

# Stop Lateral Movement and Stolen Credential Attacks with Zero Standing Privilege

Netwrix Privilege Secure for Discovery is an agentless Lateral Movement Prevention solution that administers dynamic Just-in-Time (JIT) privileged account access to help customers achieve Zero Standing Privilege. With Netwrix Privilege Secure for Discovery, IT administrators and security analysts have dynamic and continuous visibility into their organization's permanently provisioned privileged accounts and can remove them with one click. Users then self-administer privilege access, getting access to only the right resource, at the right moment and for the length of time they need to complete their job. This approach eliminates standing privileges, effectively preventing lateral movement attacks and significantly reducing an organization's attack surface.



**82%**

of ransomware attacks utilized lateral movement techniques



**74%**

of breached organizations admitted the breach involved access to a privileged account



**41%**

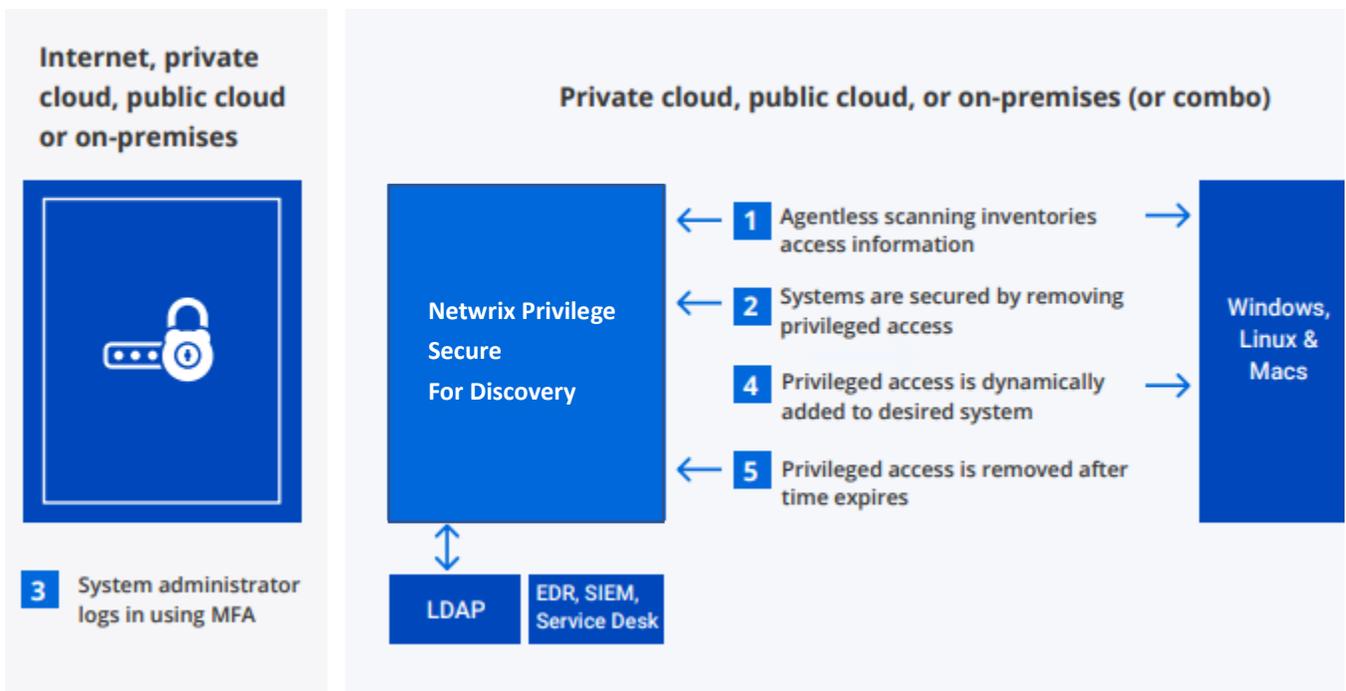
of surveyed organizations admit to allowing users to retain privileged account access indefinitely

## Benefits:

- Prevent lateral movement of compromised privileged accounts early to stop attackers from spreading identity-based threats such as ransomware and phishing
- Reduce the attack surface by removing 24X7 admin access sprawl and replacing it with JIT administration to ensure Zero Standing Privilege (ZSP)
- Simplify deployment and management. Netwrix Privilege Secure for Discovery is agentless. This architectural approach dramatically reduces the complexity of employing yet another agent and simplifies support and management
- Enable Zero Trust security with MFA to provide the right access to the right resources for just the right amount of time
- Enhance the value of our technology partners and improve the security risk posture of organizations by providing PAM context
- Complement and secure traditional PAM implementations by removing undetected 24x7 admin access sprawl that exists outside the vault.

## The Problem: Prevalence of Undetected 24x7 Privileged Access Sprawl

- **Undiscovered, always changing privileges.** Today, there is no automated way for organizations to discover and inventory all the privileged access across the enterprise. Traditional privileged access management (PAM) vendors with vaults only protect known privileges and have no visibility into the sprawl of 24x7x365 administrator privileges across an enterprise.
- **Unnecessary standing access = larger attack surface.** Standing privileged user access without business justification allows hackers to move laterally and spread identity-based threats such as ransomware across a network. It is imperative to remove these standing privileged accounts across Windows, Linux, and Mac systems and replace them with appropriate access directly to user accounts just for the time needed.
- **High friction user experience for administrators.** Administrators managed through a password vault have to check out a generic or shared ID and get approval every time there is an incident. This approach slows down their ability to respond quickly, thereby increasing Mean Time To Respond (MTTR) and impacting uptime.
- **Incomplete, inaccurate view of risk posture.** The number of privileged accounts across the enterprise is a key indicator of an organization’s overall risk posture. Today, there is no way to comprehensively report on this risk across an enterprise, nor there is a way to report on how the risk posture has evolved over time.



## Stop Lateral Movement and Stolen Credential Attacks with Zero Standing Privilege

Netwrix Privilege Secure for Discovery was purpose-built to address this problem and be a force multiplier to Identity and Access Management (IAM) and traditional PAM programs worldwide. Specifically, Netwrix Privilege Secure for Discovery was developed to:

1. Rapidly deploy, scan and inventory Windows, Linux and Mac privileged access with no agent
2. Continuously monitor
3. Remove standing access enterprise-wide with a single action, and
4. Administer privileges Just-In-Time (JIT) and MFA to enable Zero Standing Privilege (ZSP) and implement Zero Trust security

### Key Capabilities

- Dynamic and agentless discovery of 24X7 admin access sprawl across Windows, Linux and Mac systems (Scan 10,000 endpoints in approximately 25-30 minutes)
- Agentless install reduces deployment complexity: No need to install and configure intrusive PAM agents on every endpoint or system
- Single click removal (milliseconds per endpoint) of undetected and unnecessary 24X7 privileged accounts sprawl reduces the attack surface
- Visualize, analyze and manage your attack surface with Privileged Access Risk executive and practitioner dashboards
- Administer Just-in-Time (JIT) privileged access with MFA to enable Zero Standing Privilege (ZSP) and implement Zero Trust security
- Intelligent Session Capture (ISC): The ability to identify privileged accounts, access end-user session data through EDR vendors and provide context/alerts on nefarious privileged session activities such as malware download and accessing C&C sites. This enables SOC analysts to prioritize incident response/remediation.
- Leverage EDR integration for remote management of Windows systems that are located outside the corporate network with no VPN connectivity
- Protects access: Attackers have no access to endpoints or opportunity for lateral movement even if accounts are compromised
- Low friction Admin experience: Administrative experience using the admin's own account, no need for secondary or auxiliary accounts to use JIT.

## About Netwrix

Netwrix makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,000 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity and infrastructure.

For more information, visit [www.netwrix.com](http://www.netwrix.com)

## Next Steps

**See Netwrix products** — Explore the full Netwrix portfolio: [netwrix.com/products](http://netwrix.com/products)

**Get a live demo** — Take a personalized product tour with a Netwrix expert: [netwrix.com/livedemo](http://netwrix.com/livedemo)

**Request a quote** — Receive pricing information: [netwrix.com/buy](http://netwrix.com/buy)

### CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite  
100 Frisco, TX, US 75034

### PHONES:

1-949-407-5125  
Toll-free (USA): 888-638-9749

### OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

### SOCIAL:



[netwrix.com/social](http://netwrix.com/social)

---

5 New Street Square, London  
EC4A 3TW

+44 (0) 203 588 3023