What Is IT Security?

IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

- Watch overview (2:17)
- Small Business Cyber Security

- How IT Security Works
- Types of IT Security
- Related Topics

Contact Cisco

What is the need for IT security?

As hackers get smarter, the need to protect your digital assets and network devices is even greater. While providing IT security can be expensive, a significant breach costs an organization far more. Large breaches can jeopardize the health of a small business. During or after an incident, IT security teams can follow an incident response plan as a risk management tool to gain control of the situation.

What is the difference between IT security and information security (InfoSec)?

Although IT security and information security sound similar, they do refer to different types of security. Information security refers to the processes and tools designed to protect sensitive business information from invasion, whereas IT security refers to securing digital data, through computer network security.

What are the threats to IT security?

Threats to IT security can come in different forms. A common threat is malware, or malicious software, which may come in different variations to infect network devices, including:

- Ransomware
- Spyware
- Viruses

These threats make it even more important to have reliable security practices in place. Learn more about malware to stay protected.

How do I benefit from IT security?

IT security prevents malicious threats and potential security breaches that can have a huge impact on your organization. When you enter your internal company network, IT security helps ensure only authorized users can access and make changes to sensitive information that resides there. IT security works to ensure the confidentiality of your organization’s data.

Types of IT security

Network security

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability, reliability, and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users’ ability to access or use the network.

Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to public cloud.

Internet security

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls, antimalware, and antispyware.

Endpoint security

Endpoint security provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and desktop computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

Cloud security

Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. Cloud security can help secure the usage of software-as-a-service (SaaS) applications and the public cloud. A cloud-access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

Application security

With application security, applications are specifically coded at the time of their creation to be as secure as possible, to help ensure they are not vulnerable to attacks. This added layer of security involves evaluating the code of an app and identifying the vulnerabilities that may exist within the software.

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Information Security Functions & Responsibilities

Information Security Mission

The mission of Information Security is to design, implement and maintain an information security program that protects the Medical School's systems, services and data against unauthorized use, disclosure, modification, damage and loss. The Information Security Department is committed to engaging the Medical Schhol community to establish an appropriate information security governance structure that enables collaboration and support for new information security initiatives.

Information Security Approach

- Foster a culture of empowerment, accountability and continuous improvement
- Demonstrate a consistent Information Security and Compliance message through effective communication and partnerships
- Prioritize information assets and processes

- Strive to influence positive and meaningful change within IT and UMass Chan as a whole
- Identify and prioritize risks
- Implement foundational security controls across key assets
- Build a targeted security capability model
- Develop the security improvement roadmap
- Ensure governance and organization engagement

Information Security Scope

- Protect the assets of the Medical School through secure design, operations and management governance
- Align work and work products within UMass Chan-relevant laws, regulations and requirements
- Apply a risk-based approach to our security design, guidance and decisions
- Continuously safeguard against current and potential threats

Information Security Importance

The importance of a proactive Information Security team is to provide the framework for keeping sensitive data confidential and available for authorized use while building effective relationships with our business and IT partners.

Information Security Principles and Goals

- Protecting the confidentiality of data
- Preserving the integrity of data
- Promote the availability of data for authorized use
- Proactively identify risks and propose viable mitigation steps
- Cultivate a proactive risk management culture
- Implement "best practice" threat management strategies and processes to reduce threats

The Controls Framework

- Policy Development
- Security Awareness
- Internal Risk Assessments
- Third-party Risk Assessments
- Risk Remediation Support
- Secure SDLC
- Record retention schedule management
- SOC 2 Facilitation
- Threat protection & monitoring
- Malware detection (ePO)
- Threat correlation & reporting
- Incident response

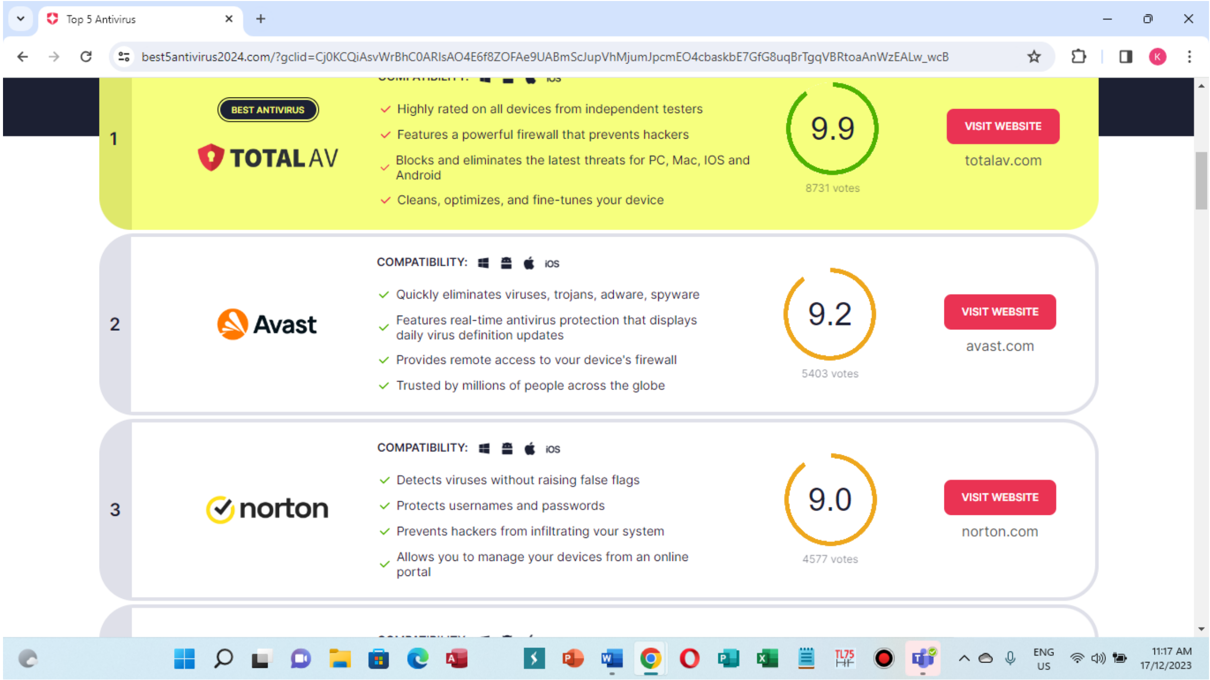
- Computer forensics
- Vulnerability management
- Application scanning
- Penetration testing
- Campus & industry threat collaboration
- Security training administration

Legislative, regulatory, contractual requirements and other policy-related requirements - Information Security works closely with several departments, including the Office of Management (OOM) and Institutional Review Board (IRB) to ensure that sensitive information is appropriately protected.

- Privacy & Compliance liaison
- UMass President's Office & UMass Chan Legal liaison
- Subpoena and Public records requests support
- Internal and External Audit participation and response
- Regulatory guidance and direction
- HIPAA Analysis / Assessment Security Oversight
- IRB Support

TOP 5 Anti Virus Software

https://best5antivirus2024.com/?gclid=Cj0KCQiAsvWrBhC0ARIsAO4E6f8ZOFAe9UABmScJupVhMjumJpcmEO4cbaskbE7GfG8uqBrTgqVBRtoaAnWzEALw_wcB



Top 5 Antivirus

best5antivirus2024.com/?gclid=Cj0KCQiAsvWrBhC0ARIsAO4E6f8ZOFAe9UABmScJupVhMjumJpcmEO4cbaskbE7GfG8uqBrTgqVBRtoaAnWzEALw_wcB

1 BEST ANTIVIRUS TOTAL AV

- ✓ Highly rated on all devices from independent testers
- ✓ Features a powerful firewall that prevents hackers
- ✓ Blocks and eliminates the latest threats for PC, Mac, IOS and Android
- ✓ Cleans, optimizes, and fine-tunes your device

9.9 8731 votes VISIT WEBSITE totalav.com

2 Avast

COMPATIBILITY: iOS

- ✓ Quickly eliminates viruses, trojans, adware, spyware
- ✓ Features real-time antivirus protection that displays daily virus definition updates
- ✓ Provides remote access to your device's firewall
- ✓ Trusted by millions of people across the globe

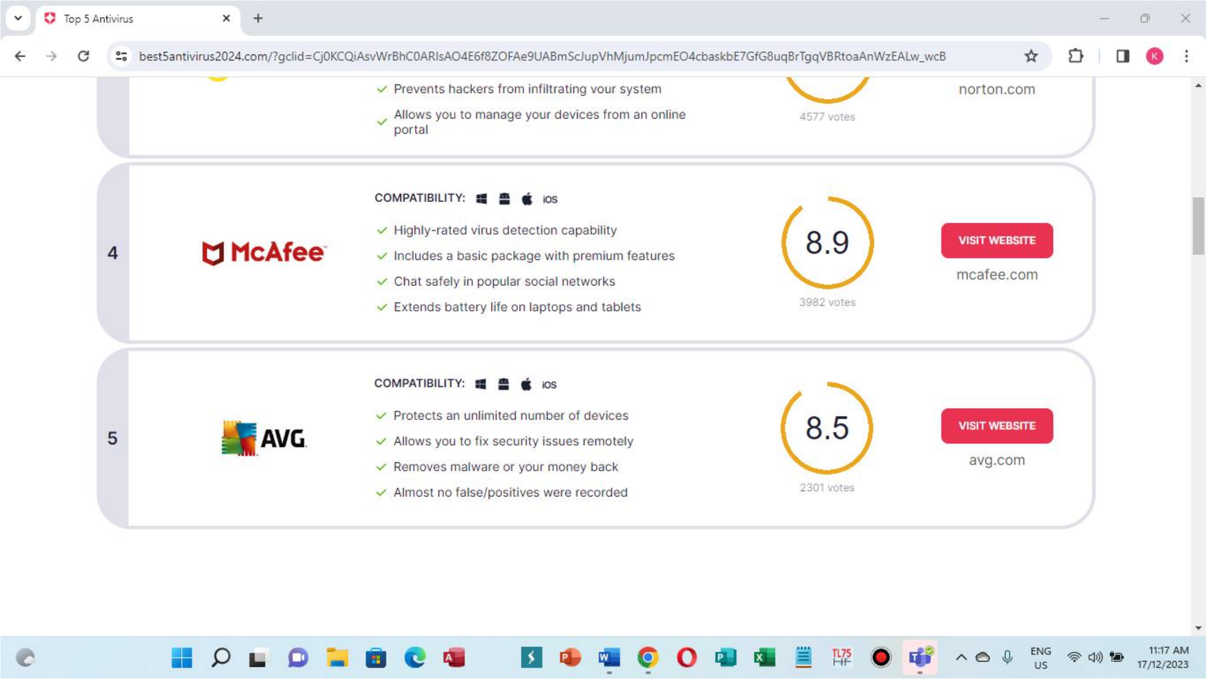
9.2 5403 votes VISIT WEBSITE avast.com

3 norton

COMPATIBILITY: iOS

- ✓ Detects viruses without raising false flags
- ✓ Protects usernames and passwords
- ✓ Prevents hackers from infiltrating your system
- ✓ Allows you to manage your devices from an online portal

9.0 4577 votes VISIT WEBSITE norton.com



Top 5 Antivirus

best5antivirus2024.com/?gclid=Cj0KCQiAsvWrBhC0ARIsAO4E6f8ZOFAe9UABmScJupVhMjumJpcmEO4cbaskbE7GfG8uqBrTgqVBRtoaAnWzEALw_wcB

- Prevents hackers from infiltrating your system
- Allows you to manage your devices from an online portal

4577 votes

norton.com

4 McAfee

COMPATIBILITY: iOS

- Highly-rated virus detection capability
- Includes a basic package with premium features
- Chat safely in popular social networks
- Extends battery life on laptops and tablets

8.9

3982 votes

VISIT WEBSITE

mcafee.com

5 AVG

COMPATIBILITY: iOS

- Protects an unlimited number of devices
- Allows you to fix security issues remotely
- Removes malware or your money back
- Almost no false/positives were recorded

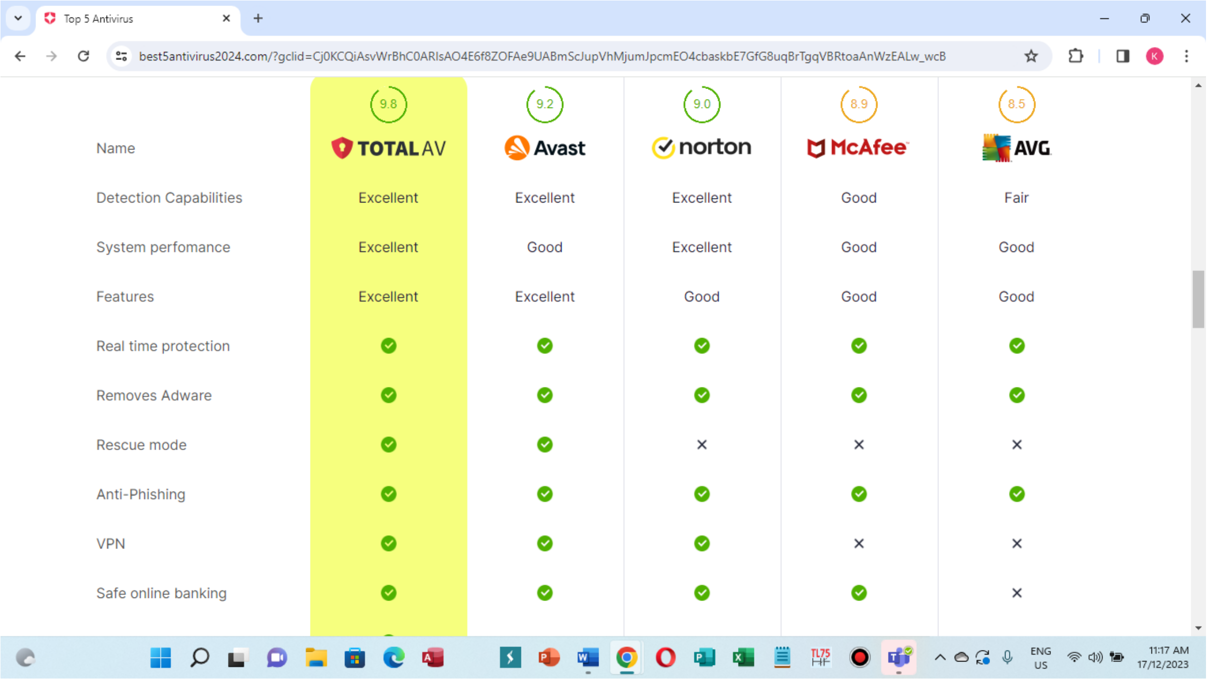
8.5

2301 votes

VISIT WEBSITE

avg.com

ENG US 11:17 AM 17/12/2023



Top 5 Antivirus

best5antivirus2024.com/?gclid=Cj0KCQiAsvWrBhC0ARIsAO4E6f8ZOFAe9UABmScJupVhMjumJpcmEO4cbaskbE7GfG8uqBrTgqVBRtoaAnWzEALw_wcB

	9.8	9.2	9.0	8.9	8.5
Name	TOTAL AV	Avast	norton	McAfee	AVG
Detection Capabilities	Excellent	Excellent	Excellent	Good	Fair
System perfomance	Excellent	Good	Excellent	Good	Good
Features	Excellent	Excellent	Good	Good	Good
Real time protection	✓	✓	✓	✓	✓
Removes Adware	✓	✓	✓	✓	✓
Rescue mode	✓	✓	×	×	×
Anti-Phishing	✓	✓	✓	✓	✓
VPN	✓	✓	✓	×	×
Safe online banking	✓	✓	✓	✓	×

ENG US 11:17 AM 17/12/2023

Facebook Posts

ပုံမှန်အရ internet မှာ IP address ဆိုတာရှိပါတယ်။ လူမှာနံမည်ရှိသလိုမျိုးပါ။ linksတိုင်းမှာ IPရှိပါတယ်။ ကိုယ်ရဲ့network IP address ကို တခြားလူက သိသွားမှသာ ကိုယ်ရဲ့အချက်အလက်ကိုခြေရာခံလို့ရတာပါ။ ပုံမှန်အရ VPNမခံပဲ FBသုံးတယ်ဆိုရင်တောင် ကိုယ့်ရဲ့ip address ကိုသိဖို့အတွက် ကြားခံ layers ၇ခု ကိုကျော်ဖြတ်နိုင်မှသိရတာပါ။

IP address ကိုသိဖို့ဆိုတာလွယ်ကူတဲ့အရာတော့မဟုတ်ပါဘူး။ ဆိုင်ဘာလုံခြုံရေးက သူလိုလိုပါပြီးသားပါ။ ဥပမာ။ မြန်မာနိုင်ငံထဲက လူနဲ့ အမေရိကန်နိုင်ငံကလူ FBပေါ်မှာ စကားပြောကြတယ်ဆိုတာ အပေါ်ယံမှာ ဘာမှမထူးခြားပေမယ့် သူတို့ရဲ့တည်နေရာကို ရှာဖို့ အရမ်းကိုခက်ခဲပါတယ်။ အဆင့်ဆင့်သွားရပါတယ်။

ကိုယ့်ဖုန်းကစာတစောင်ကို မက်ဆင်ဂျာက ပို့လိုက်တယ်ဆိုပါတော့ ။ ကိုယ့်ဖုန်းရဲ့IP ကနေ အင်တာနက် network IPကို သွားရတယ် ပြီးမှ မက်ဆင်ဂျာ app ရဲ့IPကိုပြောင်းသွားတယ်။အဲဒါကို API (application programming interface)လို့အလွယ်ခေါ်တယ်။ သူကဒီအတိုင်းလိုက်ရှာလို့မရဘူး လုံ ခြုံရေးနည်းပညာကြောင့်သူအလိုလိုပျောက်နေတယ်။

မက်ဆင်ဂျာ IPကနေ အမေရိကန်ကလူဆီတိုက်ရိုက်တန်းမရောက်ဘူး။ မြန်မာနိုင်ငံပြင်ပဖြစ်သွားတဲ့အတွက် internet exchange ဆီကိုအရင်သွားရတယ်။ အဲဒါကို ASNs(autonomous System numbers)လို့ခေါ်တယ်။ ဆာဗာချိန်းတယ်လို့အလွယ်ခေါ်တယ်။ (မြန်မာရဲ့ASNs 157 ဖြစ်ပါတယ်။ သူ့အောက်မှာ အင်တာနက် company တွေကနေမတူညီတဲ့နံမည်တွေနဲ့ဝန်ဆောင်မှုပေးကြတယ် အဲဒီလိုတခုချင်းဆီကို Hosting IPsလို့ခေါ်တယ် ။စုစုပေါင်း1517ခုရှိတယ်)

ခုနက ကိုယ်က မက်ဆင်ဂျာကနေ ပို့လိုက်တဲ့စာက exchange severဆီကို ရောက်တဲ့အချိန်ထိ တခြားလူတွေမမြင်အောင် ခိုးယူလို့မရအောင် SSL (secure socket layer) က ဖုံးကွယ်ပေးထားတယ်။ အဲဒီ exchange sever မှတဆင့် အမေရိကန်ကလူ ဆီကို ပြန်သွားတာကို TLS(transport layer security)လို့ခေါ်တယ်။ ကိုယ်ပို့လိုက်တဲ့စာကို code ပြောင်းလိုက်ပြီးမှပို့တာပါ။အဲဒီ TLS ကနေ အမေရိကန်နိုင်ငံထဲကိုဝင်ရောက်ဖို့ DNS (Domain Name System)ကိုဖြတ်သန်းရပါတယ်။ DNS ကို cloudflare severကတဆင့် လုံခြ◌ုံရေးအတွက် နံမည်ပြောင်းပြီးတည်နေရာလွဲပေးထားပါတယ်။ အဲဒီကနေ codeတွေကို စာအဖြစ်ပြန်ပြောင်းပြီးအားလုံးတူညီမှ proxy sever (gateway to internet to user) မှတဆင့် ပို့ပေးမှ မြန်မာနိုင်ငံမှ အမေရိကန်သို့ စာတစ်စောင်ရောက်တာပါ။

အခုပြောပြတာ VPNမသုံးရသေးဘူးနော်။ VPNသုံးလိုက်တဲ့သဘောက ဘယ်ကမှန်းမသိတဲ့လူက အမေရိကန်ကို စာတစောင်ပို့လိုက္တဲ့သဘောဖြစ်ပါတယ်။

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Top 11 Most Powerful CyberSecurity Software Tools In 2023

October 18, 2023

List and Comparison of the Best Cybersecurity Software to Protect Your Business from Cyber Threats:

A CyberSecurity Software is a must for Cyber Security and Privacy of a business or individual. Cybersecurity is the method that is used to protect the network, system, or applications from the cyber-attacks. It is used to avoid unauthorized data access, cyber-attacks, and identity theft.

Application security, information security, network security, disaster recovery, operational security, etc. are the different parts of cybersecurity. It needs to be maintained for various types of cyber threats like Ransomware, Malware, Social Engineering, and Phishing.

Top 11 Most Powerful CyberSecurity Software Tools In 2023

October 18, 2023

List and Comparison of the Best Cybersecurity Software to Protect Your Business from Cyber Threats:

A CyberSecurity Software is a must for Cyber Security and Privacy of a business or individual. Cybersecurity is the method that is used to protect the network, system, or applications from the cyber-attacks. It is used to avoid unauthorized data access, cyber-attacks, and identity theft.

Application security, information security, network security, disaster recovery, operational security, etc. are the different parts of cybersecurity. It needs to be maintained for various types of cyber threats like Ransomware, Malware, Social Engineering, and Phishing.

Types of CyberSecurity Tools

CyberSecurity Software can be categorized into different types as mentioned below:

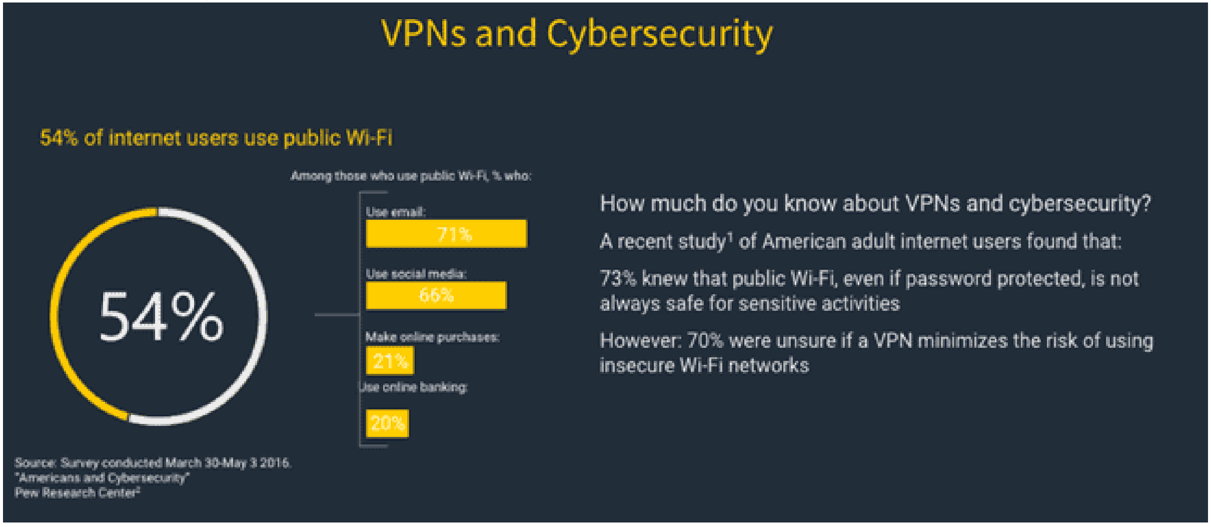
- Network Security Monitoring tools
- Encryption Tools
- Web Vulnerability Scanning tools
- Network Defence Wireless Tools
- Packet Sniffers
- Antivirus Software
- Firewall
- PKI Services
- Managed Detection Services

- Penetration Testing

How Important Is Cybersecurity?

The importance of cybersecurity can be understood through the research performed by Mimecast. It says that there is a 26% rise in the ransomware, 88% of companies saw email-based spoofing, and 67% of the organizations have reported that there is an increase in impersonation fraud.

Making use of public Wi-Fi makes your device or data more vulnerable to the attacks. According to the research performed by Norton, 54% of internet users use public Wi-Fi and 73% of people knew that public Wi-Fi is not safe even if it is passwords protected. All these statistics prove that cybersecurity is the need of the hour.



VPNs and Cybersecurity

How much do you know about VPNs and cybersecurity?

A recent study[1] of American adult internet users found that:

73% knew that public Wi-Fi, even if password protected, is not always safe for sensitive activities

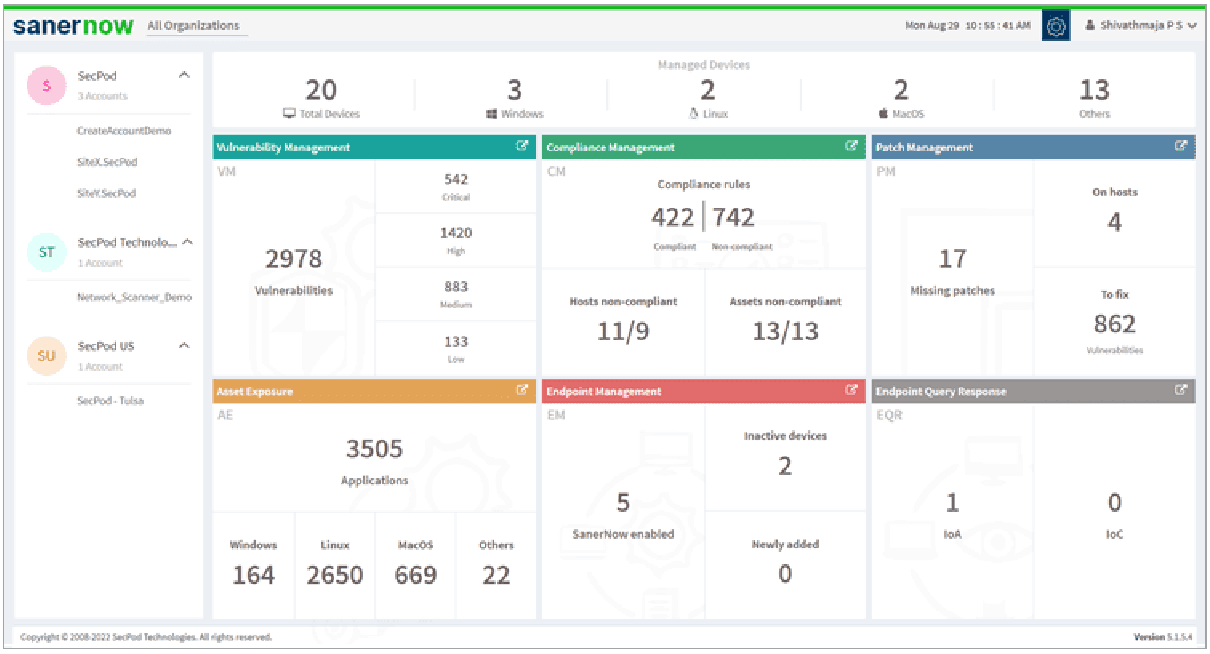
However: 70% were unsure if a VPN minimizes the risk of using insecure Wi-Fi networks

Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"
Pew Research Center[2]

[image source]

#1) SecPod SanerNow

Best for small to large businesses.



SanerNow cyberhygiene platform provides an advanced vulnerability management solution to achieve continuous security risk, and compliance posture for cyber-attack prevention. It is an advanced vulnerability management platform that integrates vulnerability assessment with instant remediation into a single unified console.

It scans for vulnerabilities, misconfigurations and more and provides remediation controls and methods to remediate them instantly and automatically.

With its natively-built system, every step of vulnerability management, from scanning to remediation, can be automated. SanerNow helps you strengthen your organization’s security posture and prevent cyberattacks.

Features:

- It uses an intelligent and lightweight multi-functional agent that performs all tasks.
- By evaluating risk potential, high-fidelity attacks, and more, SanerNow efficiently prioritizes vulnerabilities for easy remediation.
- With its integrated patching, you can quickly remediate vulnerabilities in IT assets.
- With its remediation controls beyond patching, mitigating security risks becomes easier.
- From a single cloud-based console, your organization can efficiently mitigate vulnerabilities and more.

- With SanerNow, you can perform real-time vulnerability management, from scanning to remediation.

Category: Cloud and On-premises vulnerability and patch management tool.

Verdict: With SanerNow, you get a complete cybersecurity solution that can =take your vulnerability management process to a next level by managing other security risks as well from the same console. Furthermore, it can replace multiple solutions you use for vulnerability management and patch management, helping you manage attack surfaces more effectively.

Price: Contact for a quote

=> Visit SecPod SanerNow Website

#2) Intruder

Best for small to large businesses.

Price: A 14-day Free trial is available. It includes three pricing plans i.e. Essential, Pro, and Verified. Contact them for more details about their pricing information.

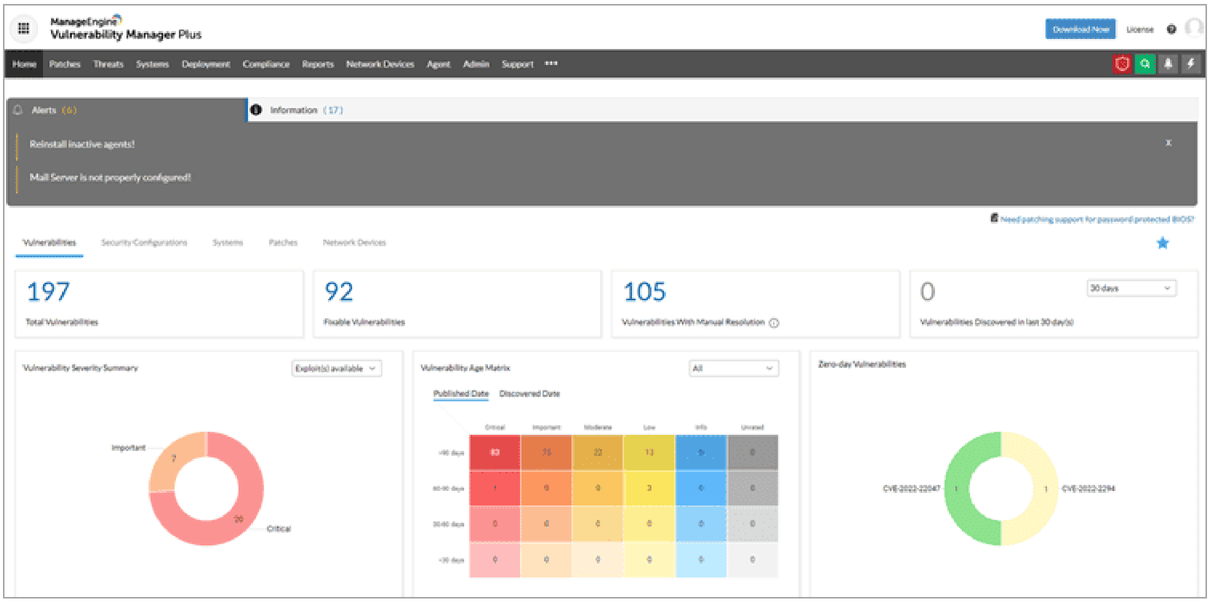
Intruder is the most popular cloud-based network vulnerability scanner that helps you to find the cybersecurity weaknesses in your most exposed systems to avoid costly data breaches. It is the right solution for your cybersecurity issues. It helps to save your time to a great extent.

Features:

- Over 9,000 security vulnerabilities.
- Unlimited scans on demand.
- Unlimited user accounts.
- Checks for web application flaws such as SQL injection and Cross-site scripting.
- Emerging threat notifications.
- Smart Recon
- Network view
- PCI ASV scans available.

Category: Cloud-based Vulnerability Scanner
Verdict: Intruder is a one-stop solution for all your cybersecurity needs.
=> **Visit Intruder Website**

#3) ManageEngine Vulnerability Manager Plus



Reinstall inactive agents!

Mail Server is not properly configured!

Need patching support for password protected BIOS?

197 Total Vulnerabilities

92 Fixable Vulnerabilities

105 Vulnerabilities With Manual Resolution

0 Vulnerabilities Discovered in last 30 day(s)

	Critical	Important	Moderate	Low	Info	Unrated
>90 days	83	75	22	13	5	0
60-90 days	1	0	0	3	0	0
30-60 days	0	0	0	0	0	0
<30 days	0	0	0	0	0	0

ManageEngine Vulnerability Manager Plus is a prioritization-focused threat and vulnerability management software for enterprises offering built-in patch management.

It’s a strategic solution for delivering comprehensive visibility, assessment, remediation, and reporting of vulnerabilities, misconfigurations, and other security loopholes across the enterprise network from a centralized console.

Features:

- Assess & prioritize exploitable and impactful vulnerabilities with a risk-based vulnerability assessment.
- Automate & customize patches to Windows, macOS, Linux.
- Identify zero-days vulnerabilities and implement workarounds before fixes arrive.
- Continually detect & remediate misconfigurations with security configuration management.
- Gain security recommendations to set up web servers in a way that’s free from multiple attack variants.
- Audit end-of-life software, peer-to-peer & insecure remote desktop sharing software and active ports in your network.

Category: On Premises end-to-end threat and vulnerability management software.

Verdict: ManageEngine Vulnerability Manager Plus is a multi-OS solution that not only offers vulnerability detection but also provides built-in remediation for vulnerabilities.

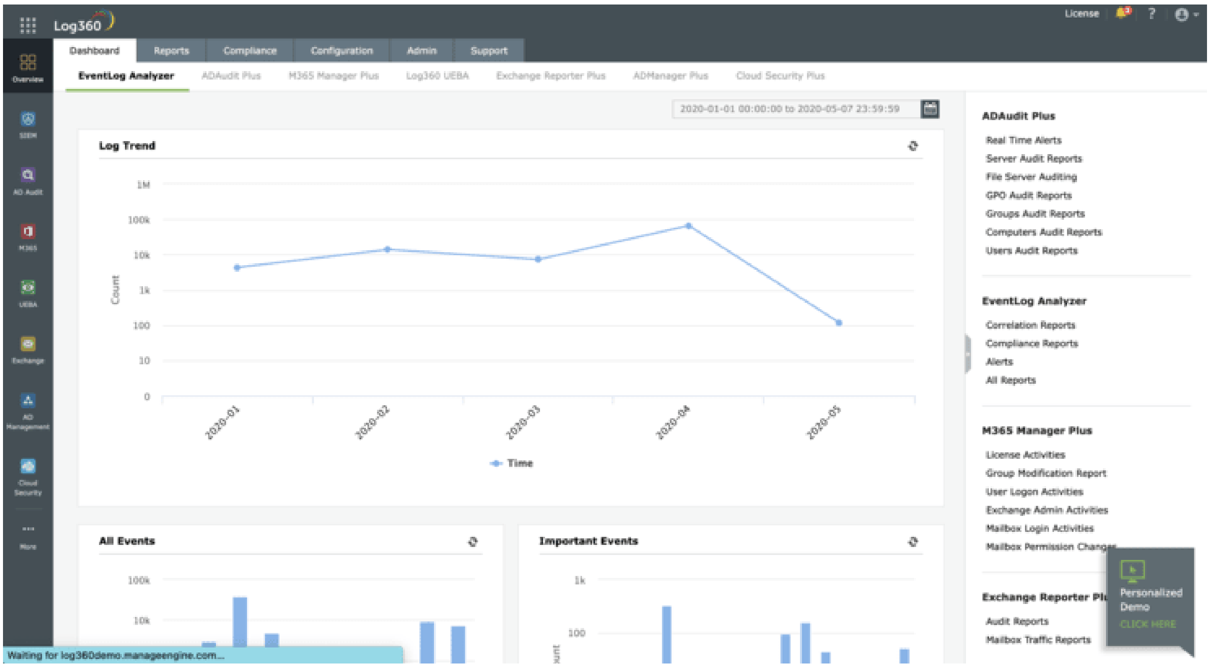
Vulnerability Manager Plus offers a wide variety of security features such as security configuration management, automated patching, web server hardening, and high-risk software auditing to maintain a secure foundation for your endpoints.

=> **Visit ManageEngine Vulnerability Manager Plus Website**

#4) ManageEngine Log360

Best for Internal and External threat protection.

Price: Contact for quote. A 30 day free trial is available.



With Log360, you get a cybersecurity solution that leverages machine learning to detect and address security threats. The platform comes with in-built threat intelligence database that makes the tool capable of tackling risk, both old and new in nature. You can also rely on the tool to manage security incidents in real-time based on customizable alerts.

Also Read => **A Complete Guide On Cybersecurity Analytics**
Features:

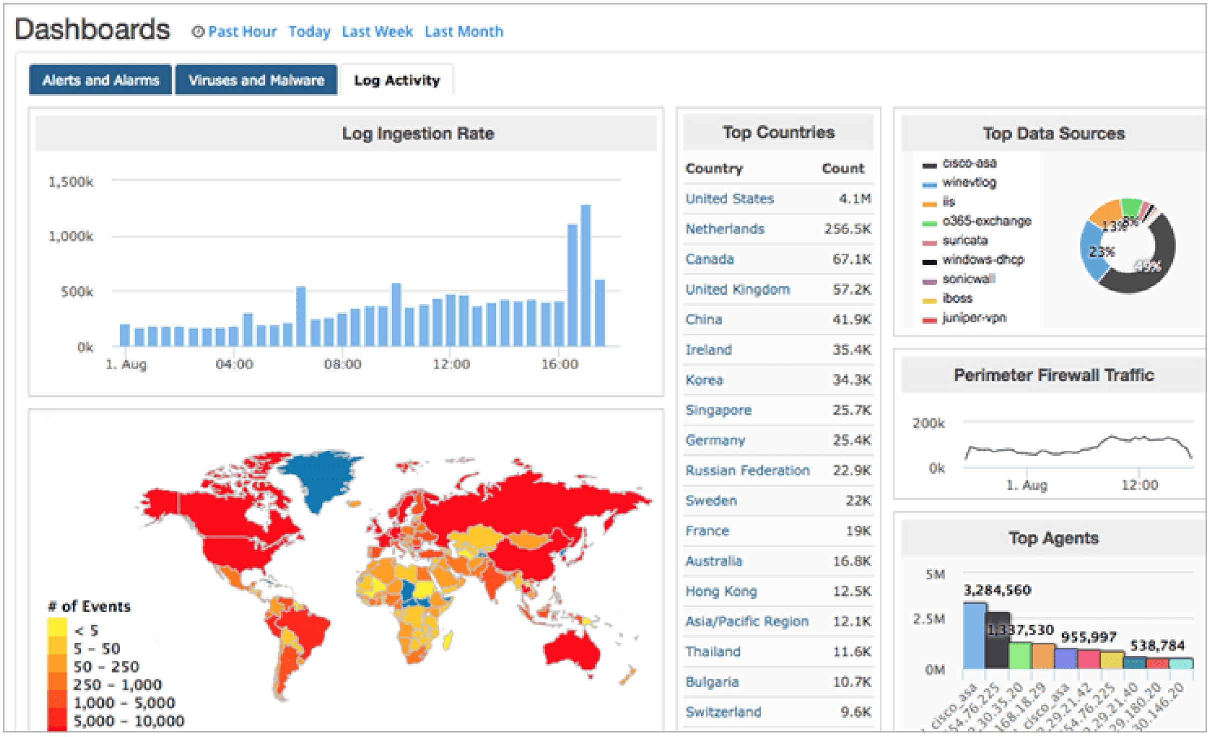
- Threat Intelligence
- Behavior Analytics
- Data Visualization
- Compliance Reporting
- Incident Management

Verdict: ManageEngine’s Log360 is one of the best SIEM solutions out there when it comes to detecting network threats, analyzing suspicious user behavior, and preventing data leakage.

=> **Visit ManageEngine Log360 Website**

#5) SolarWinds Security Event Manager

Best for small to large businesses.
Price: It provides a fully functional trial for 14 days. The price for the product starts at $4500.



Top Countries

Country	Count
United States	4.1M
Netherlands	256.5K
Canada	67.1K
United Kingdom	57.2K
China	41.9K
Ireland	35.4K
Korea	34.3K
Singapore	25.7K
Germany	25.4K
Russian Federation	22.9K
Sweden	22K
France	19K
Australia	16.8K
Hong Kong	12.5K
Asia/Pacific Region	12.1K
Thailand	11.6K
Bulgaria	10.7K
Switzerland	9.6K

SolarWinds Security Event Manager is a network and host intrusion detection system. It performs real-time monitoring, responding, and reporting of security threats. It has highly indexed log search capabilities. It is a cloud-based scalable solution.

Features:

- Threat intelligence will get continuously updated.
- It has features for Security Information and Event Manager.
- It offers features of Log correlation and Log event archive.
- It provides a comprehensive set of integrated reporting tools.

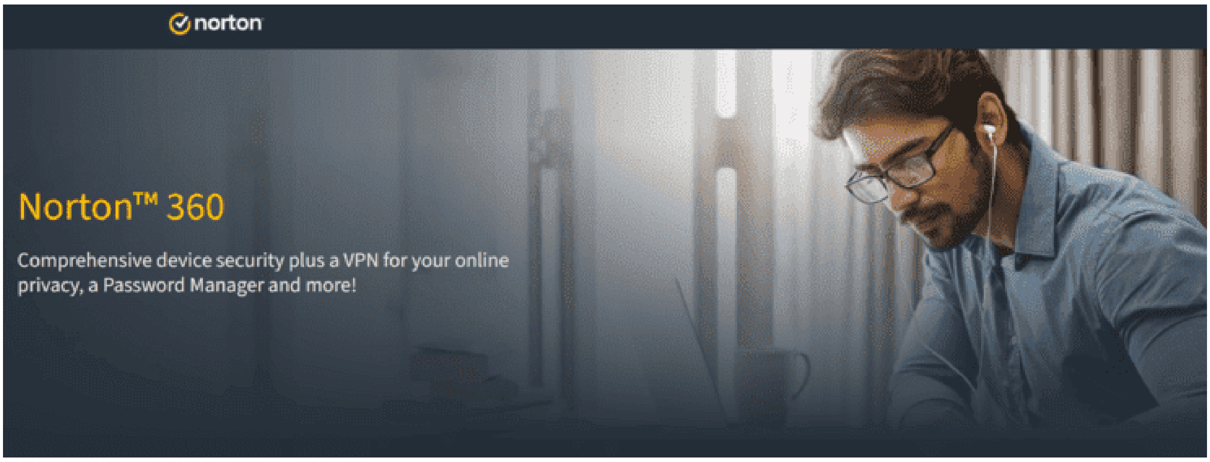
Category: Cloud-based tool for SIEM.
Verdict: Solarwinds Security Event Manager is a cloud-based solution developed for Managed Service Providers as an all-in-one solution of the SIEM tool.

=> **FREE DOWNLOAD Systems Management Bundle**

=> **Download Solarwinds Security Event Manager Free**

#6) Norton Security

Price: Norton provides a 30-day free trial for Antivirus. Antivirus price starts at $5.99 per month. Norton 360 with LifeLock price starts at $9.99 for the first 3 months.


norton
Norton™ 360
Comprehensive device security plus a VPN for your online privacy, a Password Manager and more!

Norton provides an all-in-one solution through Norton 360 with LifeLock. The company offers cybersecurity software solutions such as Antivirus, Virus Removal, Malware Protection, Cloud Backup, Password Manager, and Secure VPN.

Features

- Norton Antivirus can protect against ransomware, viruses, spyware, malware, and other online threats.
- It provides five-layer protection for recognizing and blocking threats.
- It offers cloud backup services that can store and protect files and documents.
- Norton Password Manager is a simple, secure, and smart solution for managing passwords.
- It provides a secure Norton VPN.

Verdict: Norton security Solution is for computers, smartphones, and tablets. It has a variety of solutions like Antivirus, Password Manager, and VPN.

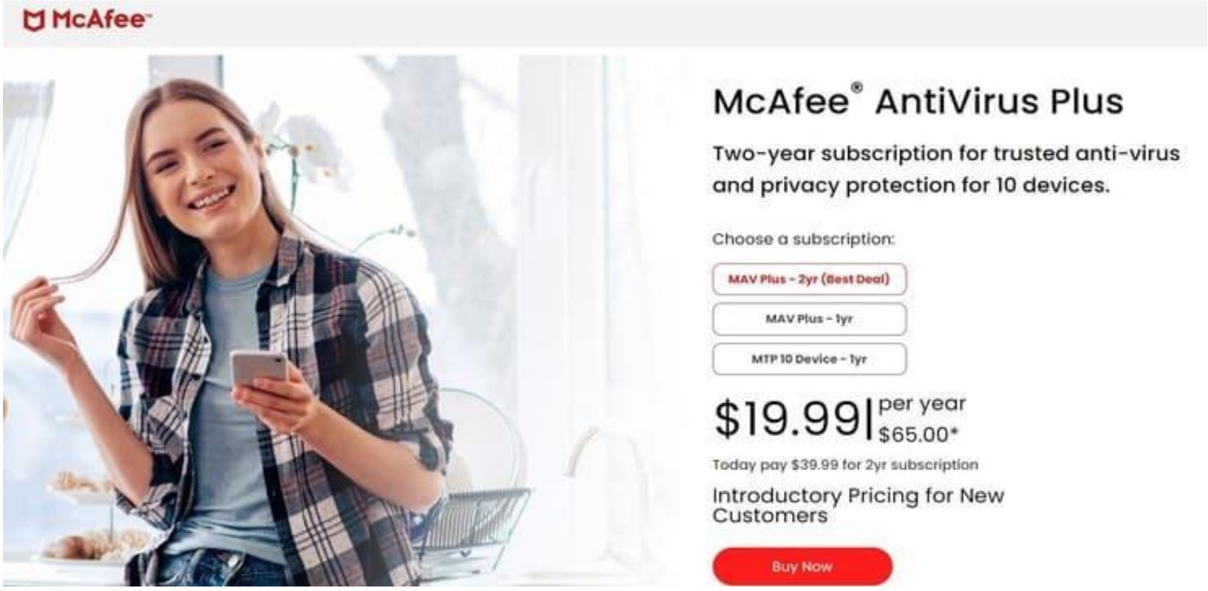
=> Visit Norton Security Website

Further Reading => List of the BEST Tufin Competitors of the Year

---

#7) McAfee

Best for Multi-faceted security protection.



McAfee® AntiVirus Plus

Two-year subscription for trusted anti-virus and privacy protection for 10 devices.

Choose a subscription:

$19.99 | per year $65.00*

Today pay $39.99 for 2yr subscription

Introductory Pricing for New Customers

McAfee offers total security protection to users by offering a combination of some of the best privacy, identity protection, and antivirus tools. The software once deployed, will protect you against ransomware, viruses, phishing scams, adware, malware, etc. in real-time. The best part about McAfee is the fact that you only need one subscription to protect up to 10 different devices.

Features:

- Antivirus protection
- Complete Firewall protection
- Full Internet Protection
- Password Manager
- Encrypted Storage

Verdict: McAfee is a fantastic cross-platform cybersecurity solution that'll protect all your devices from almost all sorts of threats in real-time. It is affordable, easy to use, and quite effective in neutralizing threats… both old and new.

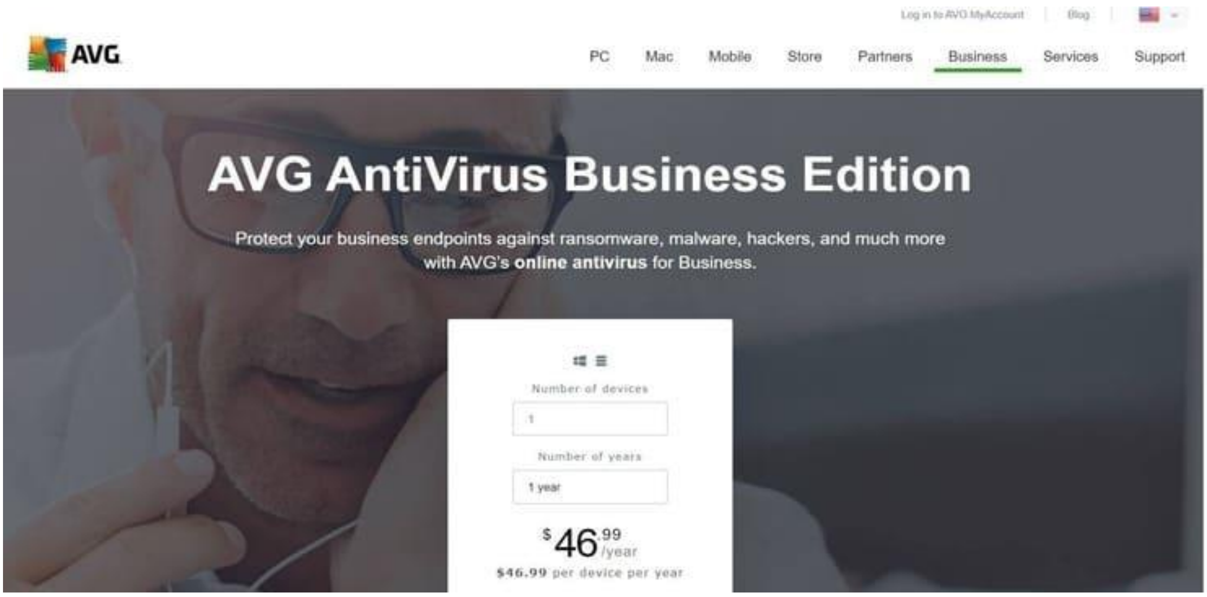
Price:

- MAV Plus: $34.99/year
- MTP 10 Device Plan: $64.99/year
- MAV Plus 2 Yr.: $19.99/year

=> **Visit McAfee Website**

#8) AVG

Best for Small to mid-sized enterprises
Price: Starts at $46.99/year per device



AVG AntiVirus Business Edition

Protect your business endpoints against ransomware, malware, hackers, and much more with AVG's **online antivirus** for Business.

Number of devices: 1

Number of years: 1 year

$46.99 /year

$46.99 per device per year

AVG offers a powerful cybersecurity solution that both small and mid-sized enterprises can benefit from. It comes jam-packed with advanced features necessary to keep office devices safe from both internal and external threats. The software is advanced enough to protect your systems against the newest viruses, ransomware, and malware threats out there.

Features:

- Smart Scanner
- Identity Protection
- File Shredder
- File Server Security
- Remote Access

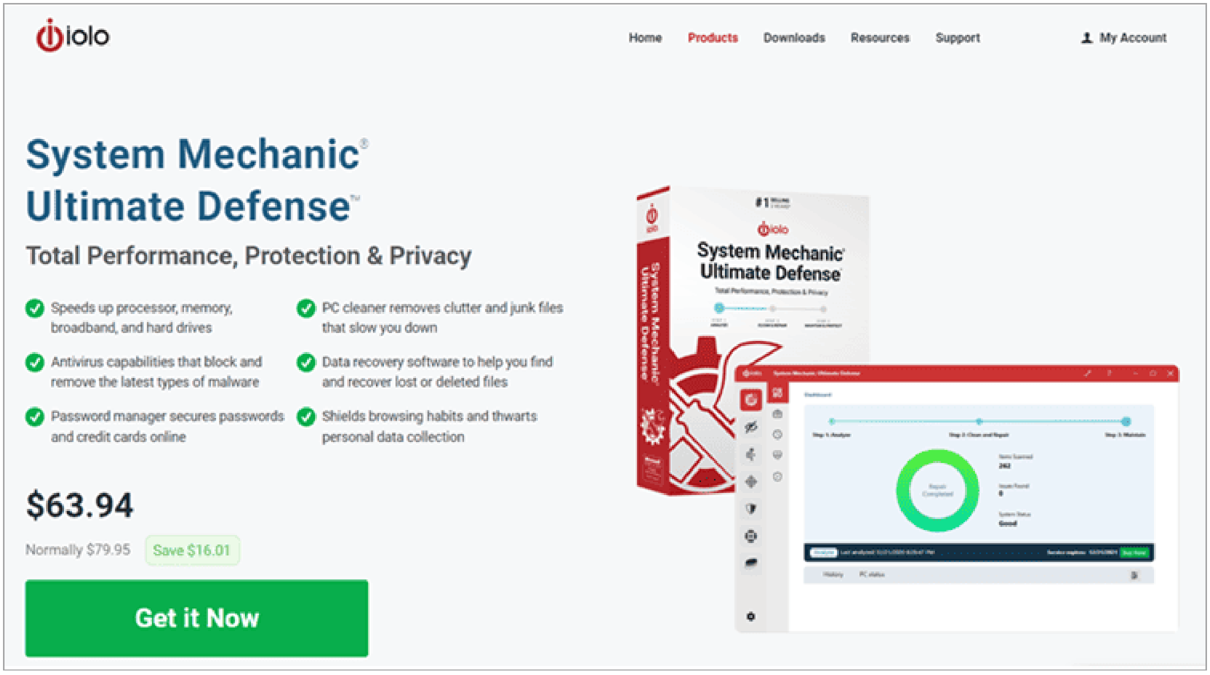
Category: Small business antivirus and firewall protection tool

Verdict: With AVG, you get an easy to install cybersecurity solution that can protect all of your devices against old and new threats round the clock. The software is affordable and packed with features for robust threat protection.

=> **Visit AVG Website**

#9) System Mechanic Ultimate Defense

Best for AI and Algorithm Powered Threat Detection.
Price: $63.94 annual plan.



System Mechanic® Ultimate Defense™

Total Performance, Protection & Privacy

- Speeds up processor, memory, broadband, and hard drives
- PC cleaner removes clutter and junk files that slow you down
- Antivirus capabilities that block and remove the latest types of malware
- Data recovery software to help you find and recover lost or deleted files
- Password manager secures passwords and credit cards online
- Shields browsing habits and thwarts personal data collection

$63.94

Normally $79.95 Save $16.01

System Mechanic Ultimate Defense serves as both an effective PC optimizer and powerful cybersecurity software. It can shield your PC against viruses, spyware, and other such threats with real-time anti-virus protection. It leverages intuitive threat detection algorithms and AI to accurately detect new and unknown threats before they have a chance to harm your system.

Features:

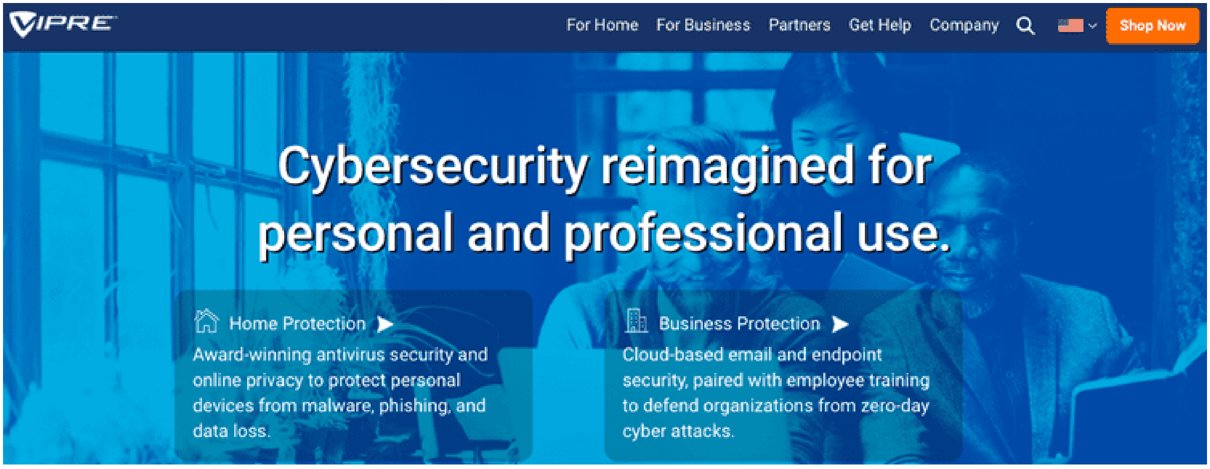
- Protects online passwords and credit card details from prying eyes online.
- Uses advanced AI to detect and remove the latest malware threats.
- Identify and remove system slowing bloatware.
- Leverage proprietary technology to analyze suspicious-looking files.

Category: On-Premise and Cloud-based Threat Detection.

Verdict: No conversation on cybersecurity software can be complete without System Mechanic Ultimate Defense. This software can detect unknown new and previous threats, thanks to the advanced AI and algorithms it uses. This is definitely one cybersecurity software that should be on your radar if it already isn't.
=> **Visit System Mechanic Ultimate Defense Website**

#10) Vipre

Best for comprehensive protection against evolving threats.
Price: Vipre business protection is available in three pricing plans i.e. Core Defense ($96 per user per year), Edge Defense ($96 per user per year), and Complete Defense ($144 per user per year). Its home protection price starts at $14.99 for the first year.



Cybersecurity reimagined for personal and professional use.

Home Protection
Award-winning antivirus security and online privacy to protect personal devices from malware, phishing, and data loss.

Business Protection
Cloud-based email and endpoint security, paired with employee training to defend organizations from zero-day cyber attacks.

Vipre offers cybersecurity solutions for personal as well as professional use. It protects against computer viruses, ransomware, and identity theft.

For business protection, it can provide comprehensive email & end-point security & privacy, and real-time threat intelligence. This provides layered protection to your business and partners. It supports Windows and Mac platforms.

Features:

- Vipre provides simplified solutions to protect your business from online threats and data risks.
- It has all-inclusive packages and scalable pricing.
- It provides unparalleled protection with the help of AI technology.

- Vipre offers a fully integrated solution that is easy to deploy and manage.
- It can also provide Email encryption capabilities.

Category: Cloud-based email & endpoint security solutions and anti-virus for home use.

Verdict: Vipre is easy to install and use. It has solutions for home protection, endpoint security, and email security. It can provide all-in-one cybersecurity protection with DLP and business VPN. It can also provide security awareness training.

=> **Visit Vipre Website**

#11) LifeLock

Best for small to large businesses.

Price: LifeLock solution is available with four pricing plans, Standard ($7.99 per month for 1st year), Select ($7.99 per month for 1st year), Advantage ($14.99 per month for 1st year), and Ultimate Plus ($20.99 per month for 1st year).

All these prices are for annual billing. Monthly billing plans are also available. You can try the product for 30 days for free.

SPEAK TO AN AGENT 1-866-302-4759

Protection for who and what matters.

Up to 25% off first year*

Identity theft protection plans to fit your needs.

Click here for offer details at bottom of page.*

LifeLock is a tool to monitor for identity theft and threats. Norton 360 with LifeLock provides all-in-one protection to your identity, devices, and online privacy. It is the platform that can block cyber threats, detect & alert, and restore & reimburse.

The solution will resolve ID theft issues with identity restoration agents. It will reimburse the funds that are stolen because of Id theft up to the limit of your plan.

Features:

- LifeLock can provide features of dark web monitoring, id verification monitoring, and fictitious identity monitoring.
- For device security, LifeLock provides features like cloud backup for Windows PCs, virus protection, parental control, ad-tracker blocker, etc.
- It can alert you of the crimes committed in your name.
- It has a privacy monitor.

Category: Identity Theft Protection.

Verdict: Norton antivirus software is included with the solution. It will block your information on public Wi-Fi through a secure VPN. It will monitor for threats to your identity. It provides alerts through phone, text, email, or mobile app. It provides 24*7 live member support.

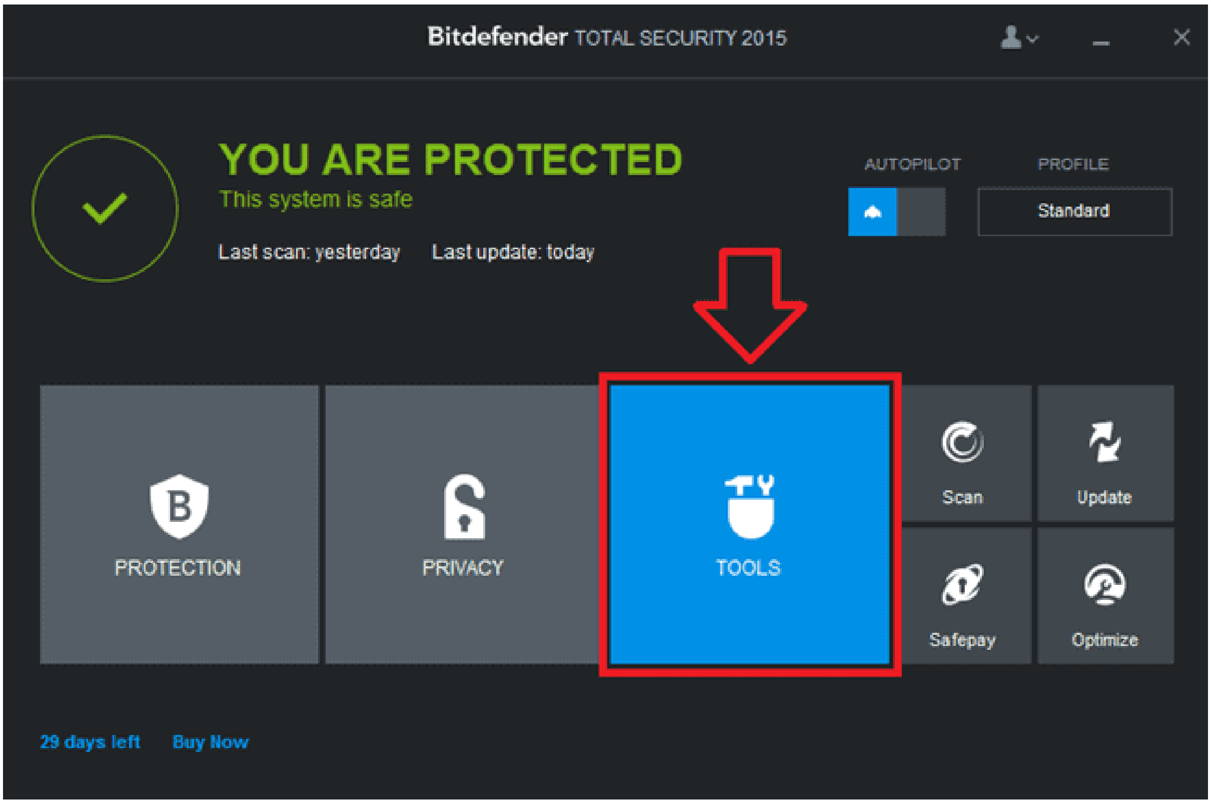
=> **Visit Here To "Get 25% OFF For The First Year" From LifeLock**

#12) Bitdefender Total Security

=> **Avail 50% OFF From Bitdefender Total Security Here**

Best for small to large businesses.

Price: Bitdefender Total Security is available for $42.99. Download it for 1 year for 5 devices for $24.99. A free trial of 30 days is available for Bitdefender Total Security.



Bitdefender TOTAL SECURITY 2015

YOU ARE PROTECTED

This system is safe

Last scan: yesterday   Last update: today

PROFILE: Standard

To provide online privacy and personal information, Bitdefender Total Security provides the features of file shredder, social network protection, privacy firewall, vulnerability assessment, safe online banking, etc. It provides 24*7 comprehensive support. It has features for Anti-Phishing and Anti-Theft.

Features:

- Bitdefender Total Security provides multi-layer ransomware protection along with ransomware remediation.
- It offers Network Threat Protection.
- It has features for complete real-time data protection and advanced threat defense.
- It has functionalities for Web Attack Prevention, Anti-Fraud, and Rescue Mode.

Category: Cybersecurity software

Verdict: Bitdefender is an anti-malware software. It supports Windows, Mac, Android, and iOS devices. It provides cybersecurity solutions for Home, businesses, Providers, and partners.

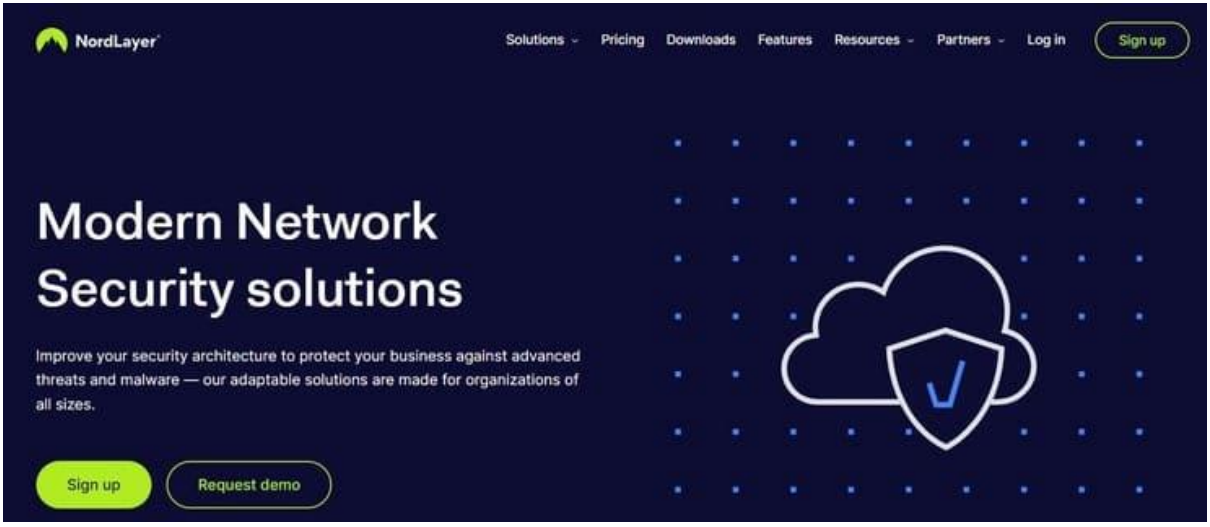
=> **Visit Here To Avail 50% OFF From Bitdefender Total Security**

#13) NordLayer

Best for Threat isolation and network security monitoring

Price: NordLayer comes with 3 plans, which are as follows:

- Basic: $7/user per month
- Advanced: $9/user per month
- Custom pricing plan



Modern Network Security solutions

Improve your security architecture to protect your business against advanced threats and malware — our adaptable solutions are made for organizations of all sizes.

NordLayer is a fantastic network security solution that was designed to strengthen security architecture by blocking advanced threats in their tracks. The software benefits from being both adaptable and scalable.

It can identify threats and automatically isolate them to prevent further harm. It also leverages information from a global threat intelligence database to offer comprehensive network security.

Features:

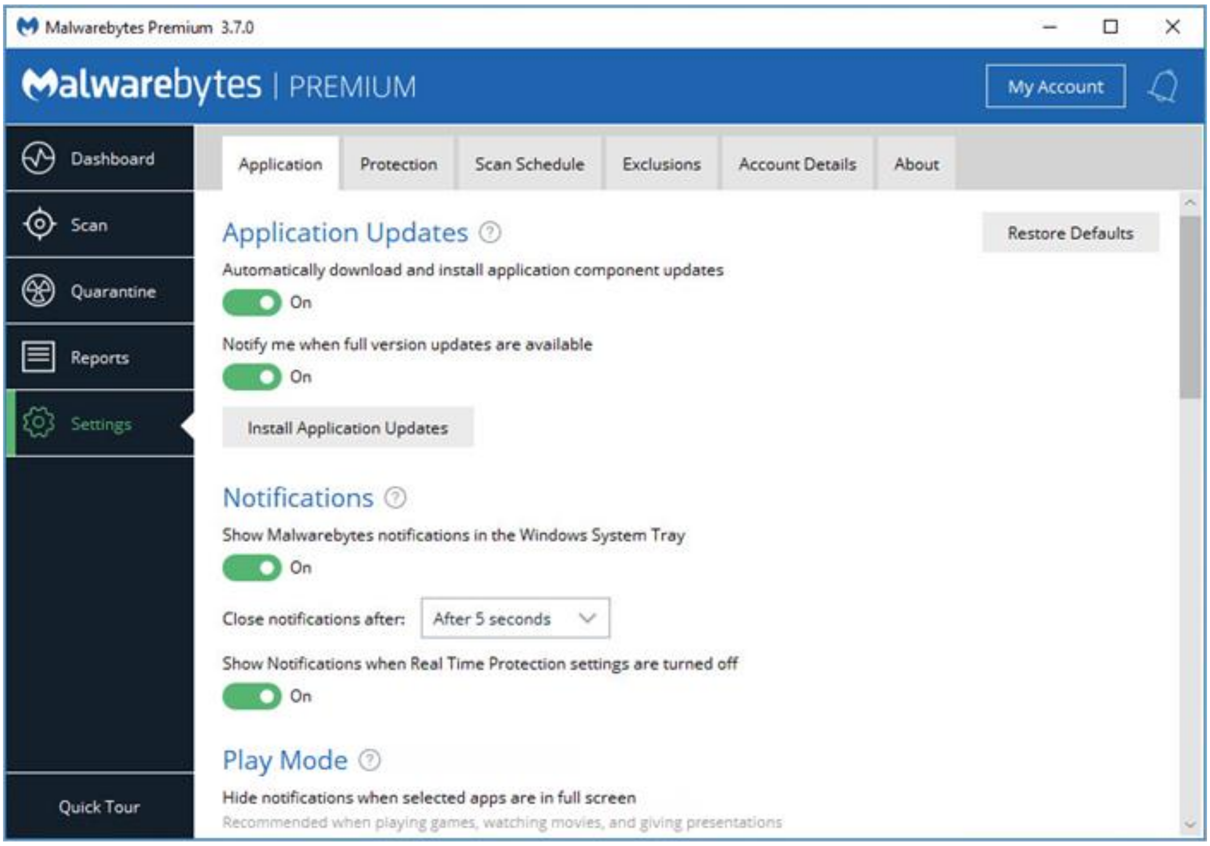
- Threat Prevention
- Network Segmentation
- Zero-Trust Implementation
- Identity and Access Management
- Multi-Factor Authentication

Verdict: With NordLayer, you get a highly scalable and adaptable solution that was tailor made to meet the needs of all organizations, regardless of their size. It's packed with advanced features and comes bolstered with impressive automation.

=> **Visit NordLayer Website**

#14) Malwarebytes

Best for small to large businesses and personal use.
Price: It offers three pricing plans For Teams ($119.97 per year, 3 endpoints), Endpoint Protection ($699.90 per year, 10 endpoints), and Endpoint Detection and Response (Get a quote).
You can increase the number of devices as per your requirements. Home solutions start at $39.99 per year. A free trial is available on request.



Application Updates

Automatically download and install application component updates

On

Notify me when full version updates are available

On

Notifications

Show Malwarebytes notifications in the Windows System Tray

On

Close notifications after: After 5 seconds

Show Notifications when Real Time Protection settings are turned off

On

Play Mode

Hide notifications when selected apps are in full screen

Recommended when playing games, watching movies, and giving presentations

Malwarebytes offers cybersecurity solutions for homes as well as businesses. It can protect against malware, ransomware, malicious websites, etc. It can also protect against advanced online threats that are not detected by the antivirus. It supports Windows, Mac, and Android, iOS, Chromebook devices.

For businesses, it offers various products and services like Endpoint security, incident response, etc. These solutions are available for Education, Finance, and Healthcare industries.

Features:

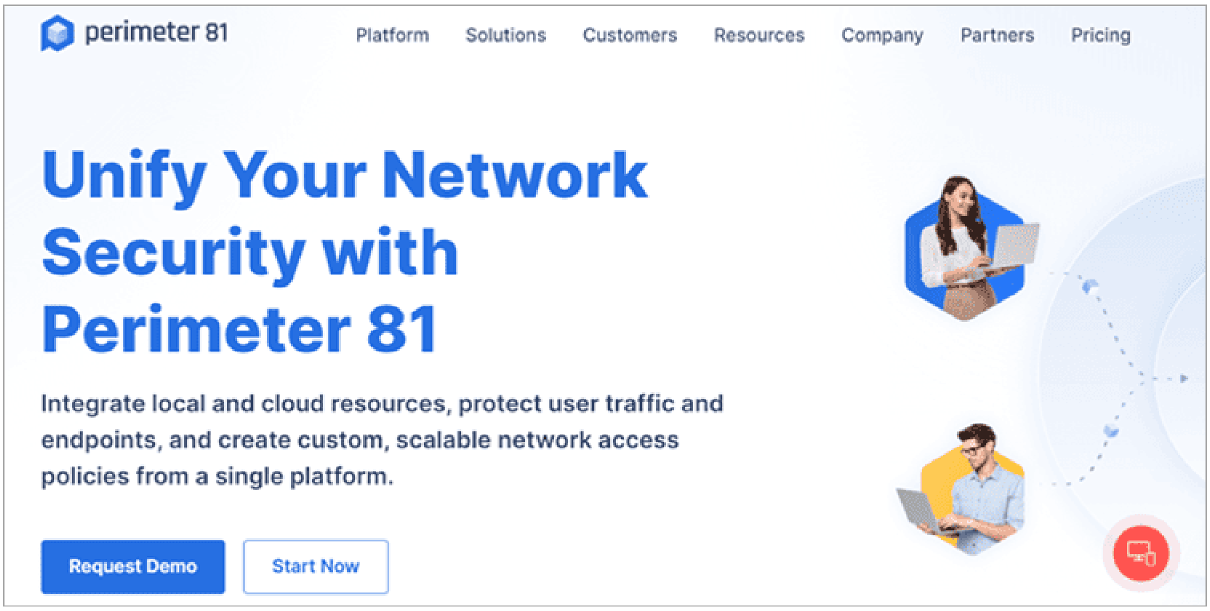
- Malwarebytes makes use of anomaly detection, behavior matching, and application hardening to protect from malware.
- It can clean up the infected devices.
- Malwarebytes will shut down the attack vectors from every angle regardless of the device you are using, Windows, Mac, or Android.
- It can provide multi-layered protection with endpoint detection and response for Windows.
- It can prevent threats in real-time.

Category: Cybersecurity for home and business.
Verdict: Malwarebytes provides the cybersecurity solution for home and businesses. It can prevent threats in real-time and defend against harmful sites.
Businesses can get the solution as per the requirements such as remotely managing endpoints, endpoint protection-detection & response services, protection for a specific number of devices, etc.

=> **Visit Malwarebytes Website**

#15) Perimeter 81

Best for Small to Large Businesses.
Price: Perimeter 81's most affordable plan starts at $8 per user per month. There is also a premium and premium plus plan that costs $12 and $16 per user per month, respectively. You also have the option to go for the custom enterprise plan.



Unify Your Network Security with Perimeter 81

Integrate local and cloud resources, protect user traffic and endpoints, and create custom, scalable network access policies from a single platform.

Perimeter 81 is the software that instantly won us over with just one glance at all of its advanced network security features. The software arms its users with a plethora of cybersecurity tools to strengthen your organization's stance against a wide range of possible threats.

With impressive features that entail device posture check, web filtering, Zero Trust Network access, and multi-factor authentication, the software simplifies the process of managing and securing your network's integrity.

Features:

- Secure network traffic across all environments with the firewall as a service.
- Achieve multi-layered security with encryption, 2FA, and Single Sign-On.
- A single management plan for unified network monitoring and management.
- Block connection from unrecognized Wi-Fi networks with Automatic Wi-Fi Protection.

Category: Cloud Based Network Security Management.

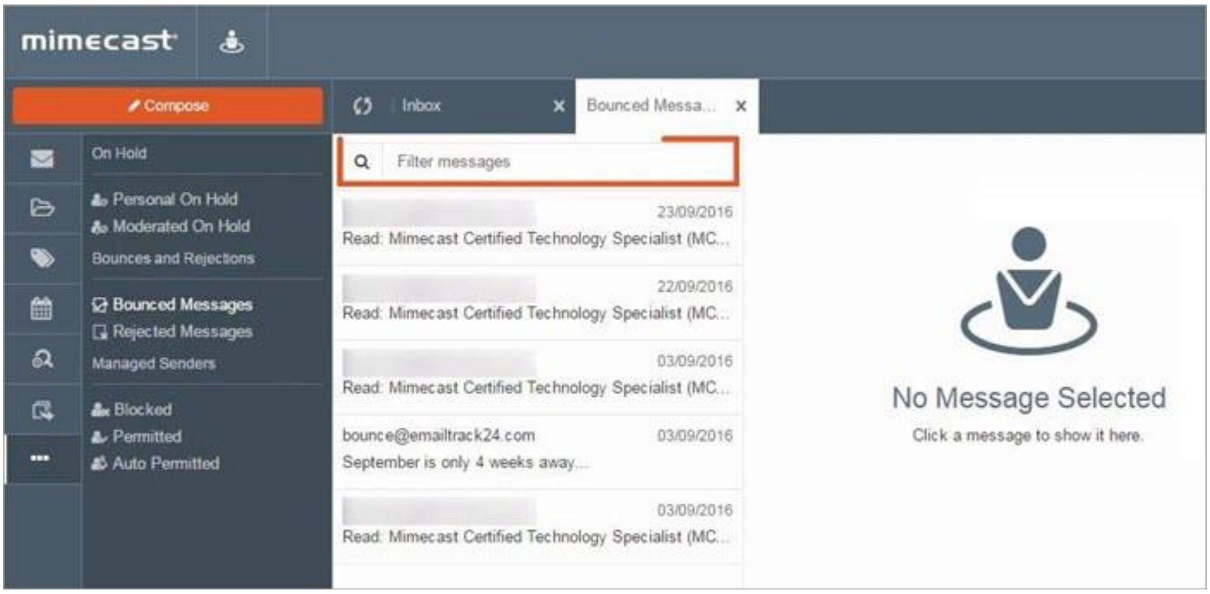
Verdict: With Perimeter 81, you get a cloud-based cybersecurity tool that boasts multiple security features that radically simplify the task of securing and managing the network. The software is also incredibly simple to deploy and use, which is precisely why we have it ranked so high on our list.

=> Visit Perimeter 81 Website

#16) Mimecast

Best for small to large businesses.

Price: You can get a quote for the pricing details. As per the reviews, the price for email security and threat protection starts at $3.50 per user per month (for 50 users).



23/09/2016
Read: Mimecast Certified Technology Specialist (MC...

22/09/2016
Read: Mimecast Certified Technology Specialist (MC...

03/09/2016
Read: Mimecast Certified Technology Specialist (MC...

bounce@emailtrack24.com 03/09/2016
September is only 4 weeks away...

03/09/2016
Read: Mimecast Certified Technology Specialist (MC...

No Message Selected
Click a message to show it here.

Mimecast is a cloud-based platform that provides you email security and cyber resilience. It provides multiple products and services like Email security with threat protection, Information protection, Web security, Cloud Archiving, etc.

Features:

- Email Security with threat protection protects from spear-phishing, ransomware, impersonation and some other types of targeted attacks.
- It has features for automated Content Control and data loss prevention.
- It provides web security by blocking inappropriate business websites and protecting against user-initiated malicious web activity & malware.
- It provides a Cloud Archiving facility to securely archive emails, files, and other data.

Category: Email Security & Compliance Platform.

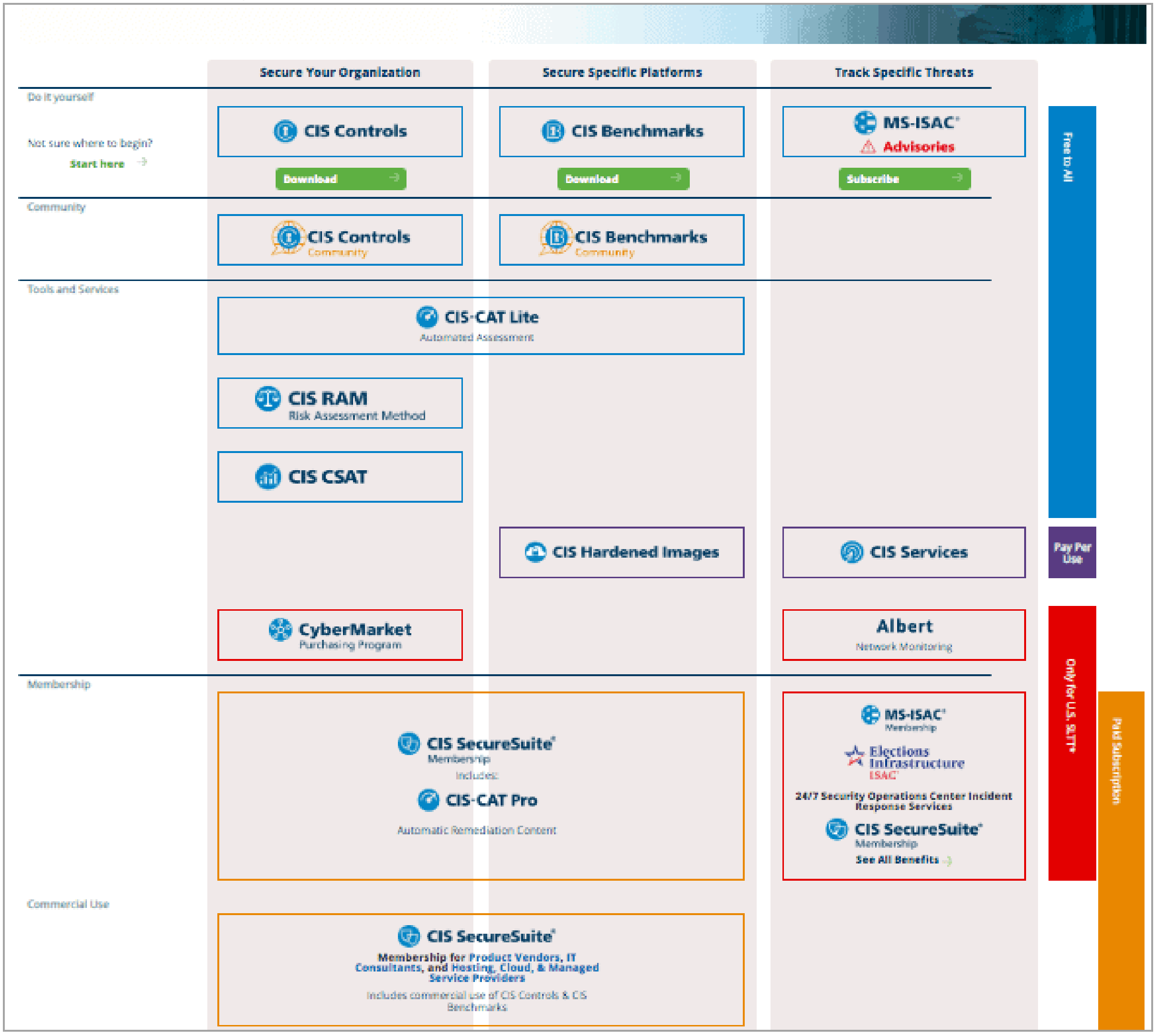
Verdict: Mimecast is good for Spam detection & blocking features and provides good email security & URL security.

Website: Mimecast

Further Reading => Most Popular Skybox Competitors of the Year

#17) CIS

Best for small to large businesses.
Price: CIS CSAT, CIS RAM, CIS-CAT Lite, CIS Controls, and CIS Benchmarks are available for free to everyone. CIS SecureSuite is available on a paid subscription. CIS Hardened Images and CIS Services are available for Pay peruse.



Secure Your Organization
Secure Specific Platforms
Track Specific Threats

Do it yourself
Not sure where to begin?
Start here
CIS Controls
Download
CIS Benchmarks
Download
MS-ISAC
Advisories
Subscribe

Community
CIS Controls Community
CIS Benchmarks Community

Tools and Services
CIS-CAT Lite
Automated Assessment
CIS RAM
Risk Assessment Method
CIS CSAT
CIS Hardened Images
CIS Services
CyberMarket
Purchasing Program
Albert
Network Monitoring

Membership
CIS SecureSuite
Membership
Includes:
CIS-CAT Pro
Automatic Remediation Content
MS-ISAC
Membership
Elections Infrastructure ISAC
24/7 Security Operations Center Incident Response Services
CIS SecureSuite
Membership
See All Benefits

Commercial Use
CIS SecureSuite
Membership for Product Vendors, IT Consultants, and Hosting, Cloud, & Managed Service Providers
Includes commercial use of CIS Controls & CIS Benchmarks

CIS stands for the Center for Internet Security. It provides various cybersecurity tools, services, and memberships. For commercial use, it provides CIS SecureSuite. CIS Security suite will include CIS controls and CIS Benchmarks.

Features:

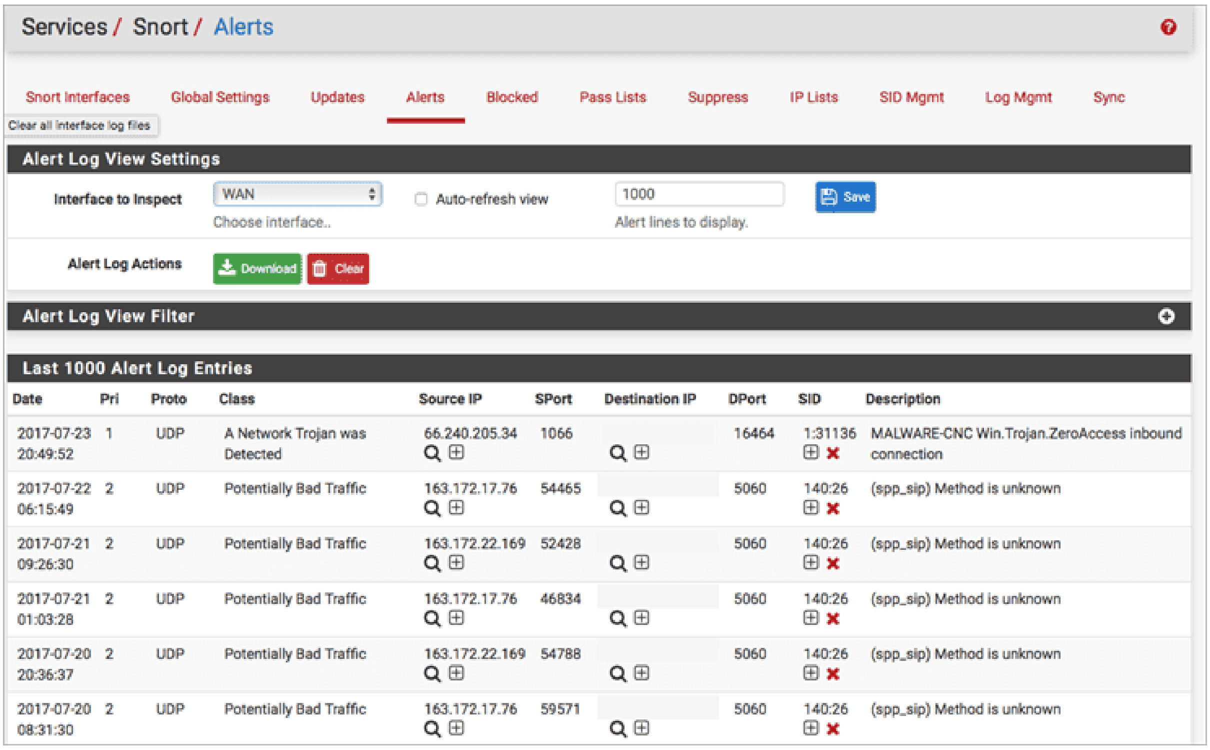
- For securing your organization, it offers a variety of products like CIS Controls, CIS-CAT Lite, CIS RAM, CIS CSAT, etc.

- CIS-CAT Lite performs an automated assessment.
- It provides 24*7 Security Operations Center and Incident Response Services.
- It provides tools like CIS-CAT Lite, CIS-CAT Pro, CIS Workbench, CIS RAM, and CIS CSAT.

Category: Cybersecurity tools
Verdict: CIS has plans for securing your organization, specific platforms, and specific threats. It provides membership to product vendors, IT consultants & Hosting, Cloud, and Managed Service Providers.
Website: **CIS**
Recommended Read **=>** **Top Penetration Testing Tools**

#18) Snort

Best for small and medium-sized businesses.
Price: Free



Alert Log View Settings

Interface to Inspect: WAN
Choose interface..
□ Auto-refresh view
1000
Alert lines to display.

Alert Log Actions

Alert Log View Filter

Last 1000 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_sip) Method is unknown

[image source]

Snort is an open-source platform. It is an application for network intrusion prevention. It supports FreeBSD, Fedora, Centos, and Windows platform. It can perform the task of watching network packets and streaming data to your screen.

Features:

- Real-time packet analysis.
- Packet logging.
- It is an Open-source platform.

Category: Network intrusion prevention system.

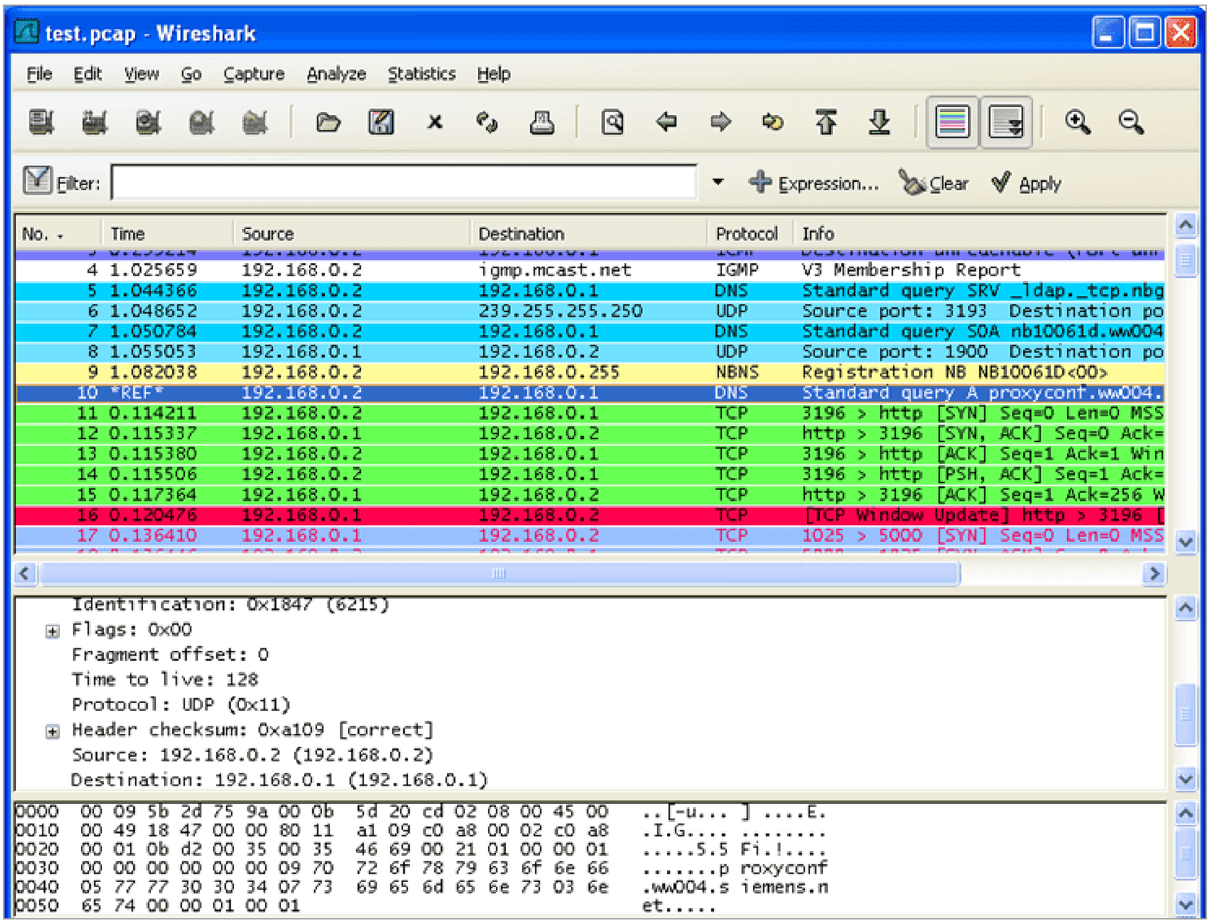
Verdict: Snort will act as the second level of defense as it sits behind the firewall. It can also compare the traffic against the set of rules.

Website: Snort

#19) Wireshark

Best for commercial and non-profit enterprises, government agencies, and educational institutions.

Price: Free



No.	Time	Source	Destination	Protocol	Info
4	1.025659	192.168.0.2	igmp.mcast.net	IGMP	V3 Membership Report
5	1.044366	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nbg
6	1.048652	192.168.0.2	239.255.255.250	UDP	Source port: 3193 Destination po
7	1.050784	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.ww004
8	1.055053	192.168.0.1	192.168.0.2	UDP	Source port: 1900 Destination po
9	1.082038	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>
10	*REF*	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.ww004.
11	0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS
12	0.115337	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=
13	0.115380	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	0.115506	192.168.0.2	192.168.0.1	TCP	3196 > http [PSH, ACK] Seq=1 Ack=
15	0.117364	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 W
16	0.120476	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196 [
17	0.136410	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Len=0 MSS

```
    Identification: 0x1847 (6215)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xa109 [correct]
    Source: 192.168.0.2 (192.168.0.2)
    Destination: 192.168.0.1 (192.168.0.1)
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 49 18 47 00 00 80 11  a1 09 c0 a8 00 02 c0 a8   .I.G.... ........
0020  00 01 0b d2 00 35 00 35  46 69 00 21 01 00 00 01   .....5.5 Fi.!....
0030  00 00 00 00 00 00 09 70  72 6f 78 79 63 6f 6e 66   .......p roxyconf
0040  05 77 77 30 30 34 07 73  69 65 6d 65 6e 73 03 6e   .ww004.s iemens.n
0050  65 74 00 00 01 00 01                               et.....
```

Wireshark network protocols analyzer supports Windows, Mac, Linux, FreeBSD, Solaris, NetBSD, etc. It has a standard three-pane packet browser. It can perform live capture and offline analysis.

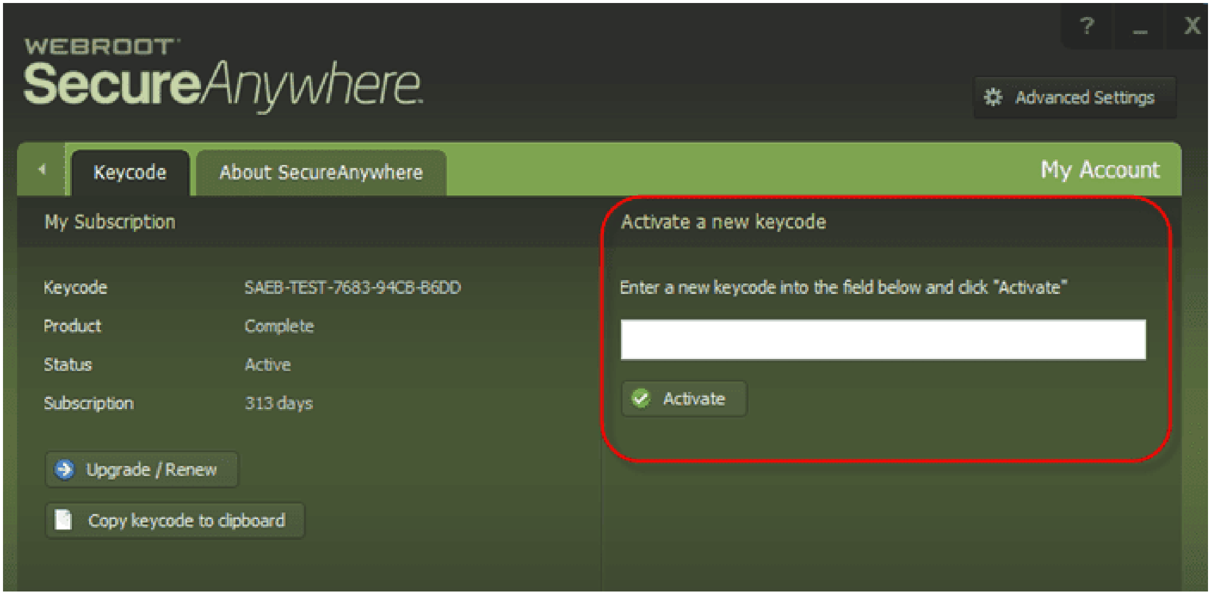
Features

- Wireshark performs deep inspection of hundreds of platforms.
- It provides powerful display filters.
- It can decompress the files that are captured with gzip.
- It supports various protocols for decryption.

Category: Network protocol analyzer.
Verdict: Wireshark will provide you detailed information about what is happening on your network. It provides decryption support for many protocols. Wireshark will allow you to export the output in XML, PostScript, CSV, or Plain Text.
Website: Wireshark

#20) Webroot

Best for small to large businesses as well as individuals.
Price: Webroot Antivirus (for PC and Mac) is available for $29.99 per device per year. Internet Security Plus which is for PC, Mac, smartphones, and tablets are available for $44.99 for 3 devices per year. Internet Security Complete comes with 25 GB of storage. It will cost you $59.99 for 5 devices per year.



My Subscription

Keycode	SAEB-TEST-7683-94CB-B6DD
Product	Complete
Status	Active
Subscription	313 days

Activate a new keycode

Enter a new keycode into the field below and click "Activate"

Webroot is a cloud-based platform. It can protect PCs, Mac computers, and mobile devices. It provides a solution for home use, home offices, businesses, and partners. It supports Windows, Mac, Android, and iOS platforms.

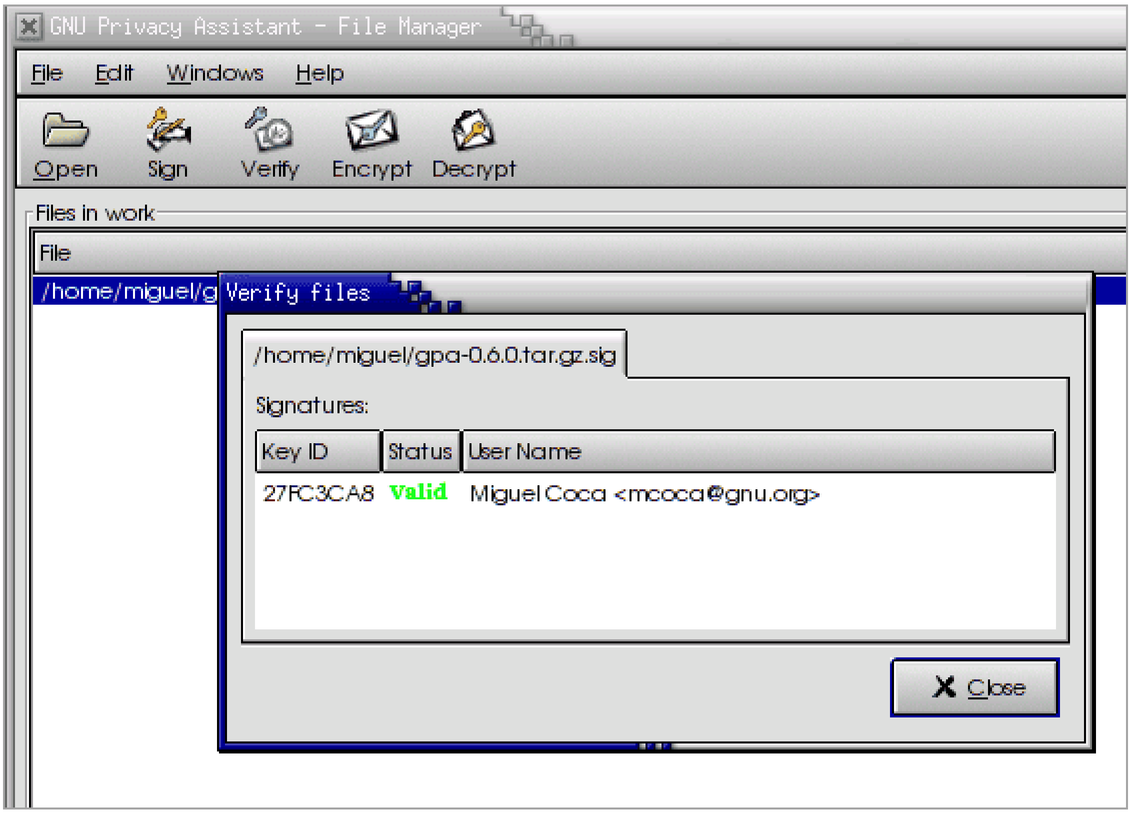
Features:

- Real-time protection against threat.
- Endpoints and networks will be protected with multi-vector protection.
- It provides cloud-based threat intelligence services.
- It offers predictive threat intelligence.

Category: Cybersecurity for endpoints, networks, PCs, & mobile devices.
Verdict: For businesses, Webroot provides DNS protection, Endpoint Protection, and threat intelligence. It also provides security awareness training to businesses. As per the customer reviews, it sometimes slows down other web applications but provides good protection to the network.
Website: **Webroot**
Suggested Read **=> Best Vulnerability Assessment Tools**

#21) GnuPG

Best for small to large businesses.
Price: Free



/home/miguel/gpa-0.6.0.tar.gz.sig

Signatures:

Key ID	Status	User Name
27FC3CA8	Valid	Miguel Coca <mcoca@gnu.org>

GnuPG is a tool for encryption and signing of data and communications. It supports Windows, Mac, and Linux platforms.

Features:

- Versatile key management system.
- It has access modules for all types of public key directories.
- It can be easily integrated with other systems.
- S/MIME and Secure Shell are supported by GnuPG.

Verdict: GnuPG is a free tool for encryption of data with a lot of features like key management and access to public key directories. It has good customer reviews for data encryption.

Website: GnuPG

#22) BluVector

Best for medium to large organizations.

Price: You can get a quote for its pricing details.

BluVector provides real-time advanced threat detection. This Network Intrusion Detection System is based on Artificial Intelligence, Machine Learning, and speculative code execution.

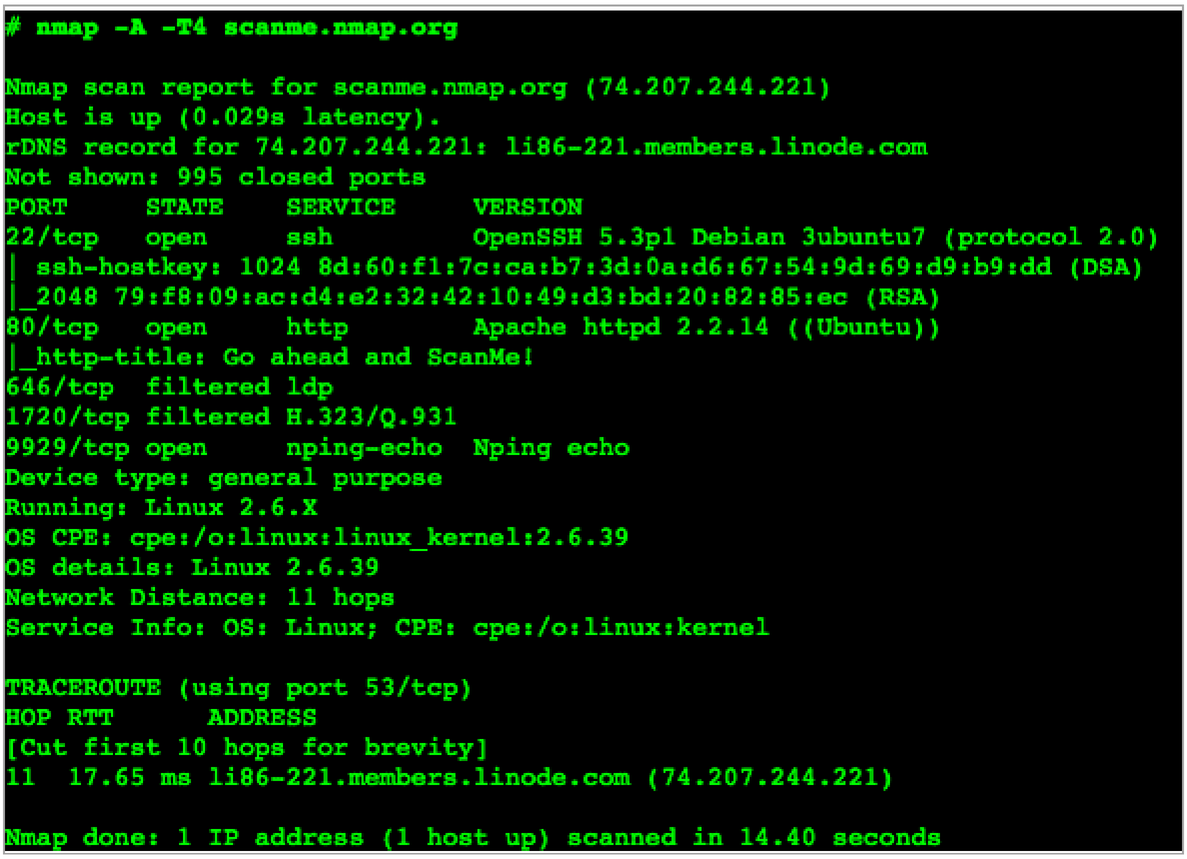
Features:

- BluVector Cortex can respond to file-less and file-based malware.
- Threats like Zero-day malware and ransomware can also be detected, analyzed, and contained in real-time.
- BluVector Cortex is composed of three components i.e. AI-based Detection Engines, Intelligent Decision Support, and Connectors Framework.

Verdict: BluVector Cortex is an AI-driven security platform. It has flexible deployment options. It provides 100% network coverage and can be used by any sized organization.
Website: **BluVector**

#23) NMap

Best for scanning large networks as well as single hosts.
Price: Free and open source.



```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

NMap is a port scanning tool. It is used for network discovery and security auditing. It can be used for Network Inventory and managing service upgrade schedules. It will also help you with monitoring host or service uptime.

Features:

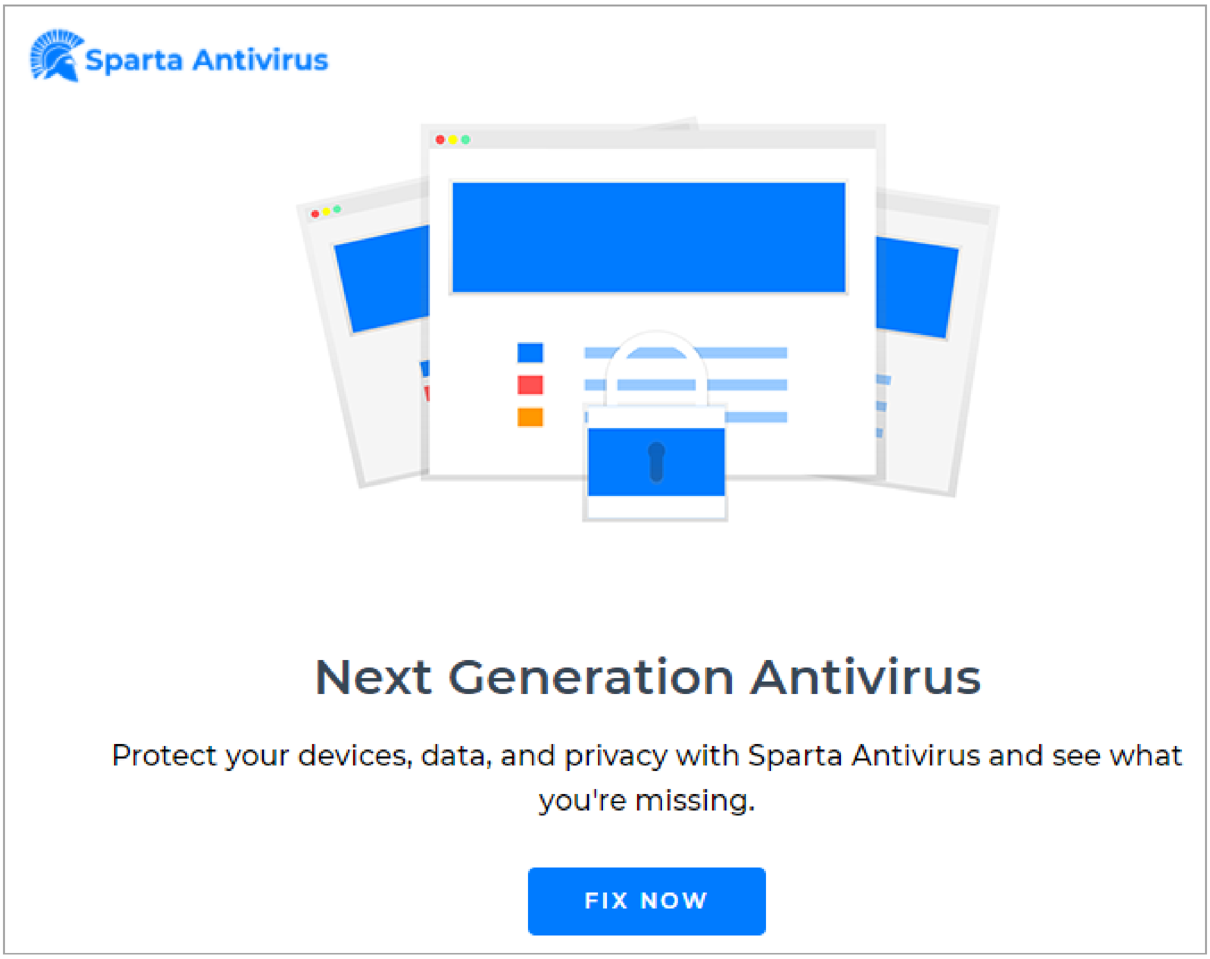
- It has a command-line interface as well as GUI.
- It supports cross-platform.
- It can scan huge networks.
- It provides support to various advanced techniques.

Verdict: Nmap is a powerful, flexible, easy, and free tool with support for various port scanning mechanisms. Nmap suite includes a variety of tools like Zenmap, Ncat, Ndiff, and Nping.

Website: NMap

#24) Sparta Antivirus

Best For Removing Malware and Fixing your PC or Mac with One Click.



Next Generation Antivirus

Protect your devices, data, and privacy with Sparta Antivirus and see what you're missing.

Sparta Antivirus provides a full range of security for your total protection. The system is designed with the latest technology of AI that will keep your environment clean from all possible threats.

Keep all your online data safe from malware, viruses, trojans, phishy websites, and more. Ultimate protection for you and your loved ones.

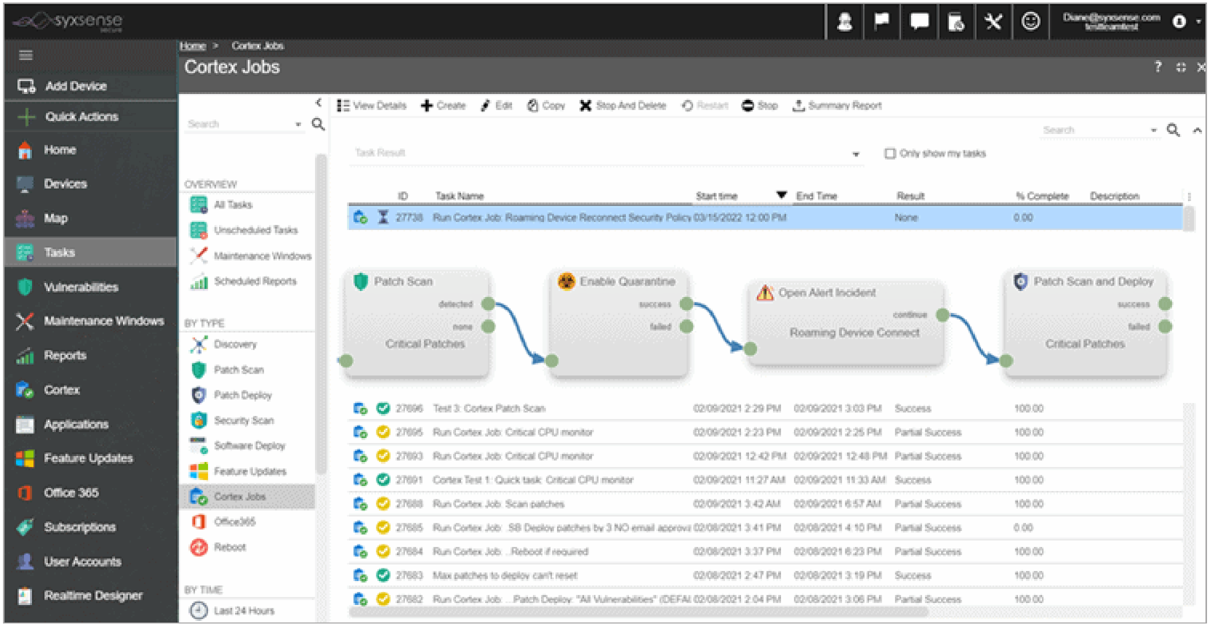
Features:

- Prevent malware attacks
- Optimize your system for peak results.
- Detect and block all cyber threats.
- Generate reports

Cons: Available in English language only.

#25) Syxsense

Best for Small to Large Businesses.
Price: Starts at $960 per year for 10 devices.



ID	Task Name	Start time	End Time	Result	% Complete	Description
27738	Run Cortex Job: Roaming Device Reconnect Security Policy	03/15/2022 12:00 PM		None	0.00	
27696	Test 3: Cortex Patch Scan	02/09/2021 2:29 PM	02/09/2021 3:03 PM	Success	100.00	
27695	Run Cortex Job: Critical CPU monitor	02/09/2021 2:23 PM	02/09/2021 2:25 PM	Partial Success	100.00	
27693	Run Cortex Job: Critical CPU monitor	02/09/2021 12:42 PM	02/09/2021 12:48 PM	Partial Success	100.00	
27691	Cortex Test 1: Quick task: Critical CPU monitor	02/09/2021 11:27 AM	02/09/2021 11:33 AM	Success	100.00	
27688	Run Cortex Job: Scan patches	02/09/2021 3:42 AM	02/09/2021 6:57 AM	Partial Success	100.00	
27685	Run Cortex Job: .SB Deploy patches by 3 NO email approva	02/08/2021 3:41 PM	02/08/2021 4:10 PM	Partial Success	0.00	
27684	Run Cortex Job: ..Reboot if required	02/08/2021 3:37 PM	02/08/2021 6:23 PM	Partial Success	100.00	
27683	Max patches to deploy can't reset	02/08/2021 2:47 PM	02/08/2021 3:19 PM	Success	100.00	
27682	Run Cortex Job: ...Patch Deploy: "All Vulnerabilities" (DEFAU	02/08/2021 2:04 PM	02/08/2021 3:06 PM	Partial Success	100.00	

Syxsense Secure provides Security Scanning, Patch Management, and Remediation in one console from the cloud, allowing IT and Security teams to stop breaches with one endpoint security solution.

Features:

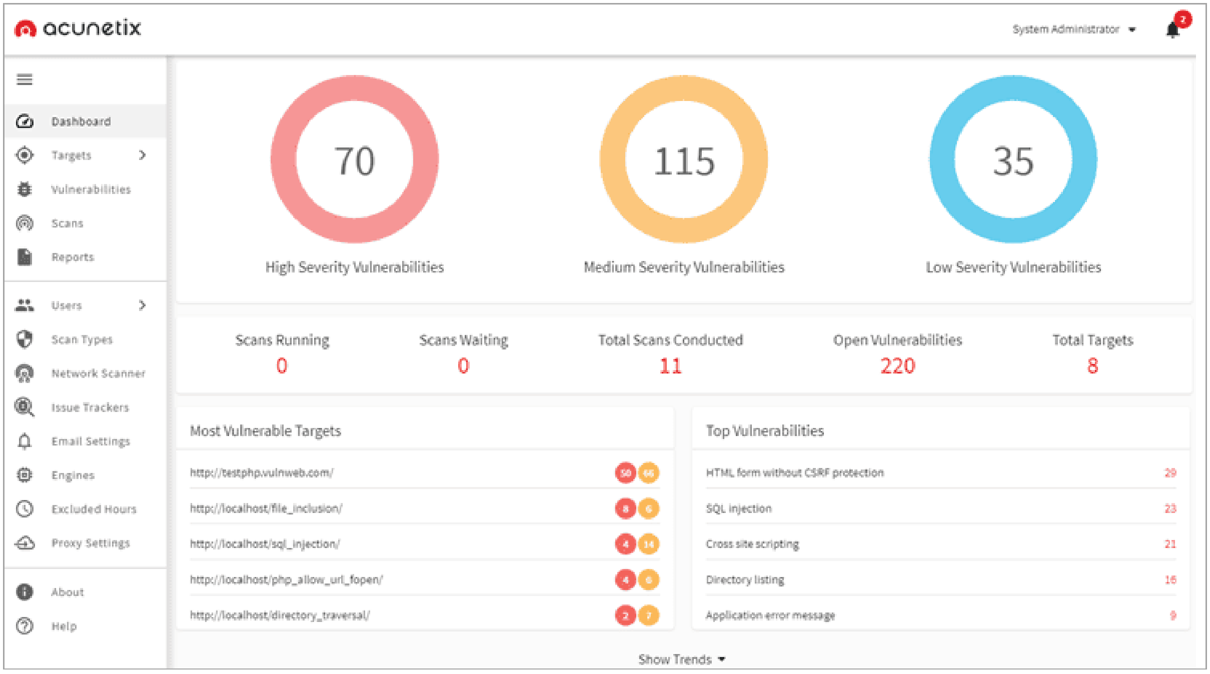
- **Scan for Vulnerabilities:** Prevent cyber-attacks with insights from our security scanner by scanning authorization issues, security implementation, and antivirus status.
- **Patch Everything:** With support for all major operating systems, automatically deploy OS and third-party patches as well as Windows 10 Feature Updates.
- **Quarantine Devices:** Block communication from an infected device to the internet, isolate the endpoint, and kill malicious processes before they spread.

Verdict: For the first time, IT and security teams can automatically collaborate in a single console to know and close attack vectors.

#26) Acunetix

Best for small businesses, enterprise customers, pentesters, and web professionals.

Price: Acunetix offers a solution with three pricing plans: Standard, Premium, and Acunetix 360. You can get a quote for pricing details. A demo is also available on request.



70 High Severity Vulnerabilities

115 Medium Severity Vulnerabilities

35 Low Severity Vulnerabilities

Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities	Total Targets
0	0	11	220	8

Most Vulnerable Targets		
http://testphp.vulnweb.com/	50	66
http://localhost/file_inclusion/	8	6
http://localhost/sql_injection/	4	14
http://localhost/php_allow_url_fopen/	4	6
http://localhost/directory_traversal/	2	7

Top Vulnerabilities	
HTML form without CSRF protection	29
SQL injection	23
Cross site scripting	21
Directory listing	16
Application error message	9

Acunetix is the solution to secure your websites, web applications, and APIs. This application security testing solution can find over 7K vulnerabilities and scan all pages, web apps, and complex web applications.

It has built-in vulnerability management functionality. On-premise and on-demand deployment options are available with Acunetix.

Features:

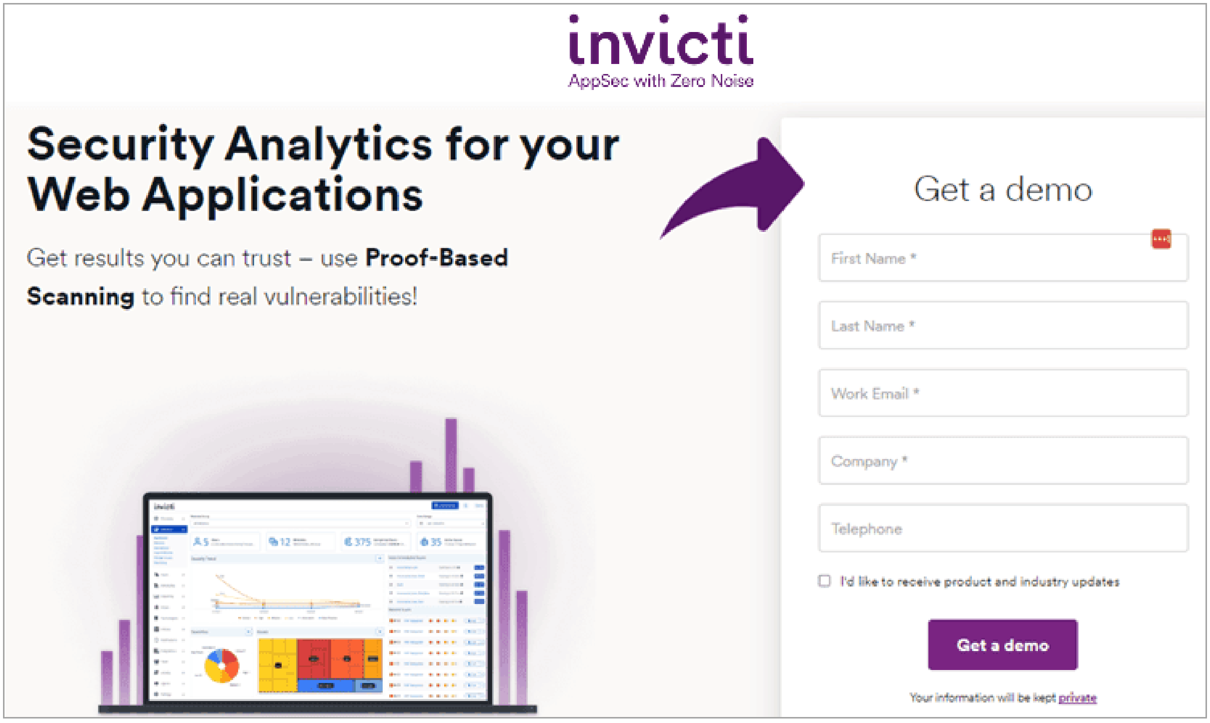
- Acunetix makes use of advanced macro recording technology that will be helpful for scanning complex multi-level forms and password-protected areas of the site.
- It performs the assessment for the severity of the issue and provides actionable insights immediately.
- It provides the functionalities for scheduling & prioritizing the full scans/incremental scans.

Category: On-premise as well as cloud-based Web Application Security Scanner.

Verdict: Acunetix is an intuitive and easy-to-use solution. It performs lightning-fast scanning. Acunetix can get seamlessly integrated into your current systems.

#27) Invicti (formerly Netsparker)

Best for small to large businesses.
Price: You can get a quote for pricing details. It offers the solution with three pricing plans, Standard, Team, and Enterprise.



invicti
AppSec with Zero Noise

Security Analytics for your Web Applications

Get results you can trust – use **Proof-Based Scanning** to find real vulnerabilities!

Get a demo

First Name *

Last Name *

Work Email *

Company *

Telephone

☐ I'd like to receive product and industry updates

Get a demo

Your information will be kept private

Invicti is an application security testing solution for enterprises. It offers the features and functionalities for automating security testing throughout the SDLC. Invicti has capabilities of automation, visibility, accuracy, scalability, and security.

Features:

- Invicti assists developers with writing the more secure code in the current environment.
- It performs comprehensive scanning and can detect vulnerabilities quickly.
- It has features of combined signature and behavior-based testing.
- It follows a unique dynamic and interactive scanning approach that can find more true vulnerabilities.

Category: Cloud-based and on-premise web application security for enterprise.
Verdict: Invicti web application security solution provides the complete picture of your application security. It provides onboarding assistance and

training. Its unique DAST + IAST approach will give you increased visibility deeper scans.

#28) Intego

Best for Small to Large businesses, Home use

Price: Produce prices start at $39.99 per year. 14-day free trial available

Intego offers a comprehensive suite of solutions that are designed to keep Mac and Windows systems safe from all forms of threats. There is an anti-virus solution that renders real-time threat protection. Then we also have the Net Barrier that facilitates advanced firewall protection. There is also a VPN that can be used for internet privacy.

Features:

- Ransomware protection
- VPN
- Advanced Firewall protection
- Zero-day protection
- Set parental controls

Verdict: Intego's comprehensive suite of cyber-security solutions does a good job of keeping users and their devices protected from all sorts of online and offline threats 24/7. The tools are affordable, easy to set up, and further bolstered with excellent customer support.

Conclusion

We have reviewed the top Cybersecurity software tools and saw the importance of cybersecurity. Gnu Privacy Guard, Wireshark, Snort are free cybersecurity tools. CIS offers some products and services for free. Mimecast provides Email security with good spam detection and blocking capabilities. Snort is a completely free platform for real-time packet analysis.

Suggested reading =>> Top 10 Folder Lock Software

Webroot provides security solutions for businesses as well as individuals. For businesses, it provides multiple solutions like DNS protection and Endpoint Protection.

SolarWinds Threat Monitor is a cloud-based solution that enables Managed Service Providers to offer an all-in-one solution. Norton provides a variety of solutions for cybersecurity like VPN, Antivirus, Password Manager, etc.

Hope this article would provide the necessary guidance to select the right CyberSecurity Software for your business or personal use.

Further reading =>> Popular Antivirus Software for Mac

=>> Contact us to suggest a listing here.