BeyondTrust

Stop hackers in their tracks with BeyondTrust privileged account and session management solutions

Address the NIS2 Directive *with* Privileged Access Management

TABLE OF CONTENTS

Introduction

The Network and Information Security (NIS) Directive, created in 2016, was the first EU-wide cybersecurity law. Its objective was to achieve a higher and more uniform level of security for network and information systems throughout the EU (European Union).

Given the considerable acceleration in digital transformation and evolution of threat vectors since then, the Directive was refreshed. NIS2 was formally adopted in November 2022 and entered into force in January 2023.

NIS2 repeals and replaces the former version of the Directive. It represents a constructive step forward in defining the requirements for EU organizations to enhance their cyber-resilience over the coming years. NIS2 also clearly details reporting rules and the repercussions for ignoring them.

NIS2 also strives to further strengthen cooperation within the EU. This includes establishing the European Network of Cyber Crisis Liaison Organizations (EU-CyCLONe) to support coordinated management of large-scale cybersecurity incidents at the EU level.

What Changes with NIS2?

Key changes under NIS2 include:

- A wider range of industry sectors.
- More rigorous incident response and crisis management reporting.
- Enhanced security requirements and controls.
- Supply chain security, meaning not only the organization, but their service providers and subcontractors as well.
- Incorporating basic IT hygiene best practices and cybersecurity training.

In view of NIS2, many organizations will have to reprioritize their budgets to urgently address this directive. Failure to comply with the new measures may result in fines of up to 2% of the company's global turnover.

You may be reading this and thinking that it's not relevant because your business isn't located in the EU. NIS2 applies to any business providing services within the EU, regardless of location. In addition, NIS was originally focused on systems supporting critical national infrastructure (CNI). NIS2 has significantly broadened the range of industry sectors that fall under the Directive.

Even if none of these factors apply to your company, the Directive, and many other regulatory compliance regimes, provide a valuable reference for best practices that can help any organization secure their environment better.

Read on to understand how BeyondTrust can help you address the following key sections of the NIS2 Directive:

- Cloud Security Management (paragraphs 33, 34, 35)
- Privileged Account and Session Management (paragraph 44)
- Privilege Elevation and Delegation Management (paragraphs 44, 49)
- Ransomware Protection (paragraph 54)
- Utility Sector Security (paragraph 53)
- Supply Chain Security (paragraph 85)
- Identity Management (paragraph 89)
- Mandatory Incident Reporting (paragraph 102)

Cloud Security Management
(NIS2 Directive paragraphs 33, 34, 35)

Cloud computing platforms such as Amazon AWS, Microsoft Azure, and Google Cloud Platform place a high focus on securing public cloud infrastructure. However, customers share equal responsibility for securing applications that run on cloud infrastructure.

For these scenarios, **BeyondTrust's Privileged Access Management** solutions implement enterprise cloud security best practices. Some key BeyondTrust capabilities in this area include:

- **Discovery and Onboarding:** Continuously inventory assets across cloud, physical, and virtual environments, and onboard them for management.
- **Least Privilege Enforcement:** Just-in-time privileges deliver the right amount of access without overexposing system credentials.
- **Secure Access and Bastion Hosts:** Secure layering, monitoring, and remote access adds security to the cloud.

Privileged Account and Session Management (paragraph 44)

Privileged access is unavoidable; however, we can ensure that access to privileged accounts, credentials, and secrets is under tight control by implementing privileged account and session management (PASM). Solutions in this space, like BeyondTrust 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, key, or secret. 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, recording sessions (including keystrokes, mouse movements, and button clicks), and providing playback for auditing and forensics purposes.

Hackers will target the well-known privileged accounts in a system to gain lateral movement through your environment. A privileged account and session management solution can effectively stop hackers in their tracks, limiting the impact of any malicious activity.

Privilege Elevation and Delegation Management (paragraphs 44, 49)

A common risk scenario within many organizations is the abundance 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 granular capabilities for this, meaning the user who needs to install Adobe Acrobat is granted full local administrator privileges to their workstation without a clear timeframe for revocation.

Using privilege elevation and delegation management solutions, such as BeyondTrust's **Privilege Management for Windows & Mac and Privilege Management for Unix & Linux** products, 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 type of least privilege access control capability not only allows users to have 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.

Additionally, the ability to say "Yes" to user requests for permissions often helps build a better relationship with the cybersecurity team, enabling better user engagement in securing the environment—something essential for successful security projects.

Ransomware Protection
(paragraph 54)

Digital transformation initiatives—from expanded cloud deployments and utilization to increased remote access—have massively increased the attack surface. Ransomware operators have taken advantage of this pitfall, claiming responsibility for spectacular attacks that have disrupted critical infrastructure for millions of people.

While ransomware attacks of yesteryear (i.e., WannaCry) tended to be untargeted, modern worm-able attacks that spread opportunistically (i.e., Ryuk, Trickbot) tend to be human-operated (hands on the keyboard) and highly targeted.

Ransomware operators typically scan for unsecured, open ports to start their attack. **Internet-exposed Remote Desktop Protocol (RDP) endpoints continue to be cited in threat reports as the #1 entry point for ransomware, giving attackers their initial foothold in roughly 50 - 80% of successful attacks.** Meanwhile, other remote access technologies, like VPNs, are also being stretched for use cases far beyond what is secure and are often poorly implemented. Another common ransomware spreading tactic is using social engineering, such as phishing emails with infected attachments or malicious links.

No matter how it is delivered, nearly all ransomware requires privileges in order to execute (install files or drivers, access registry keys, etc.) and encrypt data as well as to move laterally and spread. Increasingly, ransomware attacks are incorporating tricky fileless malware techniques to stay hidden while they advance through an organization's systems and network. BeyondTrust provides powerful, blended ransomware protection that is effective at dismantling or mitigating multiple steps of the ransomware attack chain.

How BeyondTrust Solutions Disrupt Ransomware Attack Chains

- Locks down remote access pathways and eliminates risky use of RDP, VNC, SSH, and VPNs.
- Prevents ransomware execution by enforcing least privilege and using application controls.
- Blocks malicious code from delivering ransomware payloads.
- Implements segmentation and microsegmentation to isolate assets, resources, and users to prevent lateral movement.
- Defends against attacks that exploit trusted applications and macros.
- Stops an infection in its tracks by preventing lateral movement.
- Prevents account hijacking by managing all privileged credentials.
- Enforces least privilege, secure remote access, and session management/ auditing for the services desk

Utility Sector Security
(paragraph 53)

In modern society, utility sectors provide the most important pieces of critical infrastructure. Cybercriminals, including nation-state threat actors, can inflict catastrophic damage by disrupting or otherwise compromising utility systems. This can be done for political gain or to win a high extortion fee, such as through a ransomware attack. Society at large has little tolerance for downtime of utilities. Some real-world attacks have even attempted to poison water supplies or corrupt nuclear facilities.

Operational Technology (OT) and ICS (industrial control systems), such as those found within utility provider infrastructure, are increasingly connected to the Internet and easily discoverable, potentially jeopardizing security for the entire critical infrastructure. These infrastructure environments are also highly reliant on legacy IT hardware and systems, some of which may never have been intended to become outwardly network-facing.

BeyondTrust Privileged Remote Access helps secure OT environments across the utility and other sectors, while also enabling zero trust principles. Privileged Remote Access:

- Enforces the philosophy of least privilege for remote access sessions.
- Treats managed devices with the same level of trust as an unmanaged device – which is zero.
- Provides application access independent of network access.
- Records all activities performed using remote access and disables functionality such as copy/paste.
- Enables API security to protect the integrity of data being sent from IoT devices to back-end systems.
- Enables segmentation and microsegmentation to isolate assets, and further mitigate or contain attacks.

Supply Chain Security
(paragraph 85)

Over the past several years, supply chain attacks—which compromise trusted software or hardware to infiltrate additional victims—have demanded global attention. World-shaking attacks (i.e., the SolarWinds breach, Kaseya) quickly impacted thousands of organizations, including many sensitive government entities.

By compromising a weak link—a remote worker, contractor, inadequately-hardenedsystem, overprivileged user, unmonitored machine identity, unsecured ports, or VPN vulnerabilities—an attacker can quickly infiltrate an organization and compromise software being used by thousands of customers.

BeyondTrust Privileged Access Management solutions provide foundational capabilities for hardening security and providing resistance and resilience to supply chain attacks.

Some key ways **BeyondTrust PAM** solutions improve supply chain cybersecurity include:

- Enforces least privilege and just-in-time access across the enterprise, including for remote access.
- Secures and manages every privileged credential (privileged account passwords, SSH keys, DevOps secrets, application/machine passwords, etc.)
- Manages and monitors every privileged session.
- Extends PAM best practices to the service desk.
- Unearths identity security insights to proactively improve defenses and shut down in-progress attacks.

Identity Management
(paragraph 89)

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. BeyondTrust Active Directory Bridge enables organizations to 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. Attestation and auditing capabilities ensure that what's assigned is what was provisioned.

BeyondTrust integrates with companies like SailPoint, that deliver enterprise-grade identity governance capabilities ensuring you know who has access, and to what. These integrations help provide a holistic view of privileged and unprivileged identities.

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).

Mandatory Incident Reporting (paragraph 102)

The NIS2 Directive outlines its demands for rapid, accurate reporting in paragraph 102. This reporting is critical to assess the impact of an incident and to coordinate a response so that other entities may be protected.

BeyondTrust products make it easy to see, audit, and report on privileged activity and identity-based threats. Products such as **Privileged Remote Access, Password Safe, and Remote Support** provide robust privileged session auditing capabilities, while our **Identity Security Insights** solutions provides a centralized dashboard for identity-based activity and threats.

About BeyondTrust

The BeyondTrust platform

Password Safe: Manage privileged passwords, accounts, credentials, secrets, and sessions for people and machines, ensuring complete control and security.

Privileged Remote Access: Extend privileged access security best practices beyond the perimeter by granularly controlling, managing, and auditing remote privileged access.

Remote Support: Supercharge your service desk with secure access and support for any device, any system, from anywhere—including Windows, macOS, Linux, Android, & iOS.

Privilege Management for Windows/Mac: Remove local admin rights, enforce least privilege dynamically across Windows and macOS, prevent malware and phishing attacks, and control applications.

Privilege Management for Unix/Linux: Achieve compliance, establish least privilege and zero trust, and prevent and minimize security breaches—without hurting productivity.

Active Directory Bridge: Streamline identity management and access controls by extending Microsoft AD authentication, SSO capabilities, and Group Policy configuration management to Unix and Linux systems.

Identity Security Insights: Gain a centralized view of identities, accounts, and privileged access across your IT estate, and leverage threat intelligence recommendations to improve your identity security posture.

Summary

The NIS2 Directive, like many compliance mandates, focuses on best practice processes and controls that help you deliver a more secure, reliable, and resilient environment. 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, **fundamental in adhering to NIS2.**

A strong foundation for cybersecurity 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.

BeyondTrust protects identities, stops threats, and delivers dynamic access to empower and secure today's work-from-anywhere world.

Much of what we do in monitoring our environments is focused on ensuring that users aren't misusing privileges they have been granted. In this least privilege model of security, users are only granted the privileges they absolutely need for the least amount of time. This results in less of an obligation to monitor these legitimate activities, resulting in far fewer "noise" events being generated.

To learn more about how BeyondTrust can help you address the NIS2 Directive, and any other security or compliance goals, **contact us today.**

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

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 75 of the Fortune 100, and a global partner network.
Learn more at **beyondtrust.com**