Meet NERC CIP Version 5 Cyber Security Standards with Bomgar Privileged Access Management

NERC CIP v5 REQUIREMENT FOR REMOTE ACCESS

In 2007, the Federal Energy Regulatory Commission (FERC) commissioned the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) as a mandatory standard within the United States. In 2013, FERC approved version 5 of the CIP standard, which becomes enforceable on April 1, 2016. CIP V5 builds upon previous versions, particularly in the areas of security awareness, physical security, remote access and incident response. Organizations throughout the energy sector are now scrambling to become compliant in these areas prior to the April 1st deadline.

Many of these organizations have already realized that the VPNs or similar technologies they are using for remote access do not meet the standards set forth in CIP V5. Specifically, most VPN technologies are not compliant with part 2.1 and 2.2 in CIP-005-5 Table R2. When a VPN connection is used for remote access it gives the external vendor or remote worker direct access to the BES cyber systems. This violates the controls set forth in these two sections of CIP V5. In addition, it is difficult to meet other auditing and reporting mandates within the mandate using a legacy VPN system.

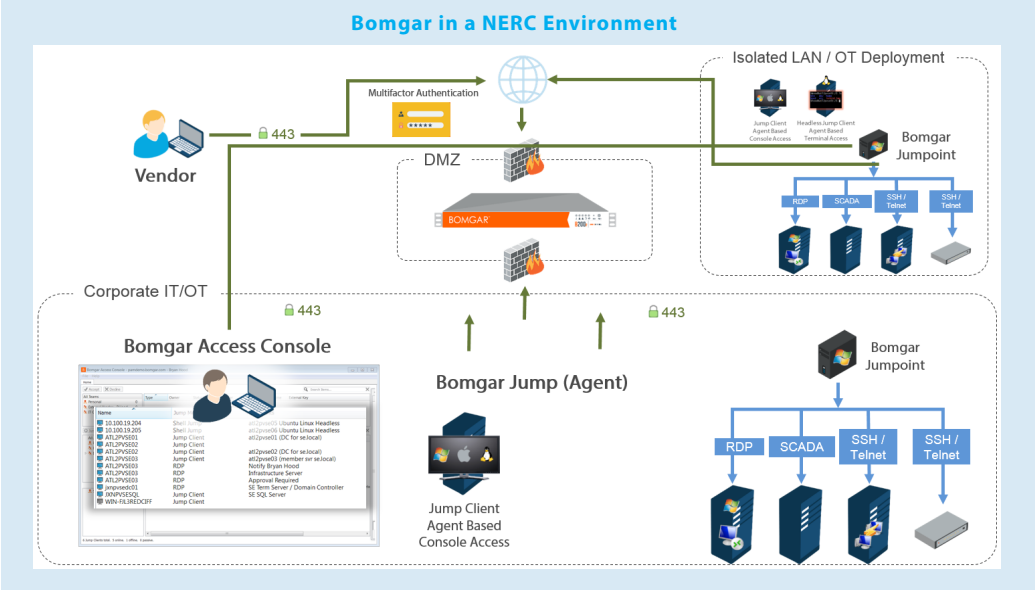
BOMGAR PRIVILEGED ACCESS MANAGEMENT

Bomgar's Privileged Access Management solution allows security sponsors to control, monitor, and audit access by privileged users and third-party vendors. Both the remote user and the endpoint connect to the Bomgar appliance via outbound connections, eliminating the need for a VPN tunnel that provides a direct connection. Bomgar is the only remote access solution that terminates connections from external parties in a manner that is compliant with parts 2.1 and 2.2 of CIP version 5.

In addition, Bomgar allows organizations to granularly set session permissions and record and monitor session activity, supporting CIP V5 standards outlined on the Electronic Security Perimeters Table R1. Using Bomgar, security sponsors can see and approve when a third-party or vendor needs access to their internal systems, limit which systems or applications they can see and access, and monitor all activity from their desktop or mobile device.

Finally, Bomgar helps organizations to meet CIP requirement 2.3, which calls for multi-factor authentication for all interactive remote access sessions. Authentication is a major challenge throughout the energy sector where old machine accounts and shared accounts are often rampant. Through Bomgar's native password vaulting technology or integrations with existing password management solutions, energy organizations can meet this requirement while improving their level of threat protection.

Bomgar in a NERC Environment



The standard requirements are represented in two main sections covering "Electronic Security Perimeter" and "Interactive Remote Access Management". Bomgar Privileged Access Management Solution can help organizations to meet these requirements and satisfy CIP V5 mandates.

ELECTRONIC SECURITY PERIMETER (ESP) TABLE R1

REQUIREMENT	BOMGAR RESPONSE
R 1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Bomgar is an on premise appliance which can reside within the ESP. The appliance facilitates secure access to cyber assets and secures routable protocols through layered granular access controls; giving administrators a detailed view in to session activity around cyber assets.
R 1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Bomgar enables secure access to assets within the EAP. All connections are outbound through the centralized Bomgar appliance and can be monitored and terminated by administrators, allowing Bomgar to act as an EAP for external connectivity.
R 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	Bomgar allows organizations to implement granular access controls and set up approval workflows that trigger real-time approval requests, notifications, and require approvers to input reason for granting access.
R 1.4 Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	With Bomgar, authentication is required for access. Only the appliance facilitates access, allowing secure connectivity to cyber assets.
R 1.5 Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Bomgar's recording features provide live surveillance and monitoring capabilities. All activity, whether malicious or non-malicious, is recorded and can be automatically populated into your SIEM tool. Malicious activity can not only be detected, but auditors can look back and see exactly what happened through video logs of all access activity.

INTERACTIVE REMOTE ACCESS MANAGEMENT TABLE R2

REQUIREMENT	BOMGAR RESPONSE
R 2.1 Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Bomgar governs access to nearly any system or device, anywhere, while keeping sensitive data and system access behind your own secure firewall. Unlike legacy solutions, such as VPN, there is no direct or unmonitored access to cyber assets since all access is brokered through the secure appliance.
R 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	All Bomgar access sessions utilize the latest TLSv1.2 encryption technologies that are terminated at the appliance. Setting granular session parameters keeps vendors and privileged users where they need to be.
R 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.	With the choice of in-house tools such as Bomgar Vault, or pre-built integrations with password vaults such as Thycotic or Lieberman; Bomgar users increase their level of protection through the use of multi-factor authentication and secure password management.

Bomgar Privileged Access Management enables power and energy plants to securely manage their networks and operate within compliance of strict cyber security regulations set by NERC.

To learn more about Bomgar's secure access solutions visit: **www.bomgar.com/access-management.**