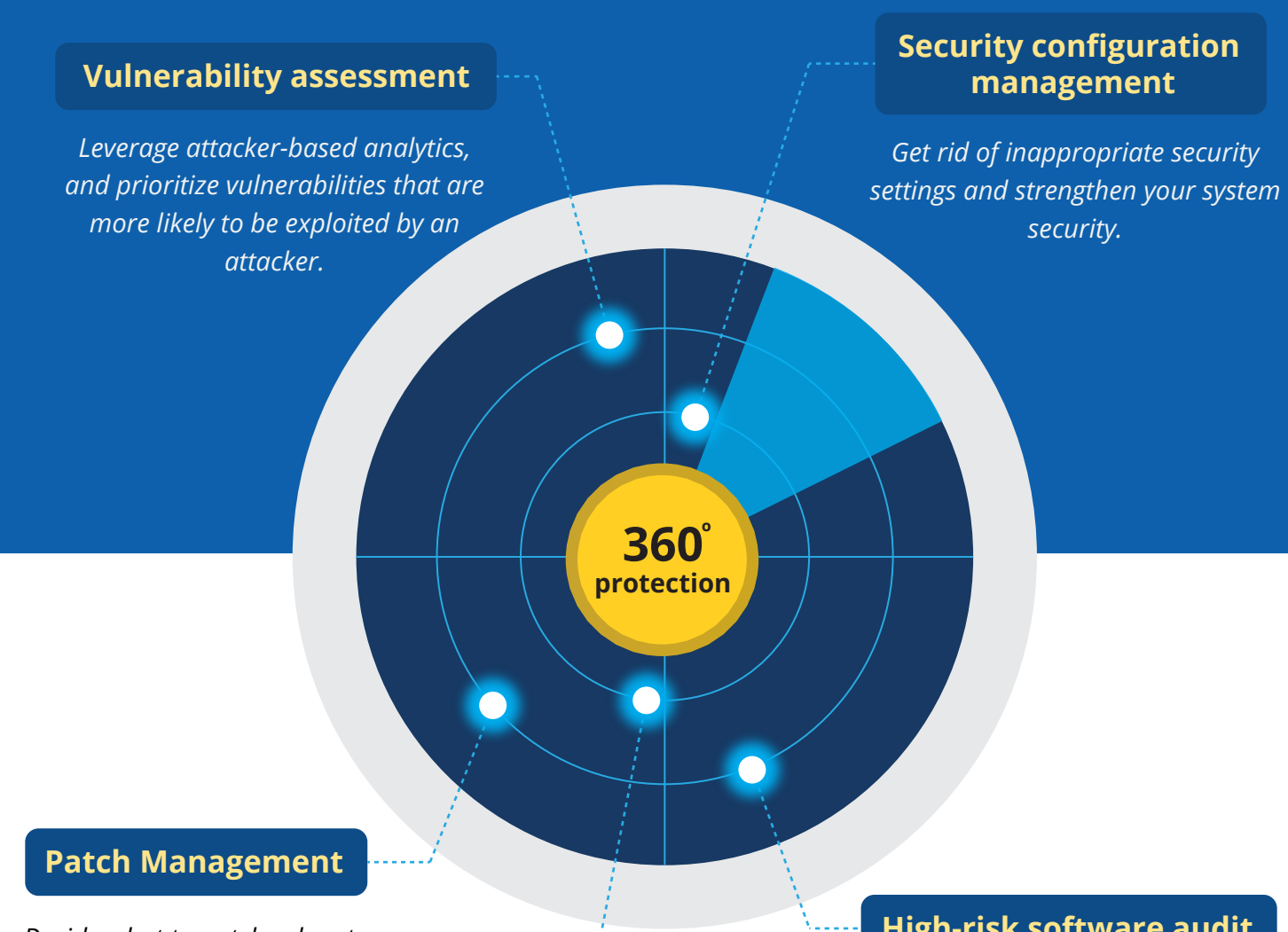
ManageEngine
Vulnerability Manager Plus

Datasheet

Reduce your attack surface with proactive vulnerability management



Today's challenge

Gartner predicts that "**99 %** of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident."Lack of awareness and the absence of a centralized way to facilitate cyberhygiene have made many organizations vulnerable to cyberattacks. On top of that, **22,316** new security loopholes were disclosed in 2019, and over one-third of them had an exploit available. With these numbers soaring, organizations need to implement a strategic approach for prioritizing and managing vulnerabilities, because not all vulnerabilities pose equal risk.

The Solution

ManageEngine Vulnerability Manager Plus is prioritization-focused vulnerability management software for enterprises, offering built-in patch management. It's a strategic solution for your security teams, delivering comprehensive visibility, assessment, and remediation of threats and vulnerabilities across all your IT assets—servers, desktops, laptops, virtual machines, DMZ servers, and roaming devices—from a single console.

Detects vulnerabilities in **800+** applications.

Supports **18** languages.

1st ever vulnerability management solution with automated patching.

Scales to **50,000** computers.

Fully functional, **30-day** free trial.

How Vulnerability Manager Plus reinforces the security stance of your network

Vulnerability assessment

- Identify vulnerabilities along with their context, such as CVSS and severity scores, to ascertain priority, urgency, and impact.
- Stay aware of whether exploit code has been publicly disclosed for a vulnerability.
- Keep tabs on how long a vulnerability has resided in your network.
- Filter vulnerabilities based on impact type and patch availability.
- Gain recommendations on high-profile vulnerabilities procured based on above risk factors.
- Leverage a dedicated tab on publicly disclosed and zero-day vulnerabilities, and utilize work-arounds to mitigate them before the fixes arrive.
- Isolate and identify vulnerabilities in critical assets, namely databases and web servers that hold critical data and perform crucial business operations.

Security Configuration management

- Identify misconfigurations in operating systems, applications, and browsers, and bring them back to compliance.
- Audit your firewalls, antivirus, and BitLocker status.
- Prevent brute-force attempts by enforcing complex password, account lockout, and secure logon policies.
- Make sure memory protection settings, such as Structured Exception Handling Overwrite Protection, Data Execution Prevention, and Address Space Layout Randomization, are enabled.
- Put an end to legacy protocols with risks that outweigh the benefits.
- Manage share permissions, modify user account controls, and disable legacy protocols to reduce your attack surface.
- Safely alter security configurations without interrupting business operations by reviewing critical deployment warnings.

Automated patch management

- Automatically correlate vulnerability intelligence and patch management.
- Automate patching for Windows, macOS, Linux, and over **300 third-party** applications.
- Customize deployment policies for hassle-free deployment. Test and approve patches before rolling them out to production machines.
- Decline patches to specific groups.

Web server hardening

- Continuously monitor your web servers for default and insecure configurations.
- Analyze web server misconfigurations based on context, and gain security recommendations.
- Ensure SSL certificates are configured and HTTPS is enabled to secure the communication between clients and servers.
- Verify whether the server root directory permissions are restricted to prevent unauthorized access.

High-risk software audit

- Stay vigilant of legacy software that has or is about to reach its end of life.
- Obtain real-time information on peer-to-peer software and remote sharing tools that are deemed unsafe, and eliminate them with just the click of a button.
- Gain continuous visibility over the active ports in your systems, and sniff out instances where a port has been activated by malicious executables

Compliance with CIS benchmarks

- Helps audit and maintain compliance with over 75 CIS benchmarks.
- Automate audits on multiple assets against multiple CIS benchmarks at once.
- Gain detailed remediation for every violation.

Agent Hardware Requirements

Processors	Processor Speed	RAM Size	Hard Disk Space
Intel Pentium	1.0 GHz	512 MB	100 MB

Server Hardware Requirements

Number of managed devices	Servers used	Processor	RAM	Hard disk space
1 to 250	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.0GHz 3MB cache	2GB	5GB
251 to 500	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.4GHz 3MB cache	4GB	10GB
501 to 1,000	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.9GHz 3MB cache	4GB	20GB
1,001 to 3,000	Vulnerability Manager Plus Server	Intel Core i5 (4 core/4 thread) 2.3GHz 6MB cache	8GB	30GB
3,001 to 5,000	Vulnerability Manager Plus Server	Intel Core i7 (6 core/12 thread) 3.2GHz 12MB cache	8GB	40GB
	SQL Server	Intel Core i7 (6 core/12 thread) 3.2GHz 12 MB cache	8GB	30GB
5,001 to 10,000	Vulnerability Manager Plus Server	Intel Xeon E5 (8 core/16 thread) 2.6GHz 20MB cache	16GB	60GB
	SQL Server	Intel Xeon E5 (8 core/16 thread) 2.6GHz 20MB cache	16GB	40GB
10,001 to 20,000	Vulnerability Manager Plus Server	Intel Xeon E5 (8 core/16 thread) 2.6GHz 40MB cache	32GB	120GB
	SQL Server	Intel Xeon E5 (12 core/24 thread) 2.7GHz 30MB cache	32GB	80GB

If you're managing more than 1,000 computers, we recommend you install Vulnerability Manager Plus on a Windows Server machine.

Software Requirements

Supported OS for Server
Windows 7 / 8 / 8.1 / 10 / Servers 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

Supported OS for Agents

Windows OS	Windows Server OS	Mac OS	Linux OS
Windows 10	Windows Server 2016	10.15	Ubuntu 10.04 & later
Windows 8.1	Windows Server 2012 R2	10.14	Debian 7 & later
Windows 8	Windows Server 2012	10.13	CentOS 6 & 7
Windows 7	Windows Server 2008 R2	10.12	Red Hat 6 & 7
Windows Vista	Windows Server 2008	10.11	SUSE Enterprise Linux 11 & later
Windows XP	Windows Server 2003 R2	10.10	
	Windows Server 2003	10.9	
		10.8	

Pricing

Free edition
Complete vulnerability management for 20 workstations and 5 servers

Professional edition
Starts at $695/year for 100 computers.

Enterprise edition
Starts at $1,195/year for 100 computers.

For more details

www.vulnerabilitymanagerplus.com
vulnerabilitymanagerplus-support@manageengine.com
Toll free: **+1-888-720-9500**

ManageEngine
IT Management, Simplified