**What is Lateral Movement?**

Lateral movement is an approach used by attackers to systematically transverse a network to access or damage valuable assets or data.

The attacker uses tools and methodologies to obtain access and [privileges](https://www.cynet.com/network-attacks/privilege-escalation/), which let them move laterally between applications and devices in a network to isolate targets, map the system and ultimately gets to the high-value targets.

**How it works**

Lateral movement tends to take place following the initial compromise of an endpoint or server. This attack methodology requires the additional compromise of user account credentials. Using these account credentials, the attacker attempts to gain [unauthorized access](https://www.cynet.com/network-attacks/unauthorized-access-5-best-practices-to-avoid-the-next-data-breach/) to other nodes.

As an attacker gathers information about the environment, they make parallel attempts to steal credentials, exploit misconfigurations, or isolate software vulnerabilities so they can dig deeper into the network. The attacker then uses lateral movement to control key points in the infected network. These additional positions help the attacker maintain persistence even if a security team detects them on a compromised machine.

**Lateral movement security challenges**

Research shows that attackers spend [80% of an attack](https://www.smokescreen.io/wp-content/uploads/2016/08/Top-20-Lateral-Movement-Tactics.pdf) during lateral movement. While the initial compromise takes place relatively quickly, pivoting from the compromised node to the final goal is a much longer process. The attacker spends most of their time transitioning from the initial breach to the final goal.

Although in the network, during the initial breach the attacker has not yet performed the harmful action for which they infiltrated the target environment in the first place. If you can identify them during this stage, you will likely end the attack. Identifying lateral movement is thus potentially very effective.

However, monitoring internal networks is challenging. Organizations have attempted using, for example, log analysis, machine learning, SIEM’s, and anomaly-based detection. However, due to the sheer volume of data, even the most innovative analytics solutions generate false positives. Consequently, many security teams don’t manage to investigate the large majority of alerts.

## Lateral Movement Techniques

Throughout this article, we will examine several of the lateral movement techniques and illustrate how an attacker can move laterally within a network to obtain information and execute commands. The demonstration will be performed on the MITRE ATT&CK® sub-techniques T1021.002, T1550.002, and T1550.003

### Lateral movement today

Today, lateral movement has been automated and commoditized and as such is often deployed by automated bots and tools.