ManageEngine

IT management, simplified

Real-time IT management solution for the new speed of business

ManageEngine

Enterprise IT management software division of Zoho Corporation

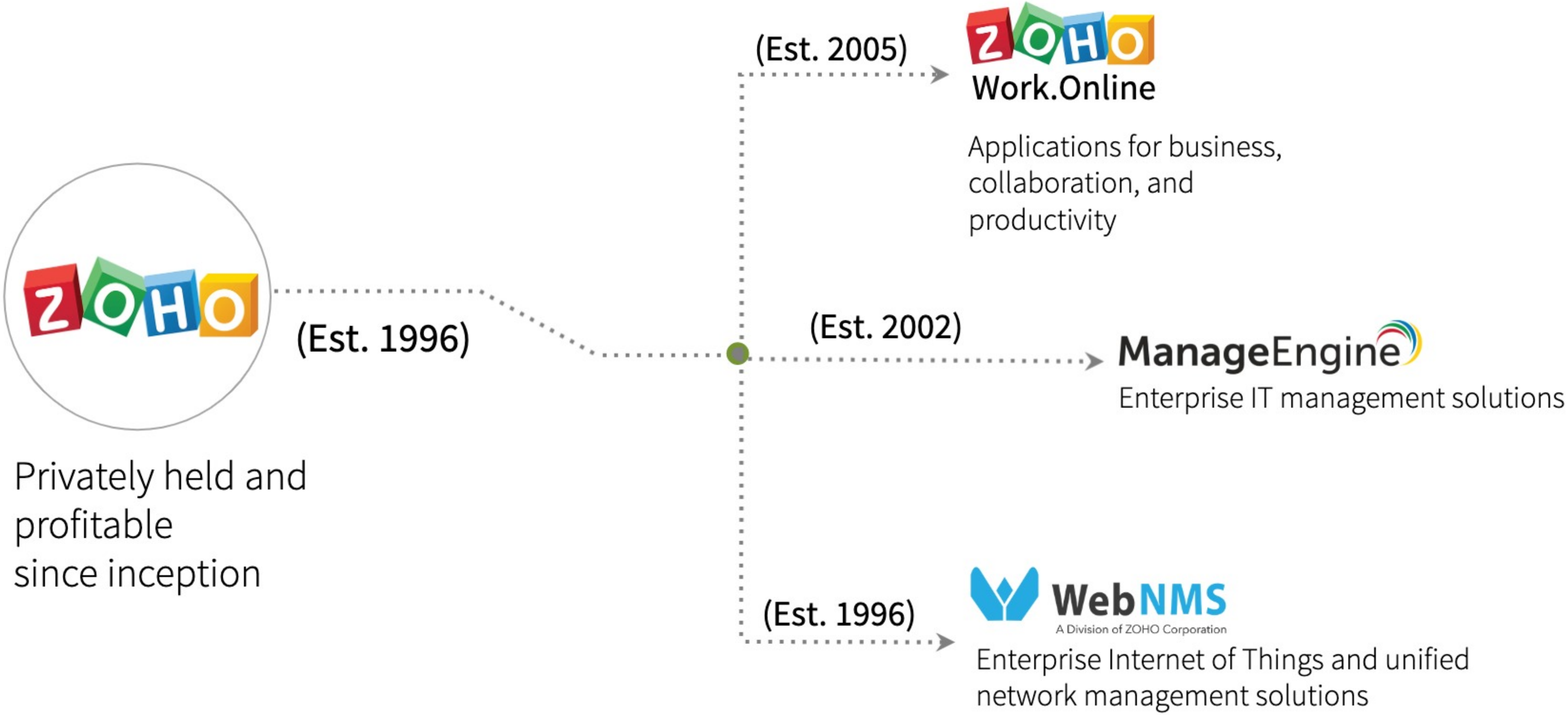
Founded in 1996 as AdventNet

Privately held, rock- solid supplier and partner

Headquartered in Pleasanton, California

Millions of customers across industries

ManageEngine: The enterprise IT management division of ZOHO Corporation



(Est. 1996)

Privately held and
profitable
since inception

(Est. 2005)

Applications for business,
collaboration, and
productivity

(Est. 2002)

Enterprise IT management solutions

(Est. 1996)

Enterprise Internet of Things and unified
network management solutions

ManageEngine **solutions**

Active Directory Management

Active Directory
Exchange Server
Self-service portal
Recovery and backup

Endpoint management

Desktop management
Mobile device management
OS deployment
Patch management
Browser management

IT service management

Help desk
Asset life cycle
CMDB and ITIL
Customer support

IT operations management

Network performance
Application performance
End-user experience
Network change and configuration
Converged infrastructure
Storage infrastructure
Bandwidth and traffic
SQL server monitoring

On demand

Application performance
Helpdesk software
Active Directory recovery and backup
Mobile device management
Patch management
Log management

IT security

Log management
Firewall analysis
Vulnerability analysis
Privileged password
Network anomaly detection

2 million users

3 of every **5** Fortune **500 companies** are ManageEngine customers

Standard Chartered

GE

BARCLAYS

L'ORÉAL

SAINT-GOBAIN

JPMORGAN CHASE & CO.

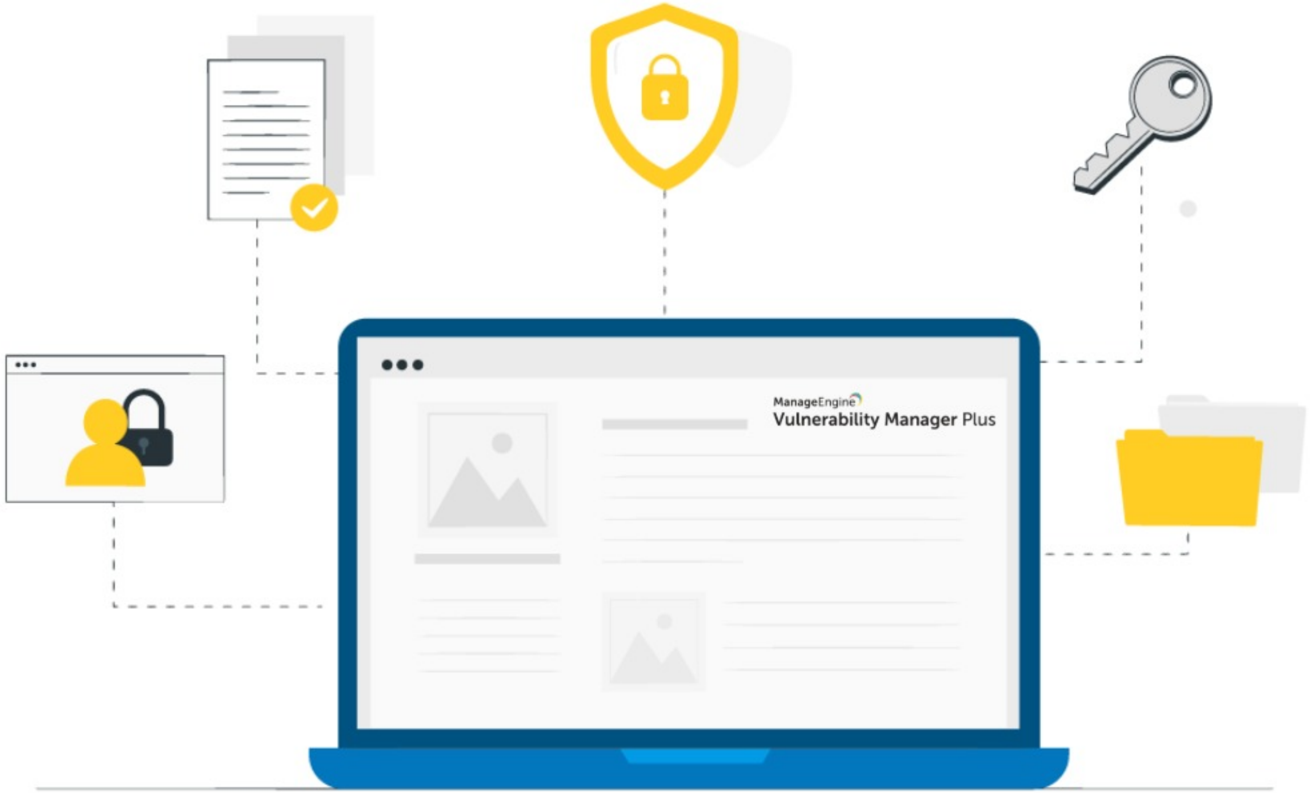
AT&T

ManageEngine

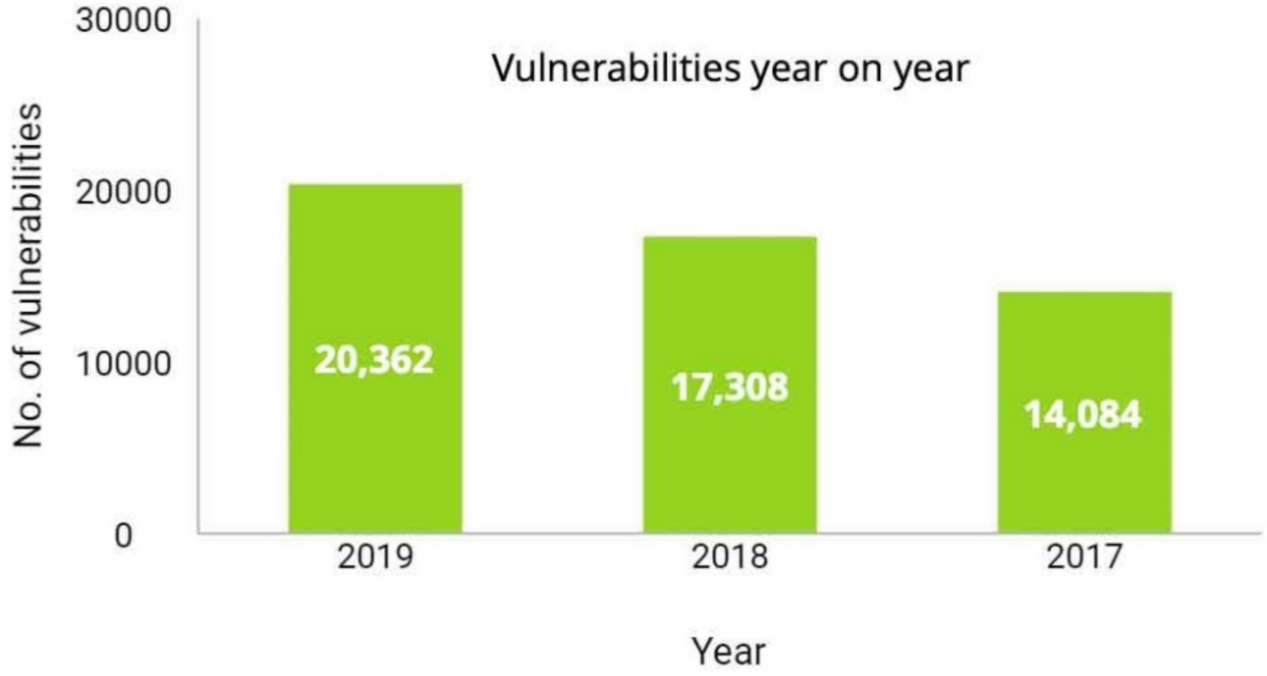
Vulnerability Manager Plus

Prioritization-focused threat and **vulnerability management software** offering built-in patching for enterprises

Why do you need **vulnerability management?**



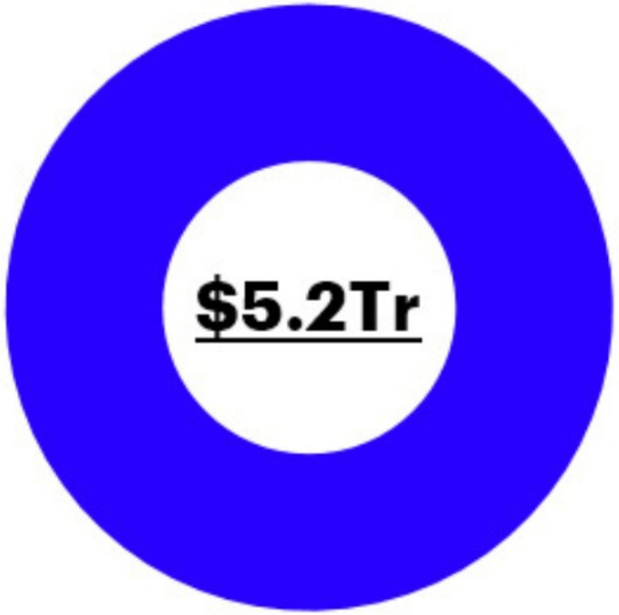
Vulnerabilities are always **on the rise**

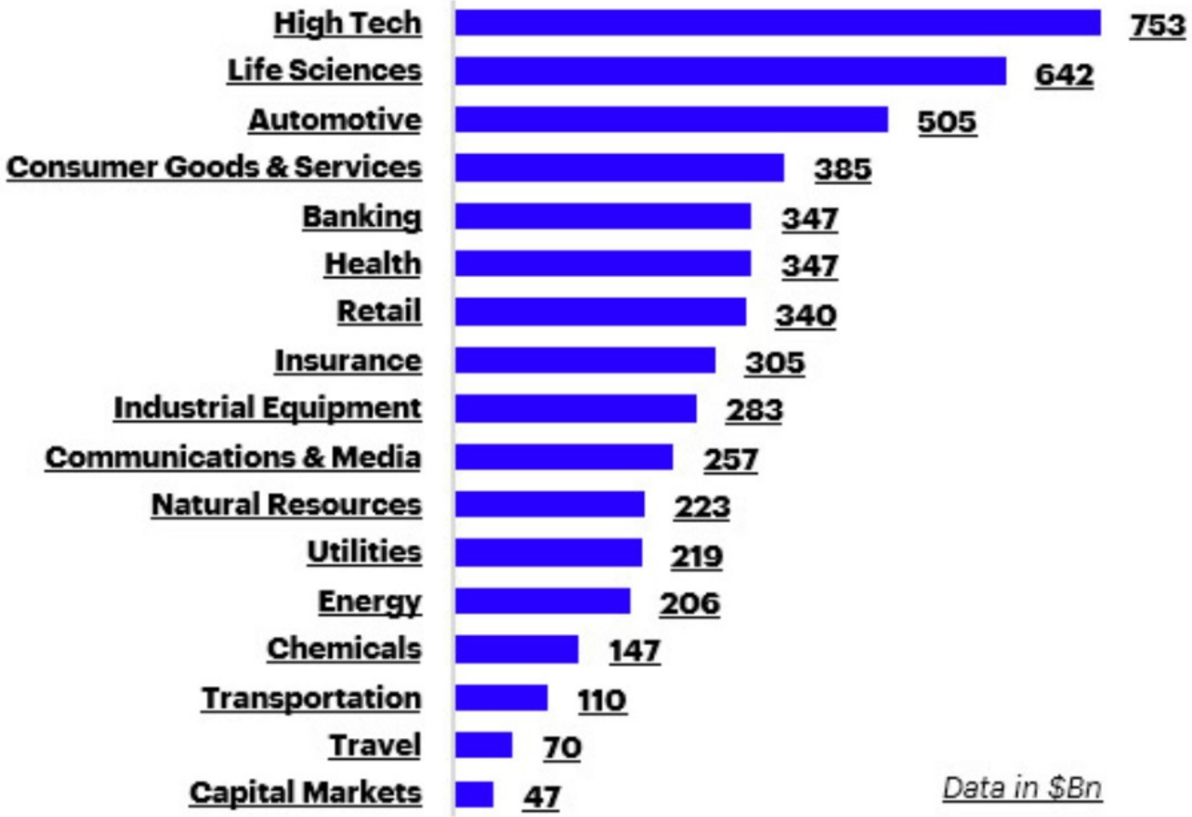


47 percent of these vulnerabilities had a public exploit available

Security Boulevard's report on the state of vulnerabilities in 2019

Negligence in **securing your endpoints could** cost you dearly





- Expected foregone revenue cumulative over the next 5 years. Calculations over a sample of 4,700 global public companies
  Source: Accenture Research

Roadblocks to effective **vulnerability management**

- Too many vulnerabilities with varying risks
- Lack of time, resources, and central means to stay on top of vulnerabilities dispersed across a heterogenous, distributed network
- Juggling multiple tools for vulnerability assessment and patch management, resulting in a fragmented and inefficient workflow
- Inability to track and remediate misconfigurations and other security loopholes
- Occasional scanning results in security lapses

How Vulnerability Manager Plus works

Scan

Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.

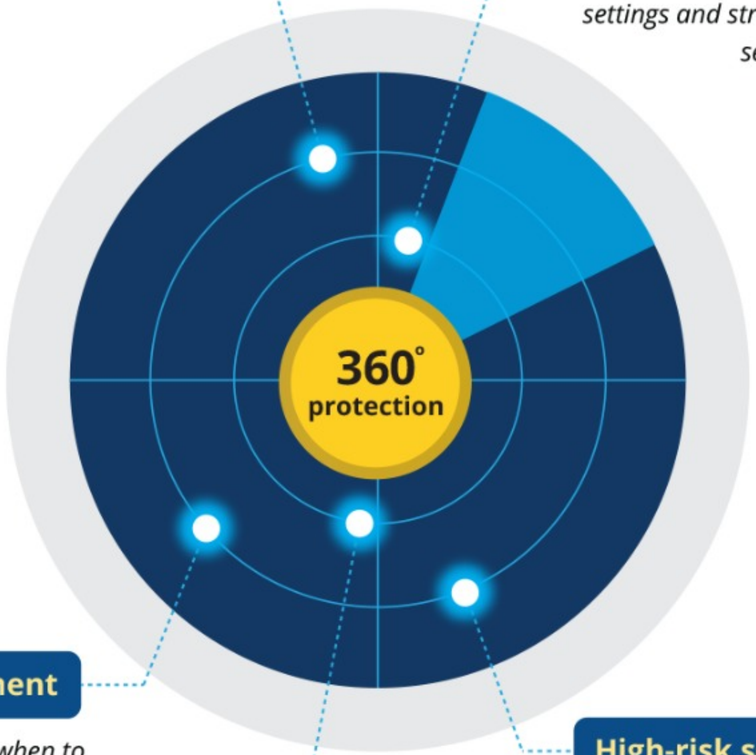
Assess

Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.

Manage

Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.

Features: Sneak peek



Vulnerability assessment

Leverage attacker-based analytics, and prioritize vulnerabilities that are more likely to be exploited by an attacker.

Security configuration management

Get rid of inappropriate security settings and strengthen your system security.

Patch management

Decide what to patch, when to patch, and how to patch. More importantly, automate it.

High-risk software audit

Audit and eliminate unauthorized, unsupported software in your network with just a click of a button.

Web server hardening

Safeguard your internet facing servers from many attack variants like XSS, Clickjacking, etc.

Prioritize what to patch with **comprehensive vulnerability assessment**

- Identify vulnerabilities along with their context, such as CVSS and severity scores, to ascertain priority, urgency, and impact
- Know 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

Establish a secure foundation with **security configuration management**

- Identify misconfigurations in operating systems, applications, and browsers, and bring them back under 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 with 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

Intelligent reports

- Executive reports
  - Executive asset summary
  - Executive vulnerability summary
  - Executive patch summary
  - Threat priority report
- More than 10 pre-defined reports available in PDF, CSV, and XLSX formats
- Schedule reports
- Custom query reports

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

Audit high-risk software and active ports

- Stay vigilant of legacy software that has or is about to reach 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

How does Vulnerability Manager Plus benefit your organization?

- Early identification of imminently exploitable threats that require little to no user intervention
- Reducing the effort spent in vulnerability management with a central console and insightful dashboards
- Eliminating the need for investing in separate patch management tools
- Avoiding hefty fines by conforming to cybersecurity compliance and regulations
- Flexible and easy to use

Deployment options

On-premises

Also hosted on:

awsmarketplace

Azure
MARKETPLACE

Awards and recognition

TOP NETWORK SECURITY SOFTWARE
goodfirms.co

RISING STAR
2019

CERTIFICATE
GREAT USER EXPERIENCE

crozdesk
TRUSTED VENDOR
HIGH MARKET PRESENCE
2020

crozdesk
QUALITY CHOICE
TOP RANKED SOLUTION
2020

VERIFIED QUALITY
FinancesOnline.com

Available in **3 editions**

01

Free Edition

Up to 25 computers

- Suitable for SMBs
- Fully functional
- Up to 25 computers

02

Professional

suitable for computers in LAN

- Vulnerability scanning and assessment
- System misconfiguration detection
- High-risk software detection
- Detection and resolution of server misconfigurations
- Vulnerability reports

03

Enterprise

suitable for computers in WAN

Professional Edition features +

- Secure configuration deployment
- Automated Patch deployment
- Test and approve patches
- High-risk software uninstallation
- Zero-day vulnerability mitigation

Useful **resources**

- Pricing and store
- System requirements
- Architecture
- User guide
- FAQs
- Free trial

Learn more

https://www.manageengine.com/vulnerability-management/

Try it for free!

https://www.manageengine.com/vulnerability-management/download.html