WHITEPAPER

Securing Privileged Access & Remote Access for Government In Australia & New Zealand

Addressing the challenges faced by government departments and agencies associated with managing and auditing privileged access and securing remote access, including recommendations from experts, including the Australian Cyber Security Centre and CERT NZ

BeyondTrust

Table of Contents

Secure Your Entire Privilege Universe with BeyondTrust

With over 20,000 worldwide customers, including thousands across the Public Sector, BeyondTrust delivers a comprehensive, integrated suite of privileged access management (PAM) solutions that have been proven in a wide range of IT environments.
In both 2018 and 2019, Gartner recognised privileged account management as the #1 IT security project based on its ability to have a big impact in terms of both reducing risk and enabling the enterprise.

BeyondTrust addresses the broadest swathe of privileged access use cases. BeyondTrust solutions help enable our public sector customers to:

- ✓ Massively reduce the threat surface and reduce security and data breach risk by securing privileged access, managing remote access, and enforcing least privilege access on any network enabled device.
- ✓ Address federal, state, local, and industry compliance initiatives with security controls, threat analytics, and reporting
- ✓ Securely and confidently embrace new technologies (cloud, IoT, robotic process automation)

This white paper provides an overview of how BeyondTrust solutions help Australian and New Zealand government at all levels and their staff comply with a slew of regulations.

Cybersecurity Initiatives Addressed by BeyondTrust

Essential 8
A baseline set of strategies developed by the Australian Cyber Security Centre (ACSC) to mitigate cybersecurity risks, implementing the Essential 8 makes it harder for criminals and adversaries to compromise systems.

Information Security Manual
The Australian Government Information Security Manual is a risk management framework developed by the Australian Cyber Security Centre. Where applied, its purpose is to assist organisations to protect their systems and data from cyber threats.

CERT NZ's Critical Controls 2021
Each year CERT NZ publishes a list of controls designed to mitigate the risks of the majority of the security incidents that the body has seen in the previous year through reports it has received along with international threat feeds.

State-based Cyber Security Policies
Australian state governments are increasingly developing policies that apply not only to state government departments and agencies but are highly recommended for local government as well. These policies often include elements based on international standards such as ISO27001.

ISO27001
Does not formally mandate specific controls. However, the standard provides a long list of extended control sets from which organisations may choose to meet their specific risk management policies.

NIST Framework
The NIST framework is utilised by other organisations in developing their recommendations and best practices, including the ACSC. Address important security and risk management controls of NIST CSIP and the NIST Cybersecurity Framework.

On the whitepapers section of our website, you can find more detailed information on how we address and map to other compliance initiatives and frameworks, including GDPR, PCI DSS, HIPAA, and SWIFT, to name just a few.

Government Organisations Must be Vigilant and Proactive

The compliance landscape for government at all levels is constantly evolving to keep pace with new threats to public sector systems and new technologies being deployed. There are always emerging requirements that departments and agencies must anticipate, implement, and report on, or be potentially subject to penalties—or worse—security and data breaches.

Government information networks – like their counterparts in public and private enterprises – are constantly vulnerable to both internal and external threats:

- **Internal threats** may be malicious (designed to cause harm) or unintentional (the result of human error), exposing weaknesses in the agency's defenses and policies. Regardless of intent, insiders can wreak significant damage quickly—they have the know-how, and, all too often, they have the access and privileges.

- **External threats** typically exploit credential flaws (embedded/default passwords, configuration errors, faulty code, reused or guessable passwords, weak 2FA or MFA, etc.) in networks and endpoints—often through remote access pathways. Threat actors seek to gain a foothold where they can act as an insider. They then cement their presence and skulk laterally throughout the IT environment—exploring opportunities to escalate their privileges, snag additional credentials, and exercise control over more assets and data.

The collateral damage of such attacks can range from "simple" non-compliance consequences to loss of intellectual property, personnel records, or personally identifiable information of citizens that can easily be sold on the dark web for profit. BeyondTrust provides solutions that can protect against external and internal threats, whether inadvertent or malicious in intent.

Privileges and remote access pathways represent two of the most common and dangerous cyberthreat vectors. Let's take a brief a look at these attack vectors and how BeyondTrust solutions address them.

1. Privileged Threat Vectors

According to Forrester Research, the misuse or abuse of privileged credentials and access is implicated in roughly 80% of IT security breaches today—and it's no surprise why. Today, privileges are built into operating systems, file systems, applications, databases, hypervisors, cloud management platforms, DevOps tools, robotic automation processes,

and more. Simply put, too many people, systems, and applications have far too many privileges. And attackers routinely exploit this tantalising attack surface.

Cybercriminals covet privileges/privileged access because it can expedite access to an organisation's most sensitive targets. With privileged credentials and access in their clutches, a cyberattacker or piece of malware essentially becomes an "insider".

As the 2021 Microsoft Vulnerabilities Report revealed, **100% of all Critical vulnerabilities in Microsoft Outlook products would have been mitigated by removing admin rights from users, while more than half of critical vulnerabilities in Windows (109 of 196) would have been mitigated through the removal of user admin rights.** That data alone makes a compelling case for enforcing least privilege and application control, such as via an endpoint privilege management solution. With a least-privilege approach, users receive permissions only to the systems, applications, and data they need based on their current role or profile in the organisation. These privileges can be user, system, or role-based as well as time-based (e.g., access granted only for certain days or hours, or for a set duration of time).

All privileged activity should be monitored and audited to ensure appropriate use, and to quickly identify, flag, and prevent misuse. By monitoring privileged users with BeyondTrust privileged access management solutions, which enable proactive alerts and reporting, you can achieve "verifiable compliance" with stated access policies – and gain assurance that your security solution can pass any audit.

2. Securing Remote Access Pathways

Commenting on the rise in remote access during and after the COVID-19 pandemic, Sean Kelley, former CISO of the U.S. Environmental Protection Agency summed up, "Where you might have had 20, 30, 50% of your workforce connecting to the VPN at any time, now you have 80-to-100% of the workforce – employees and third-party vendors - connecting via VPN all the time. And a lot of CIOs just didn't plan for that, because that's just not the scenario that we lived in before this week."

With so many remote access points, and often, sub-optimal visibility, auditing, and security controls over this access, it's only a matter of time before a remote access weak link is compromised—either via an employee or a third-party vendor. Remote access pathways represent those weakest links for most organisations—and cybercriminals know it. Examples of high-profile attacks that used this vector include the May 2021 attack on Colonial Pipeline that came via a legacy VPN with a set of credentials that should not have been active, while the 2013 Target POS terminal malware attack was initiated via systems access given to a HVAC supplier.

SLAs can help keep your vendor security on the right track, but how do you trust that your vendors are following the right security practices? What can you do to protect your

organisation if they aren't? Many government organisations rely on VPNs for third-party access, but VPNs provide far too much access.

Most security vendors providing remote access:

- Do not offer granular access control settings
- Do not provide a comprehensive audit trail
- Do not support all operating systems and scenarios, and thus require the use of multiple products

BeyondTrust can securely address the broadest range of remote access use cases—from remote support to vendor and remote worker access. Our solutions can provide fine-grained access controls, auditing all privileged activities, and can work across an expansive range of systems and use cases. This also means you can consolidate your various remote tools into one solution, saving on admin costs, while also improving security by blacklisting other remote access tools, which are often planted on computers as part of an attack.

Bringing it All Together – Enabling Security for Government

Reviewed, Tested, Trusted

Gartner, Forrester, and KuppingerCole have each recognised BeyondTrust as a Privileged Access Management Leader in their most recent industry reports.

The BeyondTrust Privileged Access Management Platform was also named the top 2019 Privileged Access Management Solution in the "ASTORS' Homeland Security Awards. American Security Today's Annual 'ASTORS' Awards program is the largest and most comprehensive in the industry, highlighting the most cutting-edge and forward-thinking security solutions in the market today. According to American Security Today, "BeyondTrust's unified solutions offer the industry's broadest set of privileged access management capabilities with a flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments."

Additionally, BeyondTrust was named a Gold winner in the 2018 Government Security News Homeland Security Awards for "Best Identity Management Platform".

Third-Party Integrations

BeyondTrust's solutions and platform are also elegantly designed to make integrations with important third-party tools as seamless and synergistic as possible. We are proud to have been recognised by McAfee as their Security Innovation Alliance (SIA) partner of the year for two consecutive years (2017 & 2018), selected from 150 SIA partners. We have certified integrations for BeyondTrust Password Safe and Endpoint Privilege Management with McAfee solutions to enable organisations to better control risk and eliminate threats.

Our System for Cross-domain Identity Management (SCIM) integration with SailPoint enables organisations to effectively manage user access for both privileged and non-privileged accounts. IT organisations benefit from full visibility into, not only role assignments and user access, but also all users and ongoing role changes. When changing roles, adding and removing access is provided to ensure the right person has the right access at all times to increase security and reduce risks.

You can learn more about our rich technology partner ecosystem that includes ServiceNow, Okta, FireEye, Palo Alto Networks, and others on our Partners page.

Core Capabilities of BeyondTrust Solutions

- ✓ **Discover, onboard, and securely manage privileged credentials**—for human and non-human accounts across diverse IT environments. This includes privileged account passwords, application/embedded passwords, SSH keys, DevOps secrets, service accounts, and more
- ✓ **Manage and monitor all privileged sessions** (including pausing and/or terminating suspicious sessions in real-time), and audit and report on all privileged activities—even those for third-party (vendor) access.
- ✓ **Control privilege elevation and delegation, and enforce least privilege** across all endpoints (Windows, Mac, Unix, Linux), network devices, etc. For instance, you can (and should) remove all local admin privileges from most non-IT users and eliminate root and superuser access wherever possible. BeyondTrust enables you to elevate application access—without elevating the user.
- ✓ **Seamless Application Control**: Deliver trust-based application whitelisting with a flexible policy engine to set broad rules. Tailored options enable organisations to choose automatic approval for advanced users – protected by full audit trails – or utilise challenge-response codes.
- ✓ **Enforce just-in-time access:** This ensures privileged accounts are not always sitting in a privilege-active state, thereby dramatically reducing the threat window. With BeyondTrust solutions, you can approach a state of zero standing privileges.
- ✓ **Securely address the broadest range of secure remote access** use cases. From providing industry leading remote support solutions that are a fixture of IT service management and internal help desks, to securing remote access for vendors and remote workers. No other IT security vendor can help you address secure remote access in all its forms as holistically as can BeyondTrust.
- ✓ **Extend privilege management best practices** to vendors and remote employees.
- ✓ **Consistently authenticate users across heterogeneous environments** by extending AD's Kerberos authentication and single sign-on capabilities across platforms (Windows, Mac, Unix, Linux, etc.).
- ✓ **Make better privilege decisions with vulnerability insights:** Leverage patented technology to automatically scan applications for vulnerabilities at runtime, enabling IT and security teams to enforce quarantine, reduce application privileges, or prevent the launch of an application.

- ✓ **Deep reporting and threat analytics:** Delivers deep analytics and reporting to multiple stakeholders, ensuring that all teams have the information and views they need to effectively manage application and asset risk, and prove compliance.
- ✓ **Leverage partner integrations to realise risk management synergies and richer reporting**: Gain a holistic view of enterprise-wide security, including risk from users, accounts and their privileges, and other security solutions, such as SIEMs and firewalls.

Key Benefits of BeyondTrust PAM Solutions for the Public Sector

- Mitigate both external threats (malware, hacker, etc.) and insider threats
- Pass audits, comply with government and industry mandates, and fulfill reporting requirements via privileged access certification reporting
- Ensure accountability through session monitoring and recording, keystroke logging, and real-time auditing
- Stay protected across your entire IT environment—on-premise, cloud, hybrid, DevOps infrastructures; we can also help secure your workloads and containers
- Enable informed, actionable IT risk management decisions from meaningful data gleaned from context-aware security intelligence, including asset, user, and account privilege information

Compliance: How BeyondTrust Holistically Mitigates Risk

BeyondTrust provides important capabilities that support a wide range of government information security requirements. Here we have broken down some of the most common and pressing mandates and regulations, showing the extent to which BeyondTrust's PAM solutions can help government at all levels achieve and maintain compliance around managing, securing and auditing privileged access and remote access.

Essential Eight

Originally published in February 2010, the Australian Signals Directorate (ASD) developed a list of strategies to mitigate targeted cyber intrusions. In 2017, four additional recommendations were added, creating the Essential Eight.

The Strategies to Mitigate Cyber Security Incidents includes a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries.

This guidance promotes the adoption of sound security and operational practices for managing technology used within Australian Government Agencies. The mitigation

strategies can be customised based on each organisation's risk profile and the adversaries they are most concerned about.

The Essential Eight is used by many organisations in both the private and public sector, and a number of Australian state government security policies require adherence to it. BeyondTrust's solutions can help organisations to meet seven of the Essential Eight mitigation strategies, including all the Top 4:

- **Application Control** – Endpoint Privilege Management
- **Patch Applications –** Endpoint Privilege Management
- **Configure Microsoft Office Macro Settings –** Endpoint Privilege Management
- **User Application Hardening** – Endpoint Privilege Management
- **Restrict Administrative Access** – Endpoint Privilege Management
- **Patch Operating Systems** – Endpoint Privilege Management
- **Multi-Factor Authentication** – Password Safe
- **Daily Backups** – no solution

For further information read our whitepaper, Complying with the Australian Signals Directorate (ACSC) Mitigation Strategies.

Australian Government Information Security Manual

The Information Security Manual (ISM) assists cybersecurity leaders and professionals to protect their systems and data from threats by outlining a cybersecurity framework that can be applied against an organisation's risk management framework.

The ISM framework is broken down into cybersecurity principles and guidelines. The principles are strategic in their guidance and are grouped into four key activities: govern, protect, detect and respond. The guidelines provide more practical guidance and cover governance, physical security, personnel security, and information and communications technology security matters.

It is recommended that organisations should be able to demonstrate how they adhere to the principles while they can consider which guidelines are relevant to each of the systems they have in place.

One area in the extensive guidelines that BeyondTrust offers significant value to its customers is that of Guidelines for System Hardening. Within this section of the ISM controls the focus is user accounts and privileges, capabilities of users to modify security functionality or run scripts, privileged accounts, application control, running macros, single and multi-factor authentication, protecting, setting and resetting user credentials.

CERT NZ's Critical Controls 2021

Each year CERT NZ publishes a list of controls based on the security incidents that the body has seen in the previous year through reports it has received along with international threat feeds. As CERT NZ notes, "when correctly implemented, these controls would prevent, detect, or contain the majority of the attacks".

A number of the controls overlap the risk mitigation strategies contained in the Essential Eight. But as this is an annually updated list it helps organisations who want to mitigate risks and maximise their cybersecurity budgets based on the latest threat intelligence.

In 2021, CERT NZ added two new controls and to an existing list while splitting out another to create a list of ten.

Through BeyondTrust's solutions, organisations can gain coverage for half of the ten controls. They are:

- ✓ **Provide and use a Password Manager** – Password Safe
- ✓ **Implement Application Allowlisting** – Endpoint Privilege Management
- ✓ **Implement Multi-factor Authentication and Verification** – Password Safe
- ✓ **Enforce the Principle of Least Privilege** – Endpoint Privilege Management
- ✓ **Set Secure Defaults for Macros** – Endpoint Privilege Management

CERT NZ provides further detailed guidance on each of the ten controls on its website.

NIST

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Department of Commerce charged with advancing measurement standards. Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents.

The NIST Risk Management Framework (NIST RMF) is the standard for integrating information security and risk management into government agency information systems. The NIST RMF encompasses a range of activities defined by several different NIST SPs. BeyondTrust supports the requirements of four key SPs relating to the NIST RMF: SP 800-53, SP 800-171, SP 800-39, and SP 800-137.

NIST SP 800-53: Security and Privacy Controls for Federal Information Systems & Organisations & NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organisations

NIST SP 800-53 sets forth a comprehensive approach to information security and risk management by providing organisations with a broad set of security controls essential to strengthen their information systems and the environments in which they operate so that

they become more resilient in the face of cyberattacks. NIST SP 800-53 outlines a "Build It Right" strategy combined with various security controls for Continuous Monitoring, striving to provide senior leaders of organisations' information to support making risk-based decisions related to their critical missions.

NIST SP 800-171 is very similar to, and largely derived from, NIST SP 800-53. While SP 800-53 pertains to federal systems and organisations, SP 800-171 pertains to non-federal systems and organisations that may interface with federal systems. This regulation strives to put protections around the vast amount of federal information that is regularly stored, processed, and transmitted by nonfederal organisations, like contractors, state and local governments, universities, and research organisations. Often, this information is sensitive and, if compromised, would have a direct negative impact on the functioning of the federal government and an agency's ability to achieve their mission. Therefore, protecting that information, both inside and while outside of federal information systems, is critically important.

BeyondTrust's solutions address several individual controls under the following control families across both SP 800-53 and SP 800-171:

- ✓ **Access Control** – Endpoint Privilege Management, Secure Remote Access
- ✓ **Audit & Accountability** – Endpoint Privilege Management, Secure Remote Access
- ✓ **Security Assessment and Authorisation** – Endpoint Privilege Management
- ✓ **Configuration Management** – Endpoint Privilege Management
- ✓ **Identification and Authentication –** Password Safe
- ✓ **Risk Assessment** – Endpoint Privilege Management
- ✓ **System & Services Acquisition** – Endpoint Privilege Management
- ✓ **System and Communications Protection** – Endpoint Privilege Management, Secure Remote Access
- ✓ **System and Information Integrity** – Endpoint Privileged Management, Auditor

NIST SP 800-137: Information Security Continuous Monitoring (ISCM)

BeyondTrust offers several solutions that enable continuous monitoring, defined by 800-39 as part of the 11 security automation domains that support continuous monitoring. In particular, BeyondTrust provides capabilities around asset and credential inventorying.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a risk-based framework for critical infrastructure organisations to voluntarily manage their cybersecurity risks. This standard was to be based on industry best practices and international standards. The adoption of the framework has steadily increased since its initial release. The Cybersecurity Framework, developed in partnership between industry and government, was designed to provide a

universal standard, yet be flexible enough to address an organisation's unique risks and risk tolerance.

The Framework core is a set of desired actions, outcomes, and references across critical infrastructure sectors. This core consists of five functions: **Identify, Protect, Detect, Respond, and Recover**. BeyondTrust PAM solutions, along with the BeyondInsight platform's behavioral and threat analytics, address various controls across each of these five functions.

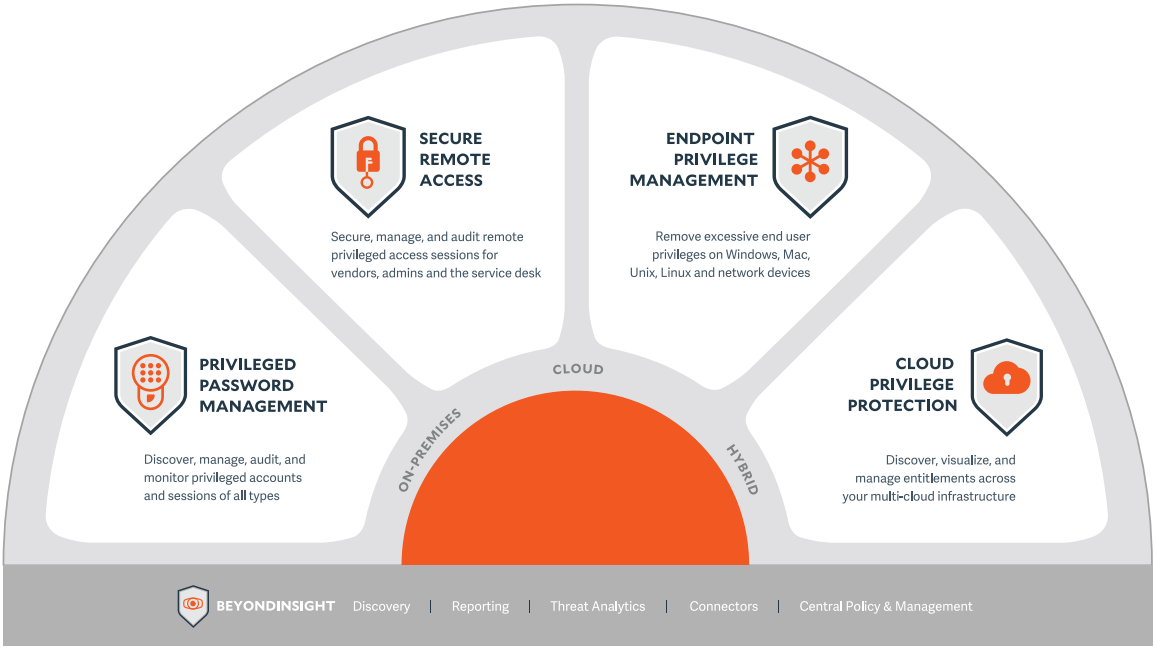
Overview of BeyondTrust Platform & Solutions

As government departments and agencies are under pressure to limit the number of discrete vendors, BeyondTrust can handle the bulk of your security initiatives around privileged and remote access—thereby helping reduce your vendor portfolio, while ensuring you have industry-leading solutions to protect against some of the most dangerous attack vectors.

Our ISO 27001 and SOC 2 Type 1 compliance demonstrates an ability to ensure customer data is safe from the most sophisticated methods of intrusion. The highly detailed validation process verifies the effectiveness of BeyondTrust's internal security operations, secure software development practices, and product capabilities.

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.

BeyondTrust Platform (BeyondInsight): BeyondInsight is the smart console shared across BeyondTrust Privileged Access Management solutions, providing centralised management and policy control. BeyondInsight provides integrated capabilities such as asset discovery, profiling, smart groups, threat analytics, reporting, and connectors to third-party systems.



BeyondTrust Privileged Password Management solutions enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities. Security teams can instantly view any active privileged session, and if required, pause or terminate it. Leverage threat analytics that aggregate user and asset data to baseline and track behaviour and alert on critical risks. Video recording, keystroke indexing, full text search, and other capabilities make it easy to pinpoint data. Reduce the risk of compromised privileged credentials for both human and non-human accounts while meeting compliance requirements.

BeyondTrust Endpoint Privilege Management combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices—without hindering productivity. Elevate applications securely and flexibly with a powerful rules engine and comprehensive exception handling. Centralised auditing and reporting simplify the path to compliance. Enforce least privilege and eliminate local admin rights with fine-grained control that scales to secure your expanding universe of privileges, while creating a frictionless user experience.

BeyondTrust Secure Remote Access solutions enable organisations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks. Users can quickly and securely access any remote system, running any platform, located anywhere, and leverage the integrated password vault to discover, onboard, and manage privileged credentials. Gain absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and create a complete, unimpeachable audit trail that simplifies your path to compliance.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organisations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organisations 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 organisations 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.