xage SECURITY

Modernizing Remote Access with Xage

Overcoming Legacy VPN Challenges in Ivanti and Cisco ASA

Recent vulnerabilities identified in legacy VPN systems such as Ivanti & Pulse Secure have prompted various urgent advisories from CISA and DHS. These legacy systems, once the backbone of enterprise remote access, have shown susceptibility to cyber threats and unpatchable vulnerabilities, underscoring the need for advanced security solutions. Xage's Zero Trust Access (combined ZTNA and PAM capabilities) emerges as a comprehensive response, offering robust protection tailored to modern cybersecurity demands.

Legacy VPN Vulnerabilities and Government Directives: Recent advisories from US federal agencies have highlighted significant vulnerabilities in these traditional VPN solutions, including *authentication bypasses, command injections,* and other exploits that enable *unauthorized access and lateral movement* within networks. The directives emphasize the immediate need for organizations to reassess and fortify their cybersecurity frameworks to protect against these evolving threats.

How Xage Zero Trust Access (ZTA) Addresses the Shortcomings of Legacy VPN Technologies?

Legacy VPNs present significant security challenges by granting broad network access, which can inadvertently expose critical resources and create opportunities for cyber threats. They allow users and potentially compromised endpoints direct entry into sensitive networks, increasing the risk of data breaches. In contrast, Xage ZTA (combined with ZTNA and PAM), ensures secure, granular, and context-aware access. With this approach users are kept outside the network, with access carefully proxied and tailored to individual assets, significantly reducing the likelihood of unauthorized access. Moreover, Xage Fabric provides an added layer of security by protecting the network's assets from potentially compromised endpoints, thus fortifying the organization's defense against cyber threats.

Below is a quick comparison of How Xage ZTA address to concerns associated with various legacy VPN solutions:

Vulnerability Type	Ivanti Solutions / Pulse Secure	Cisco ASA Solutions	Xage Zero Trust Access (ZTA)
Authentication Bypass	Vulnerable to CVEs like CVE-2023-46805, CVE-2019-11510, CVE-2024-21887.	Affected by various CVEs, often requiring patches.	Utilizes identity-driven access, ensuring authentication is verified before access is granted. Enforces least privilege access, reducing the attack surface.
Webshell Installation	Affected by CVEs allowing unauthorized access and file manipulation.	Vulnerable if misconfigured or not updated.	Provides full visibility and control of remote sessions, mitigating webshell risks.
Lateral Movement	Vulnerable due to network-centric models and allows later movement if the internal networks are compromised.	Susceptible if perimeter security is breached.	Implements identity-based segmentation to block unauthorized lateral movements.
Persistent Access	Can be compromised, allowing long-term access.	Vulnerable if updates and patches are not applied.	Employs continuous verification, eliminating all-or-nothing access and preventing persistence.
Agent-based Limitations	Relies on agents that may not cover all devices.	Often requires client software for VPN access.	Agentless, ensuring all devices, including OT and legacy systems, are protected.
Complexity and Usability	Can be complex to manage, update and patch.	Configuration can be complex and error-prone.	Simplifies secure access, offering a friction-free administration and experience for users without compromising security.