



GO BEYOND

BY BEYONDTRUST

Privileged Remote Access

WORLD
TOUR 2024



Trevor Combs

Sr. Solutions Engineer

Agenda

- ▶ **Intro**
- ▶ **Masterclass & Demos:**
 - **Vendor Portal**
 - **Network Tunnels**
- ▶ **Q&A**

Access is Only Efficient if it is Secure

The consequences of unsecured access are growing exponentially:

- ▶ In 2023, the cost of an average data breach hit a new record of **\$4.45M**
- ▶ Compare to the average cost of a data breach in 2017 at \$3.62M

BeyondTrust Products Solutions Resources Customers Partners About Watch Demo Contact Sales

Mitigating VPN Vulnerabilities: Understanding the Latest CISA Objective

February 13, 2024

Blog

Home / Blog / Mitigating VPN Vulnerabilities: Understanding the Latest CISA Objective

The [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) has issued an emergency directive ([ED 24-01](#)) following the widespread and active exploitation of vulnerabilities in two affected VPN products. The multiple vulnerabilities—[five of which were disclosed](#) in the last month alone—include authentication bypass, command injection, privilege escalation, and a server-side request forgery in the SAML component. Ed 24-01 instructs federal agencies to shut down, threat hunt adjacent systems, and remove [vulnerable](#) VPN solutions until they can be properly mitigated. Agencies are also required to perform additional forensic analysis and clean-up steps.

According to CISA, while both affected products have since been patched, the exploitation of the vulnerabilities found in these products could allow a malicious threat actor to move laterally, perform data exfiltration, and establish persistent system access, resulting in full compromise of target information systems. CISA has determined that this poses an unacceptable level of risk to Federal Civilian Executive Branch (FCEB) agencies, therefore requiring this emergency action.

Stay Up To Date

Get the latest news, ideas, and tactics from BeyondTrust. You may unsubscribe at any time.

Business Email

☐ I agree to receive product-related communications from BeyondTrust as detailed in the [Privacy Policy](#) and [Terms of Service](#), or to withdraw my consent at any time.

Up next

NIST Cybersecurity Framework 2.0 – What's New & What You Need to Know

March 8, 2024

Blog

Home / Blog / NIST Cybersecurity Framework 2.0 – What's New & What You Need to Know

Last week, NIST released Version 2.0 of the widely used Cybersecurity Framework (CSF), its landmark guidance document for reducing cybersecurity risk. The [NIST Cybersecurity Framework 2.0](#) has emerged not just as an update, but also as a transformative approach to securing digital assets and infrastructures. This evolution from its predecessor marks a significant step forward in addressing the nuanced and ever-expanding landscape of cyber threats and presents a forward-thinking perspective on cyber defense that recognizes the fluidity and complexity of the digital threat landscape.

In this blog, I cover the key updates to the framework, the cybersecurity challenges prompting NIST's latest response, the new role of privilege access management (PAM) and identity security, and why the framework's new perspective is imperative to today's cybersecurity efforts.

Stay Up To Date

Get the latest news, ideas, and tactics from BeyondTrust. You may unsubscribe at any time.

Business Email

☐ I agree to receive product-related communications from BeyondTrust as detailed in the [Privacy Policy](#) and [Terms of Service](#), or to withdraw my consent at any time.

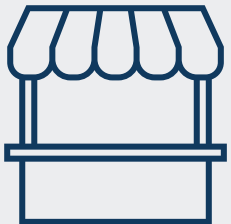
Vendor Portal

One place to secure and manage vendor access

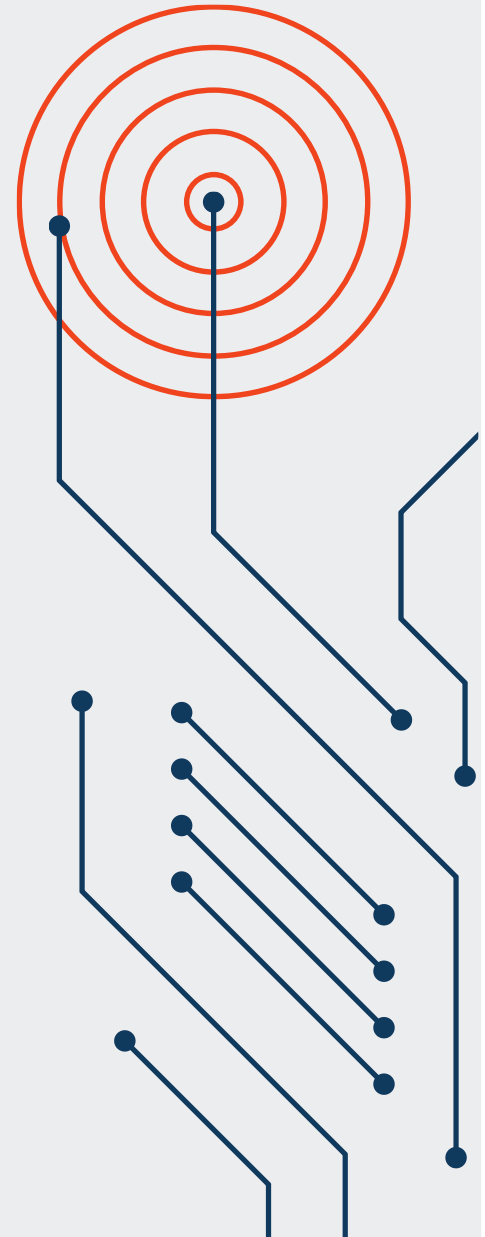


Vendor Portal

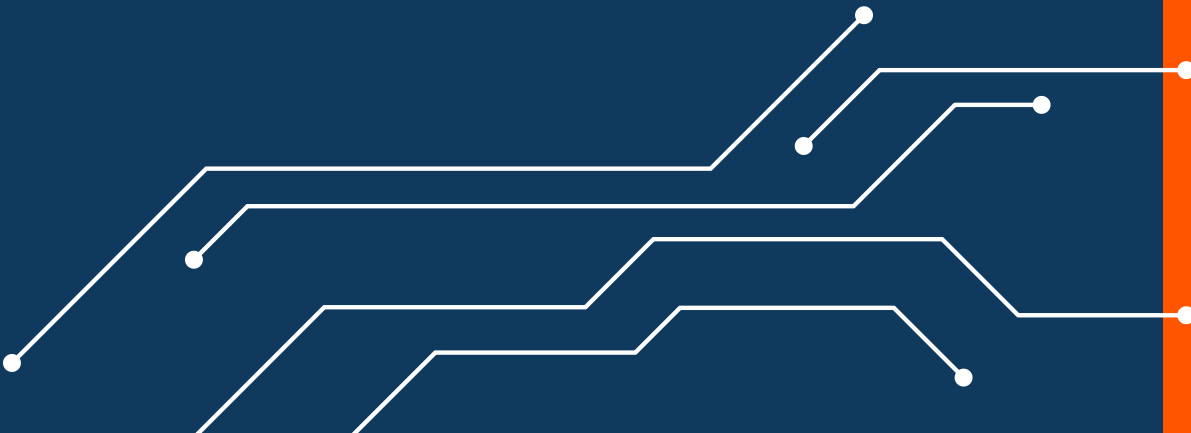
- ▶ Who here has heard of the Vendor Portal in PRA?
- ▶ Who here is using the Vendor Portal feature today?



**Alleviate your vendor management effort
with a one stop shop for your vendors**

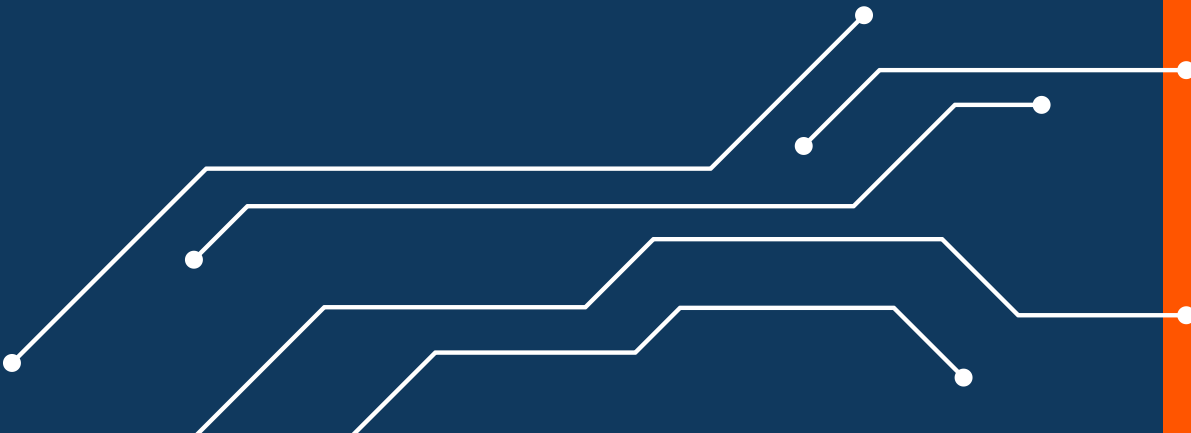


Why would you use Vendor Groups?



**To move the
account creation
and management
burden away from
the PRA Admin and
internal IAM,
without sacrificing
security. >>>**

Advantages of Vendor Groups



Advantages:

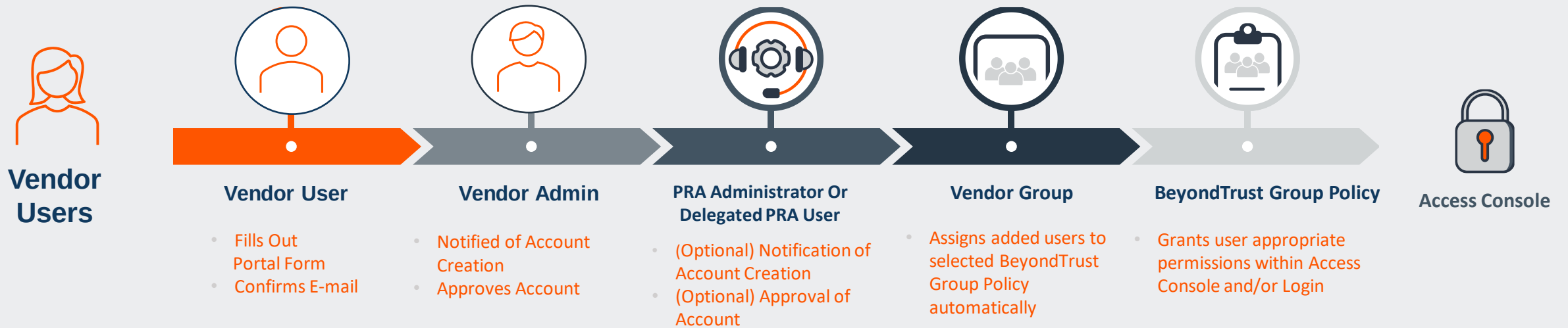
- PRA Admin does not have to set up all user accounts.
- Vendor can add new users without waiting for PRA Admin availability.
- Accounts created can auto-expire to avoid leaving unused and forgotten accounts open and available.

Account Feature Comparison

Feature	PRA User	Vendor User	Vendor Group Admin
	Delegated user that can manage vendor users and some self-registration settings.	A user account that only exists in the Vendor Group	Appointed user from Vendor that can manage the Vendor Users
Onboarding	Created by a PRA Admin or imported from Security Provider (AD, SAML, etc)	Created by the PRA User / Vendor Group Admin or Vendors can Register themselves on the Vendor Portal	Created by a PRA User / Admin
Access and Permissions	Can be a member of multiple BeyondTrust Group Policies in order to have a complex permission set.	Can only be a member of a single BeyondTrust Group Policy shared by all members of that Vendor Group	Can only be a member of a single BeyondTrust Group Policy shared by all members of that Vendor Group
PRA Admin Privileges	Can be a member of a Group Policy that grants Administrative permissions	Group Policies that grant Administrative permissions are not available for Vendors	Group Policies that grant Administrative permissions are not available for Vendors
Offboarding	Doesn't require an expiration date, but can be given one	Will auto-expire to avoid leaving forgotten accounts, but can be reactivated	Will auto-expire to avoid leaving forgotten accounts, but can be reactivated

Vendor User Self-Registration

Through Vendor Groups



Demo

Let's Setup & Use a Vendor Portal



Vendor Groups

Remember:

- Purpose is to **move account creation and management** burden away from the PRA Admin.
- A **Vendor Admin** is appointed user from Vendor that can **manage the Vendor Users**
- Vendor Users / Admins can only be associated with a **Single Group Policy** with **no Admin Permissions**
- Accounts created **auto-expire** to avoid leaving unused and forgotten accounts open and available.

Network Tunnels

Take protocol tunnels to the next level



Network Tunneling – Beyond VPNs

Entirely new from BeyondTrust

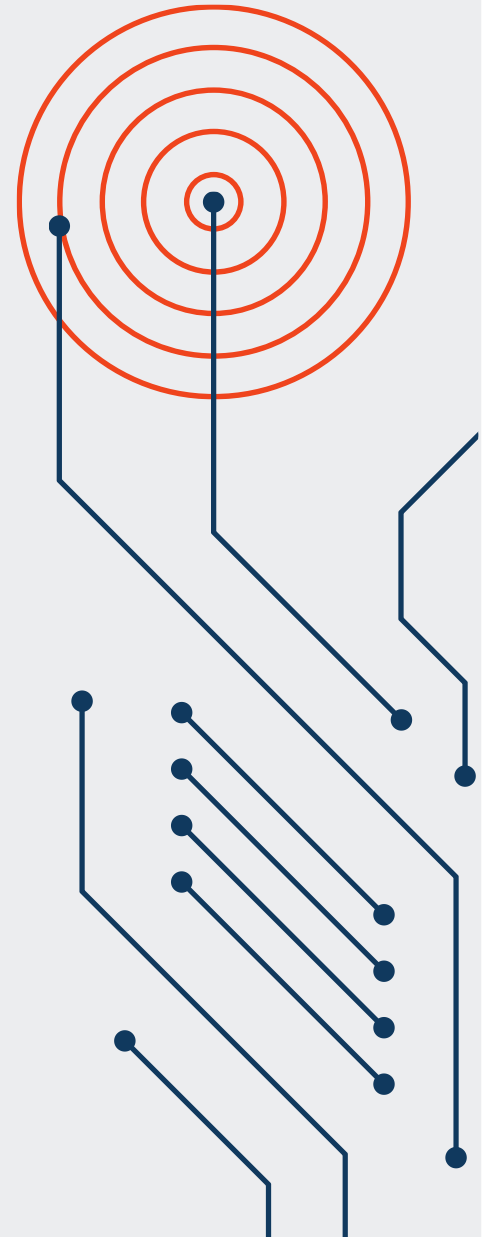
More ways to access more devices than traditional VPNs, with familiar controls.

Network Tunnels

- ▶ Total VPN replacement for all environments: the cloud to the on-prem factory floor
- ▶ Solve for OT and IoT use cases built on PLC devices, anything relying on UDP or other protocol types
- ▶ Included in your deployment at no cost – as it's an advanced feature, please ask support to switch it on



One way to connect to all things



Demo

Quick Demonstration

Create & Connect



Hands-free appliance management

Level up your organization by migrating to our SaaS deployment

- ▶ Complete feature and functionality parity
- ▶ Automatic version updates
- ▶ Eliminate maintenance costs: BeyondTrust maintains and sizes your appliance for you
- ▶ BeyondTrust handles the failover, ensuring uptime and backups
- ▶ More APIs
- ▶ Just a few clicks to migrate your entire deployment

Interested in learning more?

Reach out to your account manager and ask about migrating to the cloud

Try it Today!

- ▶ Start using your Vendor Portal today –accessible on mobile!
 - Configure and create instructions immediately
- ▶ Reach out to support to turn on Network Tunnels – start connecting right away

Create identity-secure, just-in-time access to all your environments:

cloud, on-premises, and OT.



Thank you!

A summary of today's class with
links to helpful documentation

bit.ly/pramasterclass

beyondtrust.com/gobeyond-masterclass-recap-privileged-remote-access