) just in time. This minimises the risk of unauthorised access or misuse of privileged information, a core element of ICT risk management.

Article 7: ICT Systems, Protocols, and Tools

Article 7 of Chapter II in the Digital Operational Resilience Act (DORA) focuses on the "Testing of ICT tools, systems, and processes." This article mandates financial entities to regularly test their Information and Communication Technology (ICT) tools, systems, and processes to ensure their operational resilience.

The key aspects of this article typically include:

- **Regular Testing:** Financial institutions are required to conduct regular testing of their ICT tools, systems, and processes to assess their ability to withstand ICT disruptions and threats.
- **Range of Testing Activities:** This involves a variety of testing methods, such as vulnerability assessments, penetration testing, scenario-based testing, and more.
- **Identification and Mitigation of Vulnerabilities:** The testing should help in identifying vulnerabilities in the ICT systems and processes, and institutions must take actions to mitigate these risks.
- **Reporting of Testing Outcomes:** Entities are required to document and report the outcomes of these tests to their management bodies and, in some cases, to the relevant supervisory authorities.
- **Use of External Parties for Testing:** Financial entities may use third-party service providers for testing, provided these services meet certain standards and do not compromise the integrity of the tests.

How BeyondTrust Enables Your Compliance with Article 7

BeyondTrust not only focuses on identity security and privileged access management (PAM), but also offers solutions like insights that directly supports the requirements of Article 7, particularly in identifying and mitigating vulnerabilities associated with privileged access.

Vulnerability Identification & Enhanced Visibility for Risk Assessment

Identity Security Insights is designed to analyse and monitor identities, entitlements, and access privileges across an organisation's IT environment, which includes on-premises, cloud, SaaS, and IdPs. By identifying and documenting where privileges, entitlements, and paths to privilege exist, Identity Security Insights helps pinpoint vulnerabilities related to identity and access management that could potentially be exploited during an ICT disruption.

This solution provides comprehensive visibility into the identity landscape of an organisation, which is crucial for understanding the existing risks within ICT systems and the broader digital ecosystem. This visibility supports the effective assessment and management of those risks, aligning with the testing and mitigation requirements outlined in Article 7.

Secure Testing Environments

When external parties are involved in testing ICT systems, **Privileged Remote Access** can ensure that they have secure and controlled access, maintaining the integrity of the testing environment.

Password Safe can ensure that access to systems for testing purposes is secure and controlled. By managing privileged credentials, testers are provided only with the access necessary to perform their duties, minimising the risk of excessive access that could compromise security during testing phases.

Least Privilege Enforcement & Application Control

By enforcing least privilege and controlling application usage, BeyondTrust **Endpoint Privilege Management** reduces the risk of vulnerabilities being exploited. This is particularly important for ensuring that software used in financial systems is not susceptible to known vulnerabilities that could be exploited during testing.

Audit Trails & Reporting

All BeyondTrust solutions provide comprehensive audit trails and reporting capabilities, documenting all privileged sessions including those used for testing. This documentation is essential for post-test analysis, identifying areas for improvement, and proving compliance with DORA's requirements.

Article 8: Identification

This Article emphasises the need for financial institutions to have robust mechanisms in place for the identification of information and communication technology (ICT) risks that could potentially impact their operations. This includes the identification of threats and vulnerabilities that exist within their ICT systems and the broader digital ecosystem they operate in.

The core objective is to ensure that financial entities can preemptively recognise and assess the risks to their digital operations and take appropriate measures to mitigate before they materialise into significant disruptions.

How BeyondTrust Enables Your Compliance with Article 8

Risk Identification & Behavioral Analytics

Identity Security Insights analyses user behaviors and access patterns to identify anomalies that may indicate potential security risks or vulnerabilities. This proactive approach to detecting unusual activities, especially around privileged accounts, aligns with the Article 8 requirement for financial entities to have robust mechanisms in place for the identification of ICT risks.

Identifying Risks in Remote Access Points

Privileged Remote Access provides secure, controlled access to internal networks and systems for remote employees and third-party vendors. By monitoring and auditing remote access sessions, BeyondTrust helps identify potential security risks, such as unauthorised access or risky user behaviors that could compromise ICT systems.

Password Safe enables organisations to centralise the management of privileged credentials, significantly reducing the risk of unauthorised access or breaches. By securing privileged accounts, financial institutions can better identify areas where privileged access could be exploited by malicious actors, thus addressing a key aspect of ICT risk.

Vulnerability Identification & Least Privilege Enforcement

By enforcing least privilege on endpoints and allowing elevated privileges only when necessary, **Endpoint Privilege Management** minimises the attack surface. This approach aids in identifying software vulnerabilities and misconfigurations that could be exploited by malicious actors, thereby enhancing the overall resilience of ICT systems. Moreover, asserting maximal control over privileges across endpoints prevents the lateral movement and spread of malware, ransomware, and other threats.

Article 9: Protection & Prevention

Article 9 of DORA emphasises the necessity for financial entities to establish robust measures for the protection and prevention of ICT-related incidents.

Notably, this section mandates the implementation of technical and organisational measures to safeguard against potential ICT risks that could affect the integrity, availability, and confidentiality of systems and data. The focus is on ensuring that financial institutions have effective defenses in place to prevent cyber threats, data breaches, and system failures, thereby maintaining operational resilience.

How BeyondTrust Enables Your Compliance with Article 9

Controlled & Secure Remote Access

Privileged Remote Access facilitates secure and controlled access to the institution's network and systems for both internal and external users. By implementing strict access controls and monitoring remote connections, Privileged Remote Access helps prevent unauthorised access and data breaches, directly supporting the protection and prevention requirements of Article 9.

Privileged Remote Access also provides detailed monitoring and logging of all remote access sessions, ensuring that any suspicious activity can be quickly identified and addressed. This capability is crucial for the early detection and prevention of potential ICT incidents.

Privileged Access Security

Password Safe secures, manages, and monitors privileged account credentials, preventing unauthorised access to critical systems. By ensuring that privileged accounts are only accessible to authorised users under strict conditions, Password Safe helps mitigate the risk of security breaches, a key aspect of protection and prevention under Article 9.

Password Safe automates the rotation and management of passwords, reducing the risk of credential theft or misuse. This automation supports compliance by enforcing strong password policies and minimising the attack surface for cyber threats.

Least Privilege Enforcement & Application Control

This solution enforces the principle of least privilege across endpoints, ensuring that users have only the access necessary to perform their job functions. By minimising privileges, **Endpoint Privilege Management** significantly reduces the risk of malware propagation and data breaches, aligning with the preventative measures required by Article 9.

In addition, Endpoint Privilege Management allows organisations to control application usage, preventing the execution of unauthorised or malicious software. This capability is essential for protecting against software vulnerabilities and external attacks, further supporting the requirements of Article 9.

Identity Security Insights helps achieve identity hygiene and security posture by providing comprehensive “threat-aware” visibility into identities, privileges, identity misconfigurations, and risks across your identity infrastructure on-premises, clouds, SaaS, and IdPs. Built-in privileged access management controls further reduce the attack surface created by excessive and unnecessary privileges by allowing you to limit access, enforce policies, and right size privileges.

Article 10: Detection

Article 10 underscores the importance of the detection phase within ICT risk management, emphasising that financial entities must have effective systems and procedures in place to detect ICT-related incidents promptly.

This includes the ability to identify potential threats and vulnerabilities early to prevent or minimise the impact of such incidents on the entity's operational capabilities. The article highlights the need for continuous monitoring and detection mechanisms that can swiftly identify unusual activities that may signify a cyber threat, breach, or failure in ICT systems.

How BeyondTrust Enables Your Compliance with Article 10

Identity Security Insights, designed to detect and provide centralised real-time data into all identities, accounts, entitlements, and privileged access operating across your enterprise environment, is a crucial tool for organisations seeking to earn the capabilities outlined within Article 10's requirements.

Identity Security Insights uses artificial intelligence and machine learning (AI/ML) to continuously analyse and monitor vast amounts of data about user behavior, access patterns, common attacker tactics and techniques, indicators of compromise, and anomalies to automatically detect threats driven by the abuse of identities, privileges, and identity infrastructures. When new attack methods emerge, Identity Security Insights AI/ML models automatically adapt to detect modern attacks.

Advanced Threat Detection Capabilities

Identity Security Insights leverages advanced analytics to monitor and analyse user behavior continuously. By establishing normal usage patterns and detecting deviations, it can identify potential security threats early, enabling quick response to prevent breaches. This capability aligns with Article 10's requirements for Effective Detection Systems.

Proactive Vulnerability Identification

Identity Security Insights assesses and scores the risks associated with user behaviors and access patterns, helping organisations prioritise their response to the most critical threats. This proactive approach to identifying vulnerabilities before they are exploited is essential for complying with the detection mandates of DORA.

Enhanced Visibility Across Digital Assets & Identities

BeyondTrust solutions provide a panoramic view of the entity's digital environment, including who has access to what resources and how they are being used. This visibility is crucial for detecting unauthorised access attempts, insider threats, or misuse of privileges, directly supporting the detection strategies required by Article 10.

Article 11: Response & Recovery

Article 11, "*Response and Recovery,*" requires financial institutions to establish, implement, and maintain plans and procedures to effectively respond to ICT-related incidents and recover operations.

This includes the capability to quickly assess the impact of incidents, contain and mitigate their effects, and restore normal operations while minimising disruption to services. The article emphasises the need for resilience in the face of incidents that could threaten the integrity, availability, and confidentiality of data and systems.

How BeyondTrust Enables Your Compliance with Article 11

Facilitating Swift Incident Response

Privileged Remote Access enables secure and controlled access to the institution's network and systems for both internal response teams and external support if necessary. This capability is crucial for ensuring that the right personnel can quickly respond to an incident, regardless of their physical location, thereby minimising the time to containment and mitigation.

Identity Security Insights helps streamline incident response workflows and reduce response time by directly sending detections and recommendations to your preferred tools via SIEM, SOAR, and webhook integrations. It is also natively integrated with BeyondTrust PAM tools, allowing organisations to take actions to remediate problems, block access, and implement stronger policies and controls for least privileged access.

Endpoint Privilege Management, particularly for Linux servers, plays a crucial role in complying with this directive. Ensuring that all users operate under the principle of least privilege by default reduces the risk of a security breach, limiting user access to essential tools and commands necessary for their roles. In the context of incident response, this means that if a breach occurs, the potential damage is contained because malicious actors or compromised accounts have limited access to critical system resources.

During an incident, response teams often require elevated privileges to access systems and perform necessary remediation tasks. Endpoint Privilege Management allows for controlled, on-demand elevation of user privileges. Administrators can grant temporary and time-bound access to additional resources as needed, which is essential for swift incident management and system recovery.

Isolating Affected Systems

In the event of an incident, **Privileged Remote Access** can be used to isolate affected systems to prevent further spread of the issue. This isolation is key to effective incident containment strategies.

Secure Access for Recovery Operations

Password Safe ensures that access to critical systems during the recovery phase is securely managed. By controlling and auditing access to privileged accounts, Password Safe ensures recovery efforts are not hampered by unauthorised access or further security breaches.

Automated Credential Rotation

After an incident, it's often necessary to rotate credentials as a security measure. Password Safe automates this process, quickly re-securing access points and helping to restore the integrity of access controls as part of the recovery process.

Article 16: Simplified ICT Risk Management Framework

Article 16 introduces the concept of a "Simplified ICT Risk Management Framework" tailored for smaller financial entities or those with lower risk profiles.

Recognising that one size does not fit all, this provision allows for a more proportional approach to ICT risk management. It mandates that these entities still adhere to the principles of identifying, protecting against, detecting, responding to, and recovering from ICT-related incidents but in a manner that aligns with their size, complexity, and the nature of their ICT risks. The goal is to ensure that all financial entities, regardless of size, maintain operational resilience while minimizing the impact of regulatory compliance.

How BeyondTrust Enables Your Compliance with Article 16

Proportional Risk Identification & Management with Tailored Insights

Identity Security Insights provides tailored visibility into the risks associated with user identities and access within the organisation's ICT systems. This solution can scale according to the size and complexity of the entity, supporting a simplified framework by focusing on the most relevant identity and access management risks.

Adaptive Security Posture with Customisable Monitoring & Alerts

Identity Security Insights also allows for the customisation of monitoring and alerting based on the entity's specific risk profile and regulatory requirements. Smaller institutions can focus on critical assets and user activities, ensuring compliance without the overhead of managing an overly complex monitoring system.

Efficient Compliance Reporting with Streamlined Reporting

Identity Security Insights facilitates efficient compliance reporting by generating concise, relevant reports that demonstrate adherence to the simplified ICT risk management framework. This capability is particularly beneficial for smaller entities that may lack extensive compliance resources.

For entities applying a simplified framework, understanding the specific risks associated with privileged access and user identities is crucial. Identity Security Insights can highlight areas of potential vulnerability, enabling focused and effective risk mitigation strategies that are proportionate to the entity's operational context.

Support for Proportional Response & Recovery Strategies

By providing insights into the identity and access dimensions of ICT incidents, Identity Security Insights supports the development of response and recovery strategies that are tailored to the scale and needs of the entity. This ensures that smaller entities can efficiently manage incidents without the need for a complex response infrastructure.

>>> Conclusion: BeyondTrust Solutions can be Used to Support Key DORA Requirements

Why Partner with BeyondTrust to Meet DORA Requirements?

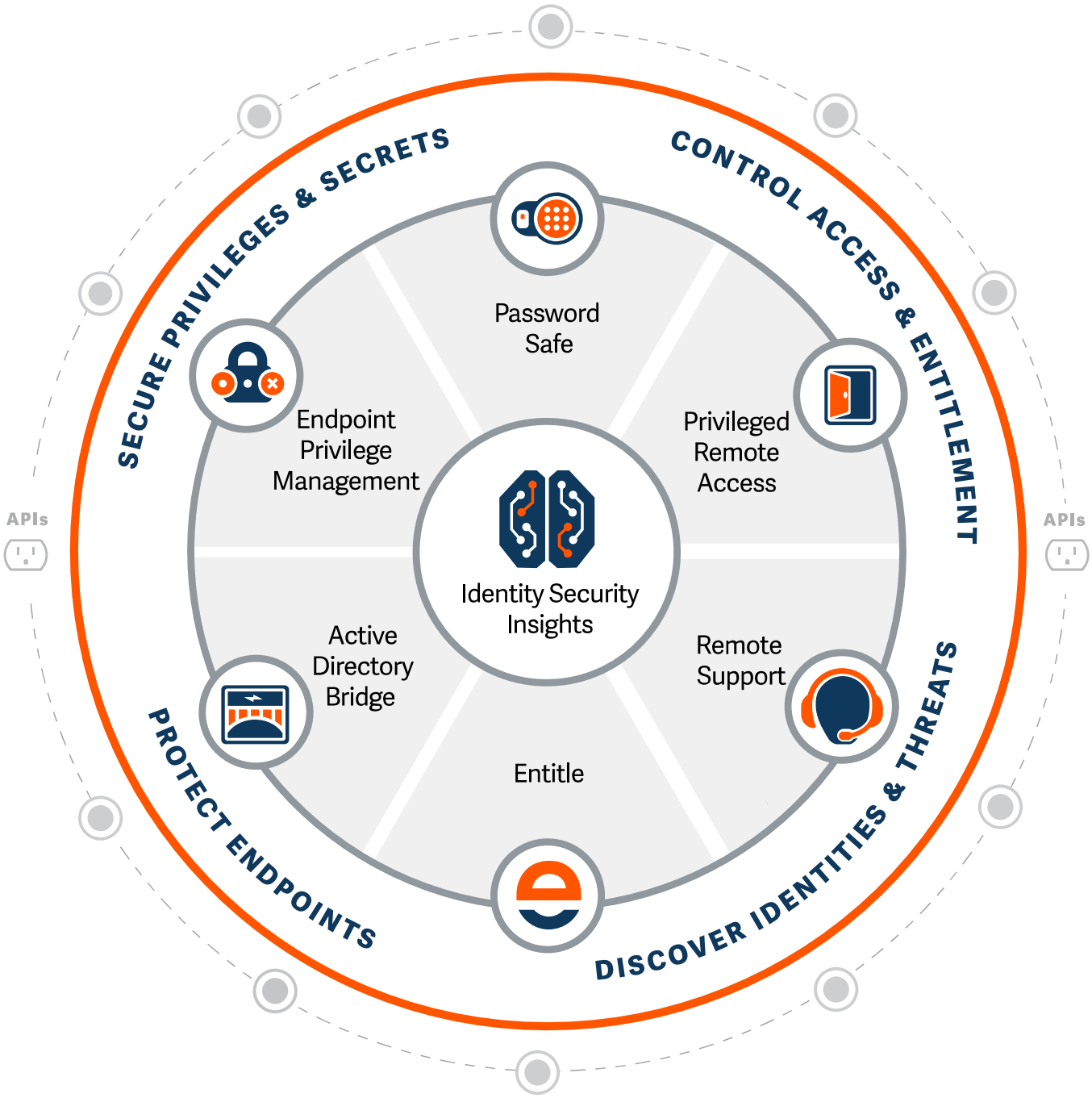
Here are the facts:

- BeyondTrust addresses major identity security and privileged access management (PAM) use cases. Our comprehensive solutions include substantive capabilities no other vendor delivers.
- Our next-generation capabilities extend your line-of-sight to privileged threat pathways and identity-based attack chains far beyond the capabilities offered by other solutions on the market.
- The breadth of our solutions and the flexibility of our offerings enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- You can choose from the deployment model that best suits your needs. No other identity security or privileged access management (PAM) vendor provides more choices.

Ready for the Next Step?

Contact our team of experts to learn more about BeyondTrust identity security and PAM solutions. Get started today with complimentary demos, free trials, and more. **Contact Us**

The BeyondTrust Platform



Identity Security Insights

Proactively strengthen your identity security posture and build resilience against threats by uncovering identity vulnerabilities and hidden paths to privilege.

Privileged Remote Access

Create identity-secure, just-in-time access to all your enterprise environments: cloud, on-premises, and OT.

Endpoint Privilege Management

Enforce least privilege dynamically to prevent malware, ransomware, and identity-based attacks, achieve compliance across Windows, macOS, and Linux endpoints, and enable your zero trust strategy — without compromising on productivity.

Password Safe

Manage privileged passwords, accounts, credentials, secrets, and sessions for people and machines, and secure non-privileged employee passwords for business applications

>>> About BeyondTrust

BeyondTrust is the global cybersecurity leader protecting your Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**