The Challenge of Vulnerability Management

Vulnerability Assessment (VA) is considered a security best practice and is an important part of any modern security program. However, an increasingly mobile enterprise with a proliferation of transient devices, coupled with the speed of today’s targeted attacks, has created new challenges for vulnerability management programs. VA systems by themselves are unable to address the following challenges:

- VA systems typically do periodic scanning and provide a snapshot of an organization’s risk posture at a given point in time. Thus, the information gathered may not be valid between scheduled scans. This leaves organizations blind to risks that have emerged since the last scan.
- With an increasing number of transient devices, many endpoints may not be assessed for vulnerabilities and risks because they are offline or off-premises during scheduled scans. As a result, the vulnerability assessment report can be incomplete.
- By themselves, VA systems are not meant to take action or mitigate security risks. Thus they only provide vulnerability information, leaving remediation and risk mitigation to other systems or human intervention. This can leave organizations with large windows of exposure to malware, targeted attacks and data breaches.

ForeScout Integration with Vulnerability Assessment Systems

ForeScout CounterACT™ gives you real-time visibility into the devices, users, applications and operating systems on your network, and enables you to mitigate endpoint security deficiencies and cyber threats. CounterACT’s built-in policy engine can flexibly enforce network and endpoint controls based on the intelligence it gathers, or information from a third-party product such as a VA system. CounterACT appliances deploy out of band and work in heterogeneous, multi-vendor network environments, without the need for agents.

CounterACT communicates bi-directionally with VA systems through ForeScout’s Vulnerability Assessment Integration Module. CounterACT detects devices they moment they connect to the network and informs the VA system. This enables several unique capabilities:

- CounterACT can trigger the VA system to perform a real-time scan of the connecting device when it joins the network. This significantly increases the chance of catching transient endpoints while they are on the network and helps produce more up-to-date and complete vulnerability reports.
- Highly security conscious organizations want to confirm an endpoint’s risk posture before it gets access to the network. In such cases, CounterACT can isolate the connecting device in an inspection VLAN while the VA system performs a scan. If the endpoint’s risk rating, as determined by the VA system, is below a configured level, CounterACT can admit the endpoint to the production network.
- CounterACT can trigger VA scans on devices that meet certain policy conditions, such as endpoints with specific applications, or when endpoint configuration changes are detected.

ForeScout Highlights

- **More Timely Vulnerability Assessments**
  Gain more up-to-date information about the risks and vulnerabilities on your network by triggering vulnerability assessment scans when devices join the network.

- **More Complete Vulnerability Reports**
  Make your vulnerability assessment programs more comprehensive by including transient devices that may be missed by periodic scans.

- **Faster Risk Mitigation**
  Reduce exposures and mitigate risks by enabling CounterACT to limit network access or quarantine endpoints that are determined to be high risk by the vulnerability assessment system.

- **Automated Remediation**
  Initiate automated remediation, based on policy, to fix security gaps on endpoints that are determined to be high risk by the vulnerability assessment system.
After the VA system scans a device, CounterACT can obtain the scan results, and initiate risk mitigation actions if vulnerabilities are detected. Based on policy, CounterACT can flexibly and seamlessly enforce controls with a level of response appropriate to the issue at hand. For example, CounterACT can quarantine endpoints with critical vulnerabilities, initiate built-in remediation actions, or trigger external remediation via patch management and other IT systems.

Through this integration, you gain:

- more up-to-date information about the vulnerabilities on your network
- more comprehensive information about the vulnerable endpoints on your network
- automated remediation and faster mitigation of risks on your network

The Vulnerability Assessment Integration Module is just one of many IT system integrations that are available within the ForeScout ControlFabric™ architecture. For more information on the ForeScout ControlFabric architecture and how ControlFabric can help IT security managers easily share information among security products and quickly respond to security issues, visit www.forescout.com/controlfabric.

**Supported Vulnerability Assessment Systems**

Products supported by the Vulnerability Assessment Integration Module include McAfee Vulnerability Manager (MVM) and Tenable Nessus.

For details on our licensing policy, see www.forescout.com/licensing.