OVERVIEW

VULNERABILITY & PATCH MANAGEMENT

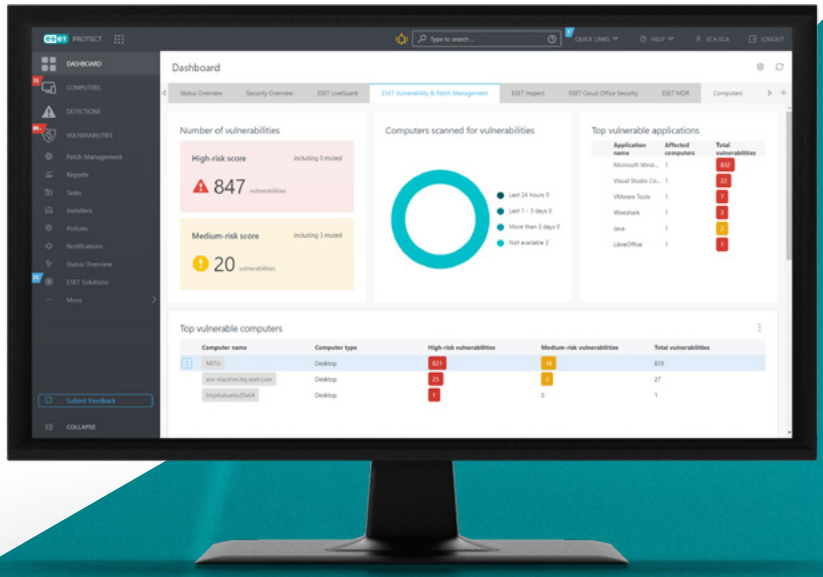
Actively track and fix vulnerabilities across all your endpoints

Progress. Protected.

What is **ESET Vulnerability and Patch Management?**

ESET Vulnerability & Patch Management actively tracks vulnerabilities in operating systems and common applications and enables automated patching across all endpoints managed through our unified platform.

Automated scanning of your endpoints' software and third-party applications, with instant reporting to the console, provides immediate visibility of vulnerabilities. To ensure continuous protection for your business, you can configure auto-patching by selecting a patching strategy (all, only allowed, or all but excluded) and defining specific time slots for when patching should occur.



Timely patching of your operating systems and applications

The patching of security holes in operating systems and applications is critical and remains one of the most time-consuming tasks in IT. ESET Vulnerability & Patch Management provides an additional layer of security to organizations that need their applications to be up to date, but who lack IT resources. It detects vulnerabilities and eliminates or mitigates them from being exploited by installing the latest patches for apps and operating systems across all endpoints.

ESET Vulnerability & Patch Management uses advanced prioritization techniques and automated workflow tools to best meet your infrastructure needs.

It is part of the ESET PROTECT Platform and, as such, it not only delivers continuous vulnerability assessment with risk-based prioritization and remediation, but also protects against threats that extend well beyond software vulnerabilities. It provides you with enterprise-grade protection against malware of all types, including ransomware, and zero-day threat prevention across all endpoints, servers, and emails—all via a single, unified solution.

Key Features

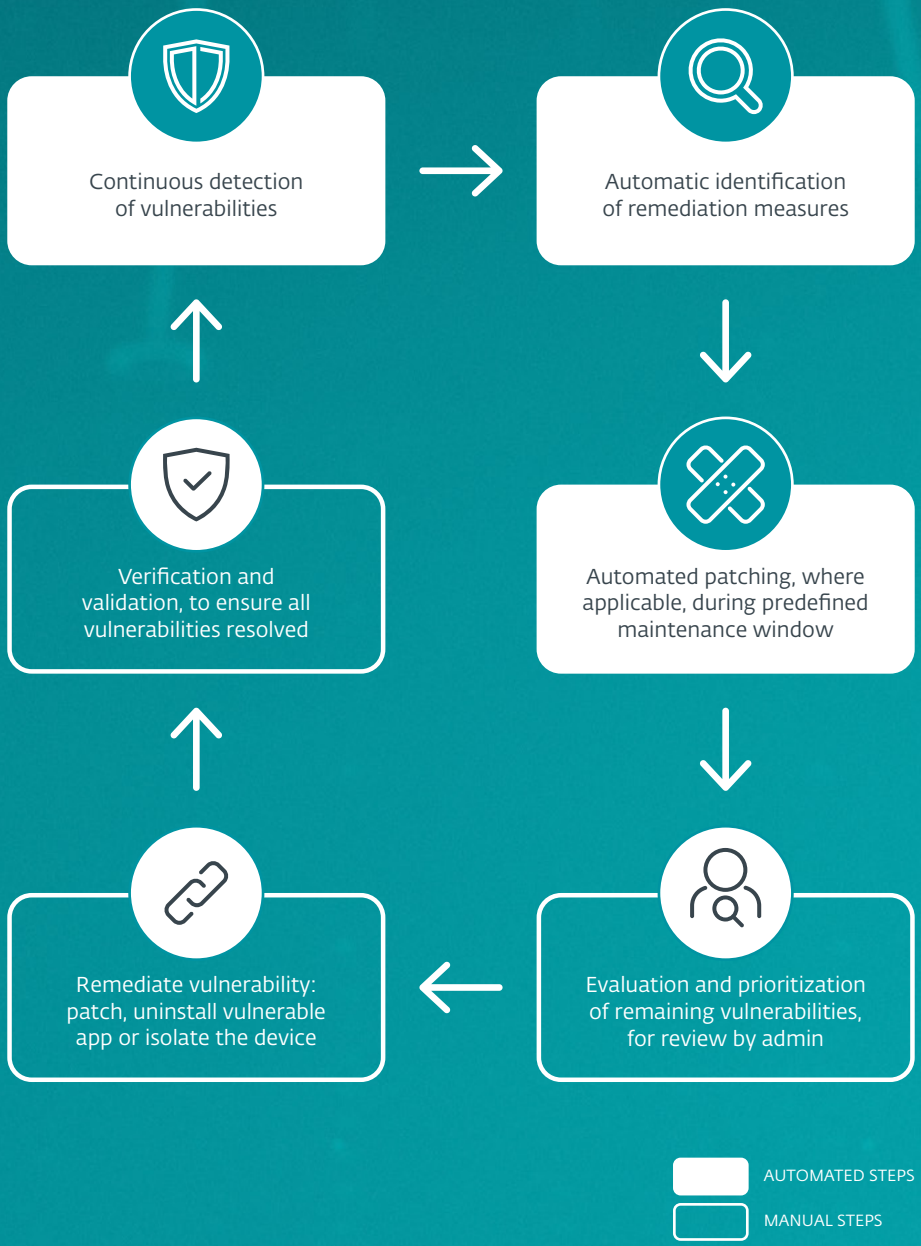
Vulnerability assessment

- Scans thousands of applications, such as Adobe Acrobat, Mozilla Firefox and Zoom Client, and supports multiple versions of Windows, Linux and macOS
- Detects over 35,000 common vulnerabilities and exposures (CVEs) – with more added as they are identified
- Automated scans with customizable schedule settings
- Prioritizes and filters vulnerabilities by exposure score and severity
- Vulnerability reports of most-vulnerable software and devices
- Supports multitenancy in complex network environments and enables visibility of vulnerabilities in specific parts of the organization
- Unified overview via the ESET PROTECT console, with multilingual support and light demands on your IT infrastructure

Patch management

- Launch immediate updates and patching via customizable options or manually
- Simplify your patching process: prioritize critical assets and schedule the remainder for off-peak times to avoid interruption.
- Register and track exceptions for patches of selected applications
- Provides an updated inventory of patches with patch name, new version of app, CVE, patch severity/importance, affected applications
- All patches available via the ESET PROTECT console

How does it work?



Use Cases

Even though the increasing number of remote workers and growing adoption of cloud services means that threat exposure has diversified beyond software vulnerabilities, timely patching of applications and operating systems remains critical for preventing security breaches.

As any admin will tell you, patching vulnerabilities is one of the most time-consuming tasks in IT. So when resources are stretched, patching tends to get postponed and vulnerabilities can develop almost unseen. Growing IT complexity can also lead to degraded coordination among cross-functional teams, gaps in inventory and limited visibility of the threat landscape.

You're behind with patching

PROBLEM

Your IT team is overloaded, and thus behind with patching

SOLUTION

Benefit from advanced prioritization and automation techniques

- ✓ Set optimal scan frequencies, and synchronize them with patching set-ups in order to address relevant and exploitable vulnerabilities without overloading your IT teams
- ✓ Filter vulnerabilities based on their severity; prioritize vulnerabilities that pose significant business risks
- ✓ Customize your patching policies. Prioritize critical assets by manually addressing severe vulnerabilities, then automate patching of other assets to take place at off-peak times to avoid interruptions
- ✓ Register and track exceptions for patches; avoid having to track every single patch

Shortage of IT resources

PROBLEM

You need your applications to be up to date, but you lack IT resources

SOLUTION

Benefit from fully automated vulnerability assessment and patch management, and ESET support:

- ✓ Automated scanning of your endpoints' software and third-party applications, with instant reporting to the console, for immediate visibility of vulnerabilities
- ✓ To ensure continuous protection for your organization, configure auto-patching by selecting a patching strategy (all, only allowed, or all but excluded) and define specific time slots for when patching should occur

Growing complexity, coordination challenges

PROBLEM

The complexity of your IT continues to grow, making coordination among cross-functional teams harder

SOLUTION

Benefit from our ESET PROTECT Platform, which allows you to manage ESET Vulnerability & Patch Management and the wider security of all your digital assets and inventory

- ✓ Centralize and automate multiple IT security and management tasks with the ESET PROTECT Platform, which includes ESET Vulnerability & Patch Management. Decrease the complexity of your IT management
- ✓ Take advantage of the ESET Vulnerability & Patch Management multitenancy functionality: enjoy full visibility over the entire network, yet be focused on your dedicated area
- ✓ Maintain up-to-date inventory and close any infrastructure blind spots
- ✓ Benefit from the prevention, detection, and response strategies of ESET PROTECT to minimize your exposure to threats that go beyond software vulnerabilities
- ✓ ESET Vulnerability & Patch Management simplifies your compliance with NIS2, FedRAMP, HIPAA, PCI DSS, and other data security requirements from industry, government, and regulatory bodies

Limited visibility of your IT stack

PROBLEM

You don't have full visibility of the security of my IT stack

SOLUTION

Benefit from the single pane of glass unified view that you get with the ESET PROTECT console

- ✓ Get full visibility of your organization's endpoints, licenses, and vulnerability and patching statuses across your asset inventory, always kept up to date
- ✓ View the real-time status of your IT security via the ESET PROTECT console
- ✓ Connect anytime, anywhere, from your favorite web browser—allowing you to respond instantly
- ✓ Create relevant reports to measure the effectiveness and progress of your vulnerability and patch management policies

How to buy:

The ESET Vulnerability & Patch Management module comes as part of these subscription tiers:

- PROTECT COMPLETE
- PROTECT ELITE
- PROTECT MDR
- PROTECT MDR ULTIMATE

For other purchase options, contact your ESET representative.

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats—targeted attacks, zero-day threats, ransomware, phishing, and more—with our AI-Native, prevention-first approach. ESET combines the power of AI and human expertise to deliver easy and effective protection.

Experience best-in-class, science-driven security, backed by over 30 years of in-house global cyber threat intelligence. Our extensive R&D network, led by industry-acclaimed researchers, powers our award-winning, cloud-first cybersecurity platform. ESET solutions are highly customizable, include local support, and have minimal impact on performance.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+
protected internet users

500k+
business customers

178
countries

11
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,500 devices

BVB 09

protected by ESET since 2019
1,200 devices & 2,700 mailboxes

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 23,000 devices

protected by ESET since 2008
2 million customer base

RECOGNITION

SE LABS ® AWARDS
Enterprise Endpoint (Windows)
WINNER 2025

Winner of the **Best Enterprise Endpoint** and **Best Small Business Endpoint** awards at the SE LABS Awards 2025

Gartner Peer Insights **Customers' Choice** 2026

Named a **Customers' Choice** in Gartner® Peer Insights™ **"Voice of the Customer" Endpoint Protection Platforms** report 2026

FROST & SULLIVAN

Named a **Leader** in Frost Radar: Endpoint Security 2025, demonstrating excellence in growth & innovation