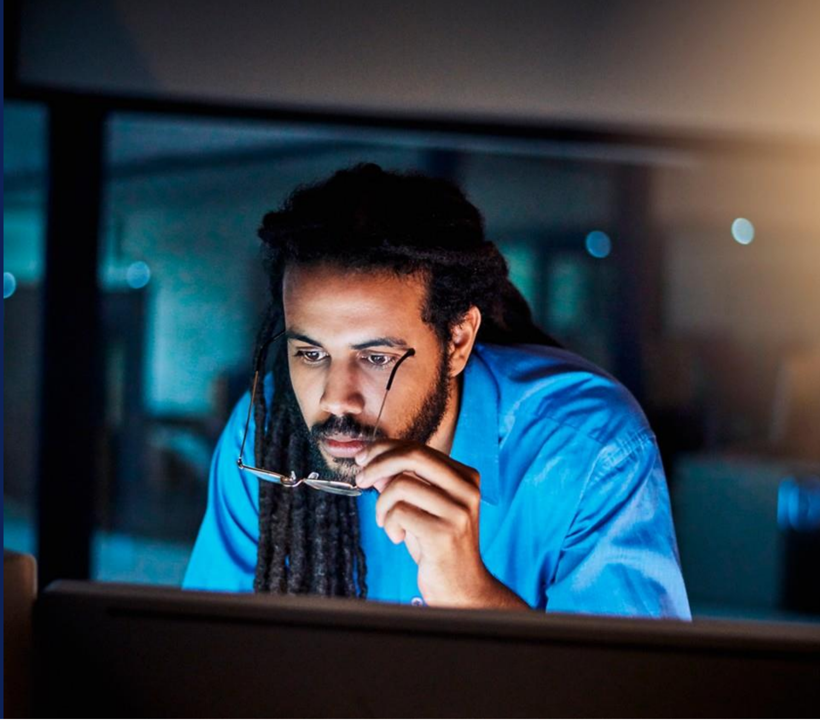
DELL Technologies

## Attack Simulation Management Penetration Testing Services

# Uncover Weaknesses Before Attackers Do



## Dell validates your security controls and policies across the full kill chain

Organizations implement hundreds of security controls, from web gateways to endpoint defenses. These controls are complex and challenging to manage. Even a single misconfiguration creates risk that cybercriminals are quick to exploit.

Challenging and validating your security controls is an effective strategy to mitigate cyber threats. Dell Penetration Testing Services and Attack Simulation Management rigorously evaluate your security controls, mimicking real-world threat tactics—including ransomware attacks—to uncover weaknesses before attackers do.

Each service approaches security with a tailored focus:

- **Attack Simulation Management**: Automated simulations designed to validate whether your security controls can withstand sophisticated threats
- **Penetration Testing Services**: Security experts use the tactics and techniques that attackers use to uncover high-risk pathways, recreating how an attacker, such as a ransomware operator, might target your critical assets.

## Key Benefits

### Attack Simulation Management

- Detect misconfigured security controls that could be exploited, using comprehensive attack simulation technology
- Account for recently emerging issues and gaps with frequent simulations
- Identify gaps in your security controls and policy configurations to prioritize remediation efforts

### Penetration Testing Services

- Inspect high-risk pathways to high-value assets or data
- Insights on novel high-risk threats with ad hoc testing

## Attack simulations test security controls

Dell security professionals use advanced attack simulation technology to test different attack vectors, such as trying to drop malware onto an endpoint or to get unauthorized information to a web server. Dell testers apply attack simulations across the full kill chain[1] against threats, including the latest attacker tactics, techniques and procedures (TTPs). The attack simulation technology is safe for production environments and is continuously updated with the latest threat information, attacks and behaviors.

## Penetration testing assesses pathways to high-value targets

Even with attack simulation, some attackers possess the skills to navigate through the environment, evading obstacles to reach valuable data. That’s where penetration testing comes in to complement attack simulation by focusing on vulnerable or high-risk pathways into an environment. Penetration testers use various threat actor techniques and even different payloads in their effort to reach a specific goal, such as capturing a high value system or stealing or disabling a particular set of files. Like a real attacker, an experienced penetration tester will shift, pivot and adapt techniques to reach the target.

## Attack Simulation Management

- Frequent, automated attack simulations based on customer's environment
- Validate security controls on perimeter and internal infrastructure components including web gateway, email gateway, data exfiltration, endpoint security and immediate threats
- Simulation tool is continuously updated with the latest threat information, attacks and behaviors
- Make alterations to simulation workflow based on previous simulations and security environment factors
- Run ad hoc simulations for newly discovered security issues, based on threat intelligence and Dell's assessment
- Provide an assessment summary to help you identify gaps in your security controls and policy configurations to prioritize remediation efforts
- Available as a 1-yr contract or 30-day health check

## Penetration Testing

- Run penetration tests against a defined set of targets, including artificial intelligence (AI), web gateways, APIs, mobile devices, networks, cloud configurations, web application firewalls and phishing
- Conduct follow-up penetration tests after findings from first test have been resolved (optional)

## Select the Best Fit for Your Organization

For organizations aiming to enhance their security, we offer flexible services to meet diverse needs.

- **Attack Simulation Management** conducts automated, scheduled assessments that mimic real-world threats, helping ensure your security controls are effective.
- **Penetration Testing Services** is a hands-on, expert-led service identifying critical gaps in your environment.
- For comprehensive coverage, **Pen Testing and Attack Simulation Management** combines the strengths of both solutions, delivering continuous validation alongside deep-dive testing. Together, these services help you confidently identify risks and strengthen your security posture.[2]

[1] "Full kill chain" – includes external threats including phishing, Web gateways, etc., compromising endpoints, lateral moves to gain credentials or spread the attack, data exfiltration, etc.
[2] Some features available in the individual offers may not be included in the combined solution.

Explore Dell Security and Resiliency Services

Contact a Dell Technologies expert

Join the conversation with #DellTechnologies