Where Can Attackers Hide Undetected on Your Network?

Get a Lateral Movement Risk Audit to Gain Visibility

Find Advanced Attackers that Move Laterally

Targeted ransomware, nation-state, and insider attackers are succeeding in executing devastating threats and exploits. Our research shows that attackers will:

- Bypass security controls and gain a beachhead in your environment
- Use unmonitored credential and connection information as a path to critical data
- Evade legacy controls and go unnoticed

We are offering a free Lateral Movement Risk Audit so you can see where your organization is at risk.

The Benefits of Auditing for Lateral Movement Risk

The Lateral Movement Attack Risk Audit is remote, free, and without any post-audit obligation. Get the audit today and you will be given a comprehensive report that will reveal significant issues across your attack surface such as:

- A risk overview by threat vector
- Unmonitored shadow and local admin accounts
- High risk connections to critical IT infrastructure and business assets
- Cached domain admin credentials contained on endpoints
- Improperly disconnected RDP sessions with heightened access
- ...and many more potential lateral movement risks

Integrate Audit Data into Standard Operational Processes

What Our Audits Revealed

1 in 5 endpoints have stored domain admin credentials

70% of endpoints have local admins with group passwords

1 in 10 endpoints have unnecessary connections to crown jewel assets

...all of which give attackers easy access to critical data if not found and removed!

Get started now!

Contact us and we can schedule a time to meet that is convenient for you.