Continuous, Comprehensive Monitoring
Move to real-time vulnerability management with always-on discovery and integrated risk assessment

Key Challenges
Unknown, unscanned assets create unknown, unmitigated risk. Today’s scanning models fall short:
• Many unknown devices and virtualized infrastructure are already in place and vulnerable on each network
• Every day brings more personally owned devices that access and leave the network between scheduled scans
• Neither active nor passive discovery alone will discover 100 percent of all devices

“Only one in 10 companies considers itself to be fully aware of all devices attaching to their networks.”
CompTIA as quoted in Denver Business Journal

Scheduled asset and vulnerability scans are convenient, predictable—and flawed. For every 10 corporate-owned systems you know about and regularly scan for vulnerabilities, another three typically lurk in the shadows of your network. These unseen open doors include smartphones, tablets, printers, Wi-Fi access points, Apple computers, applications, databases, and guest images on virtualized systems. Unknown and unmanaged, they serve as the entry point for attacks on vulnerable software that could lead to data theft and network disruption.

Consumer pricing and development schedules are driving unprecedented proliferation of IP-enabled devices, so there will be more assets attaching to your network tomorrow than there were last week. The term “asset” can encompass laptops, tablets, mobile phones, databases, applications, and virtualized desktops. Whether purchased by the company or by the user, assets can become a risk for IT to manage.

The explosion in physical and virtual systems attaching to your network means more opportunities for problems and less time to keep problems from becoming disasters. When employees carry their personal devices into the office, they aggravate risks already in place due to the limited coverage of most vulnerability management processes. There are too many devices being scanned too infrequently by inadequate scanning systems.

While managed systems may be required to have antivirus, firewalls, device controls, encryption, and data loss prevention software, unmanaged and unknown devices are free to wreak havoc on your infrastructure and your compliance program. Unknown devices on your network can introduce data-stealing malware, provide vulnerabilities for a hacker to exploit, or download content that departs with the employee or visitor. An unknown, noncompliant system can go unremediated forever. Enterprises must adapt their vulnerability management models to deliver continuous visibility into the vulnerability of new devices and potential impact of emerging threats. Up-to-date information guides mitigation of changing risks.

Active Scanning a Partial Solution
Most enterprises meet security and compliance requirements for vulnerability assessment by deploying active scanning systems that detect and explore assets attached to the network. These systems scan based on IP addresses to learn what they can about each device’s hardware and software. However, these traditional active scans have limitations that create gaps in coverage and compliance.

Intrusive scanning body
Active scanning can put a load on the network and scanned devices that many users see as inhibiting their ability to get work done. As a result, administrators schedule scans for low usage periods, such as nighttime and weekends.
Missed devices
It’s common for devices to miss a scheduled scan through being shut down (in support of green initiatives), off the network, only briefly active, or hidden by network obstacles, such as network firewalls, host-based firewalls, load balancers, and network address translation (NAT) devices. These network elements prevent the scanner from probing the full range of targeted IP addresses. As a result, network devices in these ranges can remain unscanned, and any compliance report is imperfect.

Mystery devices
In a “scheduled scan” model that scans on weekends, an employee can bring in a laptop, tablet, or Wi-Fi access point on a Monday morning and take it home on Friday afternoon without IT ever detecting or scanning it. That’s not unusual for employees that work from home or the road and contractors working sporadic assignments. Even daily scans miss a device a guest carries into and out of the enterprise within a day.

Virtualization
Virtualization adds another deep wrinkle to vulnerability management. If a known device is scanned on Sunday mornings, but the virtual machine is not running, can IT discern anything about the true vulnerability of the user’s environment? What it can see is compliant, but what about the virtual world?

False confidence
When the scheduled scan eventually executes, it may complete successfully because all known devices were scanned and compliant. But that’s not where the real risk lies. The scan doesn’t reveal that missed or mystery devices were ever present. Any viruses that mystery systems carry in, any patches they miss, and any databases they take home go undetected.

Breaking threats
Across these issues, risks change quickly. Each vulnerability in Adobe, Microsoft, Oracle, or Google Android is a potential problem, one that may go unmitigated between scheduled scans unless the administrator recognizes that the issue might affect known assets and does an ad hoc scan.

Passive Network Monitoring Is a Partial Solution
Passive scanning, which monitors network traffic, provides a way to fill in some of the gaps left by active scanning, but is not by itself a panacea. In scanning network traffic, it can pick up information about which devices are present and active on a network, seeing information up the entire TCP/IP stack and detecting “mystery” devices. However, it will miss idle assets and assets configured to bypass the monitoring point. It also may not be able to penetrate encrypted traffic or dig into the hardware and software on a given device to catalog its vulnerabilities and compliance.

Discover, Evaluate, Act
For full coverage and reliable audit results, passive and active discovery and monitoring technologies should be combined with risk-based scanning systems for instant detection, triage, and risk-based remediation. Continuous monitoring of activities on the network should reveal new assets as they connect. An initial lightweight scan of any new device can determine whether more investigation is required. Based on rules and policies, the system can then automatically instigate a more intensive scan. In seconds, an administrator can receive a detailed evaluation of risk to guide prioritization and remediation. This combined, real-time scanning approach permits more complete, accurate, and fine-grained vulnerability management.
Asset or liability?
Discovering and characterizing assets in real time is the key to managing risk without weighing down the network. An instant lightweight assessment can determine if assets on your network are at risk, perhaps through missing patches, or if they are creating a vulnerability for your company’s security, as is common with devices that can install apps and content from the Internet.

Urgent or benign?
As you detect new assets for evaluation, you should determine how urgent a problem your business is facing. Printer malware is a genuine issue, but not cause for a red alert. A noncompliant laptop running a copy of your company’s customer database, however, could merit an immediate office visit from the local administrator.

Mitigate or remediate?
An accurate and detailed inventory of all assets allows you to know how breaking threats affect your devices and systems. Perhaps you get an emergency vulnerability bulletin from a key vendor. Some issues can be ignored where countermeasures in the network or on the system provide sufficient protection. Other issues may need an active response, such as a software update, a new firewall rule, a device quarantine, or a visit.

Go Real Time Today
Instead of the incomplete coverage of a scheduled, static scanning model, your enterprise can adopt continuous and integrated processes that provide comprehensive asset coverage within a dynamic, responsive vulnerability management approach. With near real-time asset discovery, evaluation, and incident response, your team will have a risk management posture that matches today’s expanding threats, devices, and governance expectations.

About McAfee Security Management Solutions
The extensive McAfee® product portfolio integrates and automates products to drastically improve situational awareness and optimize risk management while lowering total cost of ownership. Unlike traditional vulnerability assessment products, McAfee Vulnerability Manager uses a combination of passive and active techniques to expand coverage to all devices at all times. This continuous asset monitoring integrates with industry-leading vulnerability scanning and incident management workflows to enable continuous asset compliance. Learn more at www.mcafee.com/vm.

“Vulnerability scanning is a critical part of a vulnerability management process, but vulnerability assessment (VA) scanning must be augmented with other technologies and analytics for enterprises to realize effective protection from advanced targeted threats. Deployment options, assessment of virtual and mobile technologies, flexible analysis and reporting, and integration with other security technologies and IT management products and processes should be key criteria when selecting a vulnerability assessment vendor.”

—Kelly M. Kavanagh,
Gartner G00230435