What isLateral Movement?

illumio.com/cybersecurity-101/lateral-movement

Lateral movement has become synonymous with data breaches over the past several years, which references cybercriminals' techniques once they gain access to a network. Lateral movement allows hackers to move deeper into a system to track sensitive data, intellectual information, and other high-value assets.

The threat actor initially gains access to the system through an endpoint via a phishing or ransomware attack or malware infection. They then impersonate an authorized user to continue. Once inside the network, the threat actor moves from one asset to the next, maintaining ongoing access by traveling through the compromised system and stealing advanced user privileges using various remote access tools.

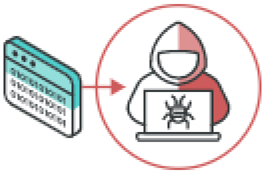
Cyberattackers use lateral movement as a core tactic, moving today's advanced persistent threats (APTs) far beyond yesterday's more simplistic cyberattacks. Internal network security teams must work overtime to detect lateral movement and stop it in its tracks.

Back

Common Reasons Lateral Movement Occurs

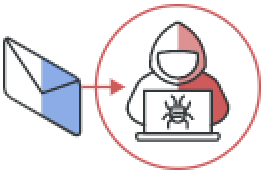
Malicious threat actors generally have one primary goal in mind, and it can vary from one hacker to the next. Some reasons why cybercriminals use lateral movement to gain access to a network include:

Accessing a developer's work device to steal intellectual data, such as a project's source code.



Reading an executive's email for company information to manipulate the stock market or steal banking information.

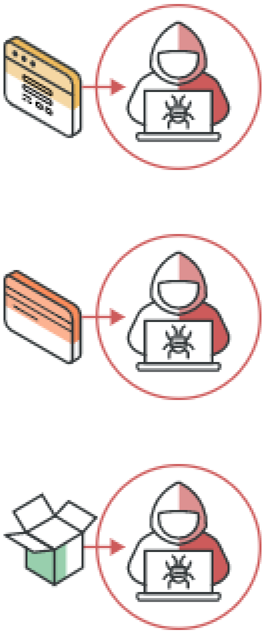
Obtaining credentials or escalating privileges.



Stealing customer data from the server responsible for hosting payment card information (PCI).

Gaining access to some other type of asset or payload.

Regardless of the reason, a bad actor's main objective is to compromise the system and move through a network that contains what they want.



3 Stages of Lateral Movement

There are three stages of lateral movement used in most cyberattacks:

1. **Reconnaissance.** During this initial stage, the attacker explores and maps the business's network, devices, and users. They use this stage to get to know the company's network hierarchies, host naming conventions, various operating systems, location of potential payloads, and further intelligence to make any additional moves throughout the system.
2. **Credential dumping and privilege gathering.** To move through any network with minimal-to-no-detection, a threat actor needs valid login credentials. The commonly used term for illegally obtaining network credentials is "credential dumping." One way cybercriminals do this is by fooling users into sharing their credentials via phishing attacks and typosquatting.
3. **Gaining access to other communication and computing points in the network.** Once inside the network, the attacker can repeat the process of lateral movement, bypassing security controls to thwart and compromise successive devices until ultimately detected and stopped.

What Lateral Movement Does for a Threat Actor During a Cyberattack

Lateral movement gives the threat actor the ability to avoid detection and response by a company's security teams. With this free movement throughout a network and lack of detection, they can retain access, even if the IT team recorded the system's or machine's initial infection.

Lateral movement allows an extended dwell time for the threat actor, allowing them access to a system for weeks or months after the initial breach. It is a trap that gives the company's detection and response team a false sense of security, causing everyone to let their guard down, leaving the system open to data theft.

Detecting Lateral Movement

Lateral movement manifests and presents as obvious, anomalous network activity, making it suspicious to vigilant IT teams right away.

For instance, if a device or computer that usually communicates with a select few other devices and their users starts randomly scanning the network, it is time to take note and prepare to respond. Any activity out of the norm is worthy of a response. Even if it is not a clear lateral movement scenario, it is better to investigate and dismiss it as an organic aberration in the course of business than taking the risk of letting it pass.

It is difficult for cybersecurity teams to detect lateral movement while performing core business and other daily activities. They need a reliable and dynamic application that monitors how their network applications communicate, allowing them to provide vulnerability exposure insights.

With all the necessary observations and information, the application takes control of container software, for example, as well as bare-metal and virtual machines to provide network security to stop threat actors before they gain access, preventing them from lateral movement and administrative privileges.

How to Prevent Lateral Movement

Micro-segmentation is a proven strategy to stop the lateral movement of ransomware and cyberattacks. Segmentation allows you to isolate applications and assets, and prevent ransomware and cybercriminals from spreading through the network.

Illumio Core and Illumio Edge apply Zero Trust segmentation to applications, containers, clouds, data centers and endpoints. Illumio’s approach delivers comprehensive visibility into application dependencies and provides the automated segmentation needed to prevent lateral movement, contain cyberattacks, and protect critical assets.