# Validate security controls and policies to close attack vectors

Simulate attacker techniques for initial access, malicious file execution, data theft and more

## Pen Testing and Attack Simulation Management

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

Organizations have hundreds of security controls, from endpoints to web and email gateways. Controls are often complex and difficult to manage, and a misconfiguration can lead to risky exposure. Threat actors look to exploit broken or out-of-date controls.

To challenge and validate the effectiveness of your security controls, Dell Pen Testing and Attack Simulation Management closely mimics real-world threat actions.

The service combines:

- monthly automated breach and attack simulations (BAS) to confirm that your controls are working properly
- an annual penetration test, where skilled experts attempt to breach defenses for critical assets and data

### Attack simulations test security controls

Dell security professionals use advanced BAS technology to test different attack vectors, for example trying to drop malware onto an endpoint or to get unauthorized information from a web server. Dell testers apply BAS to simulate attacks across the full kill chain[1] against threats, including the latest attacker TTPs[2].

The BAS technology is safe for production environments and is continuously updated with the latest threat information, attacks and behaviors.

### Pen 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.

### Key benefits:

- Detect misconfigured security controls that could be exploited, using comprehensive breach and attack simulations
- Account for recently emerging issues and gaps with monthly simulations
- Closely inspect high-risk pathways to high-value assets or data with annual pen testing
- Report test results, quarterly trends and notable activity to help you improve security posture
- Get quick insight on novel high-risk threats with ad hoc testing

Penetration testing complements BAS – rather than testing individual controls or sets of controls, pen testing focuses on vulnerable or high-risk pathways into an environment. Dell pen testers can emulate 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 pen tester can shift, pivot and adapt techniques to reach the target.

## Apply test information to improve security posture

Dell Technologies Services will provide monthly reporting of the security control issues to be corrected based on the results from running the BAS sequences. On a quarterly basis, Dell will review the trends from the various attack simulations, report notable activity observed within your IT environment, and discuss recommendations for improving your security posture.

## Key Features

### Breach and Attack Simulation (BAS)

- Run automated breach and attack simulations monthly according to customer's environment
- Validate security controls on perimeter and internal infrastructure components including web gateway, email gateway and endpoints
- Update BAS tool continuously 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

### Penetration Testing

- Run annual penetration test against defined subset of Web gateways, APIs, mobile devices, external IP addresses, internal IP addresses, cloud configurations
- Re-run pen test after findings from first test are fixed (optional)

### Reporting and Review

- Provide monthly reporting on conducted breach and attack simulations
- Deliver quarterly report and review of trends and notable activity observed within customer's IT environment
- Make recommendations to improve overall security posture

### Onboarding

- Conduct service initiation meeting
- Review pre-engagement checklist completed by customer
- Review customer IT environment
- Activate BAS application for customer
- Provide agent rollout assistance

# Contact your sales representative today.

[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]"TTPs" – tactics, techniques and procedures



DELL Technologies