WHITEPAPER

Mapping BeyondTrust PAM Solutions to UK Critical National Infrastructure

A Controls-based Approach Using Privileged Access Management

BeyondTrust

CONTENTS

Introduction

On 10th May 2018, somewhat overshadowed by GDPR, the NIS Directive came into force. The NIS Directive is based on the EU Directive on the Security of Network and Information Systems (Directive (EU) 2016/1148) which seeks to deliver a common level of network and information systems security across the EU, focused on systems supporting critical national infrastructure (CNI), i.e., essential services such as the supply of electricity, gas, and water, healthcare, and passenger and freight transport.

Any cyber-attack, however successful, could cause significant damage to the UK's infrastructure and economy, and result in substantial financial losses. It's clear that attacks are on the increase and that infrastructure is being targeted. We only have to look back at the attacks in recent years targeting electricity networks (Ukraine 2015), water supply (USA 2016), and utility control rooms (USA 2018). Further, CNI has historically lagged in IT security as was demonstrated in the WannaCry outbreak in 2017 which caused significant impact to the UK National Health Service (NHS); the result of patches not being applied in a timely manner.

Like many industries, CNI have focused primarily on their delivery of services, with IT security an afterthought. The NIS directive is intended to remedy this situation by laying out a standards-based approach to managing and securing the CNI behind these services. The National Cyber Security Centre (NCSC), the organisation behind the UK implementation of the Directive, have provided guidance on how to comply; that guidance is based on international standards such as ISO/IEC 27002:2013 (Code of Practice), ISO/IEC 27001:2013 (Information Security Management System), ISO/IEC 27035:2016 (Information Security Incident Management), and ISO 22301:2012 (Business Continuity Management System).

While much of the NIS Directive is focused on best practices, there is little direct technical guidance on how to address the requirements. It's great that we are free to approach these requirements with the tactics and technologies that work best for our environment, but many organisations struggle to map this path for themselves. This is where it's vitally important to engage with great partners who are experts in cyber security, and who are able to apply their experience to your environment. This paper will focus on the proven controls necessary to ensure the infrastructure is secure.

Three Pillars to Ensure Effective Controls

A strong foundation for cyber security is based on proven controls. Specifically, controlling access into your systems, monitoring activity when that access is being used, and providing audit data for analysis after the access has completed. The three pillars (or key technologies) that make up this foundation are:

1. **Comprehensive identity management**
    a. Providing a single source of truth for who should and shouldn't have access to your systems.
    b. Enabling one set of credentials (username and password) for users across all systems; this also helps users remember their password as they only have one.
    c. Securing multi-factor authentication (MFA) to guarantee the user is who they say they are.

2. **Privileged account and session management:** Controlling access to the shared privileged accounts in the environment, i.e. Windows Administrator, Unix/Linux root, appliance admin accounts, etc., and monitoring their usage.

3. **Privilege elevation and delegation management:** A security approach that operates on explicit, fine-grained privilege assignment for users rather than trying to restrict the implicit privileges of the superuser accounts in the system. This allows the application of the Principle of Least Privilege (PoLP), ensuring users and processes have the minimal level of access necessary for them to perform their routine tasks.

These pillars help build a base that, not only secures your environment at a fundamental level and provides a stable base on which to build, but also deliver a simpler security model by being explicit as to where, when, how, and to whom access is granted. This has the additional benefit of reducing the amount of noise there is in your monitoring and forensic systems.

Much of what we do in monitoring our environments is focused on ensuring that users aren't misusing the privileges they have been granted. In this explicit model of security, users can only do the things they should be able to so there is less need to monitor these legitimate activities resulting in far fewer 'noise' events being generated. This delivers extra value from monitoring tools which are more easily able to identify malicious activity.

You may be reading this and thinking that it's not relevant as your business isn't part of the CNI. While the Directive may not apply to you directly, it and many other regulatory compliance regimes provide a valuable reference for best practices that can help any

organisation better secure their environment, delivering dividends for your business by giving you a head start. Let's look at each of the pillars in more detail.

Identity Management (NIS Directive Principles – B.2, B.3, B.4)

Controlling who has access to your systems and applications is critical regardless of the level of that access. Some essential approaches to user identity include the following:

Single Identity Across the Environment

Directory services, such as Microsoft Active Directory (AD), allow you to have a resilient, reliable mechanism to provide base authentication for users in one place. Additional solutions like Active Directory Bridge enable you to then extend the control and management of AD into Unix and Linux-based systems, thereby eliminating the need for additional directories or local accounts. The fewer usernames and passwords users have, the more likely it is they can use a complex password without forgetting it or needing to write it down.

Single Source of Truth

Identity and Access Management (IAM) solutions go a step further in providing a mechanism to reliably assign roles and responsibilities to users with attestation and auditing to ensure that what's assigned is what was provisioned. Solutions from companies like SailPoint deliver enterprise-grade identity governance capabilities ensuring you know who, what and why an identity can access critical data or systems.

Multi-Factor Authentication

Authentication can be broken down into three basic elements: Something you know, something you have, and something you are. Most systems and applications rely on something you know, i.e., your password. This is rarely sufficient in today's hyper-connected world where users are regularly using the same password in multiple places (Yes, even their work account password gets reused!).

Increasingly, we are seeing the adoption of a second authentication factor, either something you have (i.e. an app which generates predictable, secure tokens or delivers out-of- band verification of possession of a device), or something you are (i.e. biometric validation through iris, fingerprint, or facial recognition). There are many vendors of these solutions and it's recommended that at least two factors are employed with more for particularly sensitive and/or privileged system access.

Privileged Account and Session Management (NIS Directive Principles – B.2, B.3, B.4)

Access to privileged accounts in the environment is unavoidable; however, we can make sure that access to those accounts is under tight control by implementing privileged account and session management. Solutions in this space, like Password Safe, provide mechanisms to manage privileged accounts across operating systems, applications, network infrastructure, and appliances (including IoT). This includes:

- Password management – Restricting access to the password, applying workflow rules for check in/checkout, and enforcing strong password criteria.
- Session monitoring and management – Providing managed access to systems without revealing the password, utilising the four-eyes principle, recording the session (including keystrokes, mouse movements, and button clicks), and providing playback for auditing and forensics purposes.

Hackers will target all privileged accounts in a system to allow them to move laterally through your environment looking for valuable data. A privileged account and session management solution can effectively stop the hackers in their tracks limiting the impact of any malicious activity.

Privilege Elevation and Delegation Management (NIS Directive Principles – B.2, B.3, B.4)

A common risk scenario within many organisations is the preponderance of over-privileged users. Ideally, users would only have the privilege level necessary for them to be productive in their jobs. This is commonly referred to as the principle of least privilege, but most operating systems don't provide the capabilities for this – meaning the user who needs to install Adobe Acrobat is granted full local administrator privileges to their workstation, often without a clear timeframe for revocation.

Using privilege elevation and delegation management solutions such as Endpoint Privilege Management it's possible to allow the user to have the specific privileges they need, i.e. the ability to install a particular application or run a specific application in a privileged state, without exposing the system to the full risk of a privileged account. This kind of capability not only allows users to have seemingly more permissions on their system while reducing the actual risk level, but also eliminates the need to monitor what they are using privileged accounts for, thereby limiting the amount of monitoring 'noise' in the system.

This ability to say "Yes" to user requests for permissions more often also helps build a better relationship with the cyber security team, enabling better user engagement in securing the environment – something essential for successful security projects.

Summary

The NIS Directive, like many compliance regimes, focuses on best practice processes and procedures that help you deliver a more secure, reliable, and resilient environment. Using technologies like identity and access management and privileged access management to build a solid cyber security foundation will help in meeting compliance requirements, while enabling productivity.

Appendix – The BeyondTrust Privileged Access Management Platform

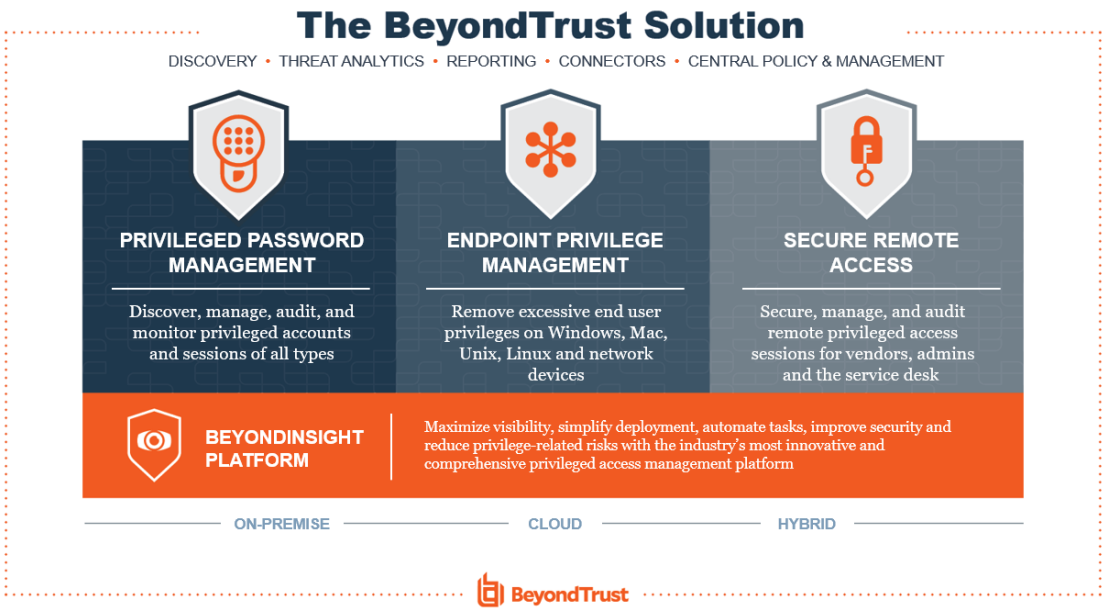
The BeyondTrust Privileged Access Management platform is an integrated solution to provide control and visibility over all privileged accounts and users across all enterprise platforms. By uniting best of breed capabilities that many alternative providers offer as disjointed tools, the BeyondTrust Privileged Access Management platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks. (see platform diagram on next page).

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. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

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'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.

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 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.