BEST PRACTICES FOR NETWORK SECURITY CONSOLIDATION IN GOVERNMENT

Through network security consolidation, government agencies can achieve tighter integration between previously disparate systems while automating and simplifying the process for responding to and preventing malicious activity. Outlined here are best practices to ensure a smooth migration.

1. Know what and who you are protecting as well as where they are located.

Before undergoing network security consolidation, government agencies should take inventory of their networks and systems to understand where critical data and infrastructure lie. It is also important to identify the critical users within the network and extend additional protections to them. For example, implementing credential theft prevention will ensure users' credentials aren't compromised, and multi-factor authentication will prevent the abuse of stolen credentials to access critical systems, information and data.

2. Understand who can, and should be able to, access what you are protecting.

Gone should be the days of large, flat data centers with open IP networks that allow access by anyone with the IP address. Instead, government agencies should apply role-based access controls, or RBAC, and the Zero Trust principle to ensure access is only granted to those who require it. RBAC regulates access to data and applications based on the roles of individual users within a government body. Similarly, Zero Trust, rooted in the principle, "never trust, always verify," is designed to address lateral threat movement within the network, such as exploitation and credential abuse, by employing micro-segmentation and granular perimeter enforcement based on user, data and location.

3. Identify why and from where users access what you are protecting.

Government agencies must be able to prevent bad actor states from accessing critical data or infrastructure. This requires insight into users' specific locations as well as knowledge of the devices being used. Access should be limited to locations and devices that are explicitly approved. It is equally important to understand why a given user needs access to a given system or application. This should be determined based on job function and regulated on an ongoing basis to determine access to systems over time. Primary communication channels should be encrypted to ensure data confidentiality and integrity. Conversely, encrypted applications should be decrypted to prevent malicious activity hiding within them.

When done correctly, consolidating multiple security point products into one integrated platform allows for easier adoption of security best practices to reduce opportunities for attack. A platform approach also allows for automation of routine tasks so government security teams can focus on hunting down and stopping the threats that matter most.

To learn more about the benefits of network security consolidation in government, read the white paper "Reduce Costs and Complexity With Network Security Consolidation."