netwrix

What is Lateral Movement?

Attackers seldom breach a network at their final destination. They look for the easiest entry point—a forgotten endpoint device, a compromised admin password extracted from the dark web, or an unwitting employee who downloads and installs malware. Once they gain this initial foothold, they use lateral movement, typically with compromised or newly discovered admin accounts to reach their goal: Personally Identifiable Information (PII data), sensitive emails, strategic information, or anything else of value. They then use unprotected privileged access to steal this data and lock it away with ransomware.

In its simplest terms, lateral movement is when attackers take control of one asset within your network and then obtain privileged access to move around and exploit other assets.

As happened with the 2013 Target breach, attackers may island-hop into your network from a smaller, less protected third party's network or they may gain access directly. Regardless, once they're in, they move laterally across your network until they reach their target or land upon something else, they know is valuable.

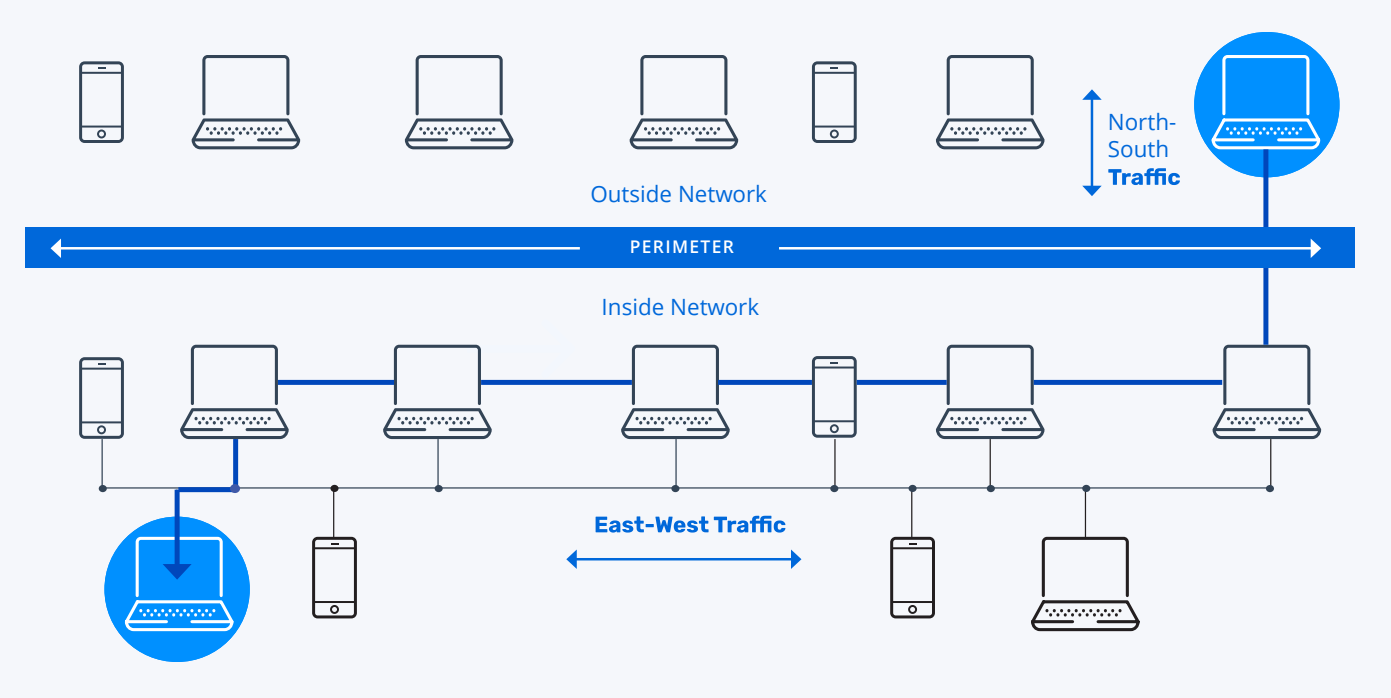
Think back to the SolarWinds attack. If anything positive came from that attack, it's that even more people now realize how dangerous lateral movement can be— and why it's important to build up a defense against it. A year later, hackers broke into Colonial Pipeline's network via a compromised username and password and threatened to seize control of the largest fuel pipeline in the US. As a result, Colonial Pipeline shut down the pipeline for the first time in its 57-year history. The company paid 75 bitcoins to ransom the network—almost $4.5 million.

Those attacks were not outliers. Attacks—and their severities— have been on the rise. During 2020, ransomware attacks rose 485% year-over-year. Many factors—the COVID-19 pandemic, growing numbers of work- from-home workers, and the commoditization of ransomware-as-a-service— drove this growth, but the fact remains: lateral movement attacks will remain part of our reality for a long time.

Perhaps most importantly, this surge in ransomware attacks exposed the weak or reactive security practices that organizations have been forced to cobble together as they raced to navigate the technological—and social—change brought on by demand for digital transformation and the hard realities of the pandemic over the last 24 months. Many of these security tools and practices had to be rolled out quickly. As a result, there are gaps that allow attackers to gain access to and move laterally from one system to another with relative ease.

How Does Lateral Movement Work?

Network diagrams often show traffic entering and leaving your network on the Y axis and movement within your network on the X axis. That's why capabilities moving laterally within your network often get called east-west traffic, while capabilities that cross your perimeters are called north-south traffic. It's how malware designed to perform reconnaissance downloads its weaponization, when it uses lateral movement to achieve a more advantageous vantage point on the network, for example.



After cyber attackers breach your perimeter—perhaps by phishing login credentials from an unwitting, overly helpful employee—they use that access to harvest and steal additional privileged user credentials (or even just the hashes) with greater levels of access, ultimately including privileged access.

By stealing the credentials (literally, the identities) of your employees, these cyber criminals move laterally across your network by logging into other accounts and machines, searching for other assets or credentials to steal. They become digital insiders and can stay for days, months, and years— dormant and lurking—until they're ready to execute their attack.

It is difficult to detect lateral movement attacks because these cybercriminals are masquerading as your trusted users and weaponizing their access. While the breach is occurring, it's hard to even know it. The access and the account will probably be authorized, even though the bad actor who is dialing in from miles, or continents, away isn't.

The Three Stages of Lateral Movement

These stages aren't unlike the steps a tourist takes in a foreign country when they're trying to keep a low profile and blend in before they venture out to explore. Even attackers often follow the predictable patterns of human nature.

Stage 1: Thieves Start by Learning the "Lay of the Land"

Before they can, or even know how to, move laterally across your network, thieves start by laying low and learning about the setup and culture of your IT ecosystem. They watch your administrative users and devices. They map your network. They're looking to learn from you, so they can learn how to attack you.

They want to understand:

- Network hierarchies
- Host naming conventions
- The location of your payloads
- Your operating systems
- Access control systems

Like that timid tourist navigating a new country, they don't want to make a wrong move that will expose them. They want to stay invisible.

These bad actors come armed with tools. Their tools tell them where you've put your firewalls and other end-point security. They learn what's available to access, and where these assets are located in your network. They build their own or adapt open-source tools, but often, can purchase the entire stack of attack tools from dark web marketplaces.

During this reconnaissance phase, attackers lurk and gather data until they know enough about you, your privileged users, and your ecosystem. Then, they move.

Stage 2: Thieves Then Steal Log-In Credentials

To do anything inside a network—valid or illicit—you need a user ID and a password that work. Lateral movement is no different. The lowest-tech way to steal a privileged user's login credentials is still to … just ask for them.

PHISHING

In phishing, cyber-criminals prey on an employees' trusting nature, unfamiliarity, or even indifference to a technical looking request. They may impersonate your tech support team and ask admin users to enter their ID and password into a fake portal, for example. Or they call your admin user, impersonate a technical employee, and hoodwink the user to verify their identity by asking and getting their username and password. They only need one privileged user in your company to be helpful.

It happens more often than you think. December 2020 research from Security Boulevard shows that over 30% of phishing emails are opened and 12% are clicked through.

TYPO SQUATTING

One step more complex than phishing, cybercriminals use typo-squatting when they set up a fake website that impersonates a valid one. In the fake site's URL, they may make a common misspelling to the true website's name, move a letter, or add a period. Another common method is to add a hyphen and another word to a valid site name.

At the fake site, the cybercriminals appropriate the logos, branding, and color scheme of the target company to treat the unwitting visitor to a mimicked user experience.

Once they begin receiving hits, these cybercriminals steal credentials, payment card details, and other PII. After they gain access to a user's credentials, the bad guys use lateral movement within the network or island-hop to reach the crown jewels.

ADVANCED PASSWORD-STEALING SCHEME

Beyond phishing and typo-squatting, cybercriminals can target the user login credentials of even the savviest users on your network—without them ever knowing. Through a Pass the-hash attack, cybercriminals steal the hashes of a user's password without ever needing to learn the actual plaintext password. They then use the hashes to authenticate to a remote service or server.

Cybercriminals may also use tools like Mimikatz to pilfer passwords and user credentials stored in the memory of a machine or keylogging tools to steal a password as it's being typed.

Stage 3: Intelligence Gathering

After they've gained the confidence to move around your network and have stolen the identity of one or more of your admin users, Cybercriminals now set about searching out the assets they want. They move laterally along the paths that will take them there.

From the privileged user they've hacked, they move through your network, seeking new and more important locations and users. They hope to find the holy grail—privileged access that's been left active and forgotten. They need that standing privilege to enter your network's most protected areas.

Why Is It So Hard to Detect Lateral Movement?

Over the last two years especially, we've seen the damage that lateral movement can cause, but it's an attack strategy that has plagued the industry for years. Why? As an industry, we've put so a majority of our collective efforts into improving endpoint cyber security controls. Privileged access is most commonly an IT function; thus controls just have not kept up.

Cyber attackers exploit this lack of privileged access management as an easy attack vector. They see it as a simpler task to gain access through a compromised credential or privilege escalation and to ride that lateral movement across your network. That's what happened in the SolarWinds attack. The cyber attackers gained access to the SolarWinds network and then installed malicious code into Orion, SolarWinds' software system.

When SolarWinds unknowingly pushed trojanized updates to this software out to as many as 33,000 customers, the malicious code went with it, replicating across cyberspace and granting the cyber attackers footholds in thousands of companies to move laterally. At last count, the fallout from the SolarWinds attack is estimated to have reached some 18,000 SolarWinds customers, ranging from well-known Fortune 500 companies to high-level agencies within the US government.

Why Are Breaches Like SolarWinds So Hard to Detect?

It's hard to detect lateral movement within a network because it's hard to determine who is driving that authorized credential and what their intent might be. It might just look like normal network traffic. SolarWinds customers certainly didn't automatically red flag their Orion updates as they arrived, even though they had been trojanized with malicious code sent by cyber attackers.

How to Use Zero Trust to Contain Lateral Movement

With the right tools, you can contain lateral movement and mitigate the damage cyber attackers can do to you and your environment.

Even if an intrusion occurs, lateral movement becomes much harder to accomplish if you've removed 24x7 administrator access with a Zero Trust access model. With a Zero Trust approach, any system must reverify your access and reestablish trust explicitly. That's not always as easy as it sounds. That's why excess standing privilege is so prevalent across today's networks.

1,322,935 total instances of standing privilege (from systems successfully scanned)

131,400 broken down by server

1,191,535 broken down by workstation

186 average number by server

697 average number by workstation

How much standing privilege do you have lurking in your system? With Netwrix SecureOne, you can discover and reduce standing privilege by 99% in just minutes. You can then add back privileged access on a Just-in-Time (JIT) basis with MFA to enable Zero Standing Privilege (ZSP) and implement Zero Trust security. This prevents lateral movement by providing the admin user access to only the right resource for a limited amount of time after which the JIT session is revoked.

We don't replace EDR or traditional PAM. We work with them. When you use Netwrix SecureOne with your existing PAM or endpoint security solution, you'll find that we're better together, improving your security controls across the board. So, what does Netwrix SecureOne offer that EDR, and PAM don't?

Complement EDRs

We didn't create Netwrix SecureOne to replace Endpoint Detection & Response (EDR). We built Netwrix SecureOne to complement EDR's best qualities. Netwrix SecureOne now integrates with CrowdStrike Falcon, Sentinel One, and VMware Carbon Black Cloud to deliver the industry's first PAM and EDR solution. By integrating with endpoint security solutions, Netwrix product leverages the EDR agent to enable and revoke JIT access on remote Windows systems that are outside the corporate network and have no VPN connectivity.

While traditional EDR protects your endpoints by monitoring them, Netwrix SecureOne brings you the confidence that comes when you know your standing privilege is managed and that the people using it are the people it was assigned to.

Where Traditional PAM Falls Short

Even with the best Privileged Access Management (PAM) solution, you can still fall victim to a breach. Traditional PAM manages credentials, not access. That's because traditional PAM leaves lots of Just-in-Case administrative access (standing privilege) in place rather than accomplishing Zero Standing Privilege (ZSP) and establishing a Zero Trust model.

Traditional PAM doesn't help customers eliminate the 24x7 standing access that attackers use once they compromise a privileged user. And, with Netwrix SecureOne, we'll help you create a process to stop excess standing privilege from coming back.

How Netwrix Can Help

It's hard to detect lateral movement—even while it's happening. With the right controls and tools, however, you can prevent lateral movement from occurring or even stop a breach in progress. By implementing a Zero Trust privileged access model for your administrators, you remove the 24x7 admin rights that cyber attackers need to move laterally across your network even if they successfully gain access to a trusted user's privileged account, they will not be able to weaponize that access if it's been turned off.

With a Zero Trust model, a credential's access to an endpoint or server gets revoked and cannot be used for lateral movement. When your privileged user needs that access again, Netwrix SecureOne helps you provision that access back on a time limited, principle-of-least-privilege basis.

Netwrix SecureOne helps you implement a Zero Trust approach in your organization by:

- Finding and removing privileged access
- Reducing your attack surface
- Implementing just-in-time access, going forward with MFA to enable ZSP
- Protecting against lateral movement attacks such as ransomware

Adopting Zero Standing Privilege through Netwrix SecureOne reduces an attacker's ability to move laterally from endpoint to endpoint and removes a key tactic attackers use when they breach your network.

As organizations continue to pursue their digital transformation goals, Netwrix SecureONE helps Security Architects and Security Managers implement and maintain critical privileged access controls through its agentless Zero Trust approach.

Different than legacy PAM solutions, Netwrix SecureONE detects and enforces Zero Standing Privilege at scale. Working together with other security platforms, Netwrix SecureONE helps you achieve attack surface reduction and strengthen the controls protecting your organization against lateral movement attacks.

- 5.5 hours to enable across all servers
- 99% reduction in risk

And it's easy to implement. Netwrix SecureOne takes just 5.5 hours to enable across all servers and delivers an improved Total Cost of Ownership with its 99% reduction in risk with no additional FTE requirements. Can we help you prevent lateral movement next?

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

Next Steps

See Netwrix products — Explore the full Netwrix portfolio: netwrix.com/products

Get a live demo — Take a personalized product tour with a Netwrix expert: netwrix.com/livedemo

Request a quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:

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

5 New Street Square, London
EC4A 3TW

PHONES:

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

+44 (0) 203 588 3023

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