OVERVIEW

CLOUD WORKLOAD PROTECTION

Protect cloud virtual machines
from advanced cyber threats

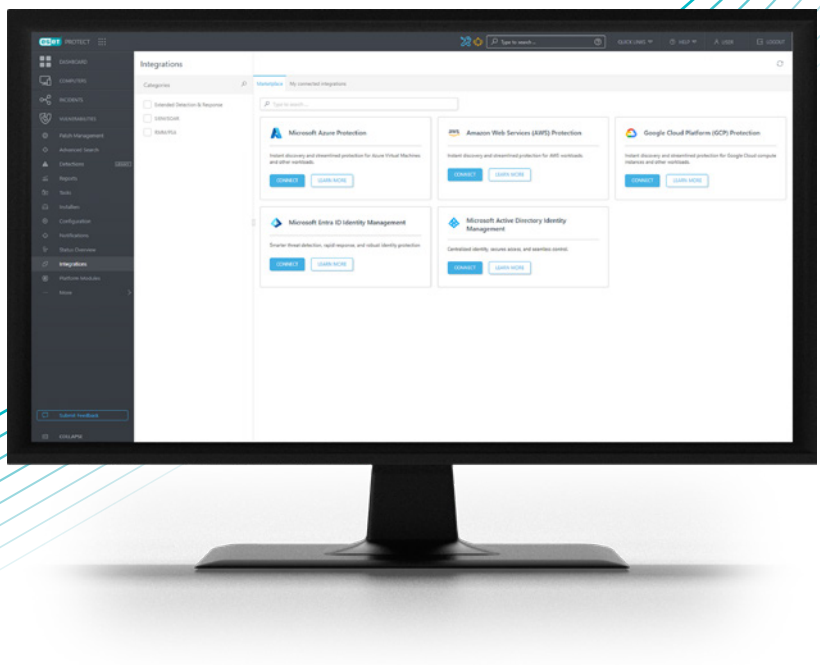


Progress. Protected.

What is **ESET Cloud Workload Protection?**

ESET Cloud Workload Protection (CWP) provides AI-powered, multilayered protection for virtual machines (VMs) in public cloud environments to prevent malware, stop cyberattacks and minimize downtime across workloads.

It's a cybersecurity solution designed to protect workloads, specifically virtual machines, running in Amazon Web Services, Microsoft Azure or Google Cloud Platform environments. CWP provides visibility, threat detection, and runtime protection against vulnerabilities and cyberattacks targeting cloud-hosted applications.



This solution is delivered as a service and managed via a unified ESET PROTECT Web Console that's accessible anywhere.

Why is reinforcing the security of the cloud critical?

80% of organizations[1] regard the public cloud as crucial to their digital business initiatives. Cloud usage continues to grow and is rapidly becoming the new normal. Recent industry research shows that the majority of organizations have already experienced cloud-related security breaches. With the average cost of a public cloud data breach reaching $5.17 million[2], cloud security is no longer optional—it's mission-critical.

Cloud environments bring incredible agility, but also growing complexity. Workloads are dynamic, distributed, and often invisible to traditional security tools. Attackers know this. They're targeting cloud workloads with increasing sophistication—causing downtime, data loss, and lasting reputational damage.

Key pain points to address

- Inconsistent security across environments
- Fast spread of cyber threats from the cloud
- Efficiency and compliance challenges

Key benefits to gain

✓ SIMPLICITY

Enjoy seamless integration with public cloud providers (AWS, Azure, and GCP). Use the ESET PROTECT console for easy centralized cloud VMs and endpoint management. Licensing is simple—get one subscription for endpoint and cloud VMs security as required.

✓ EFFECTIVENESS

Proven technology provides real-time detection and automated threat prevention that goes far beyond native cloud security. A lightweight agent is deployed on your VMs to achieve increased security for your assets without compromising system performance.

✓ FLEXIBILITY

Scale your security as you grow or as your requirements change. Mix and match unit counts with endpoints in a hybrid cloud setup or multi-cloud environments.

[1] Gartner: Solution Path for Security in the Public Cloud Report, March 2025

[2] 2025 IBM Cost of a Data Breach Report

eset Cybersecurity
Progress. Protected.

Use Cases

Costly disruptions or downtime?

You want to be agile and benefit from the power of the cloud, but without proper protection, a single ransomware or malware attack can halt operations and lead to expensive downtime.

Problem: Unprotected cloud VMs are vulnerable to ransomware and malware infections. A single breach can halt operations, cause data loss, and lead to expensive downtime.

Solution: ESET Cloud Workload Protection delivers real-time, agent-based protection for cloud VMs across Azure, AWS, and GCP. Integrated XDR capabilities detect anomalies early, minimizing operational risk.

PROTECTION APPLIED:

- Advanced malware detection and exploit blocking
- XDR monitoring for suspicious file executions
- Automated remediation policies or dedicated MDR service

Data breaches and rapid attack escalation?

You want to scale securely in the cloud, but without strong security measures and real-time visibility, attackers can quickly compromise exposed workloads.

Problem: SMBs scaling workloads to cloud VMs face similar risks as traditional endpoints but are often more exposed due to constant connectivity. Without overseeing processes, behaviors, and lateral movement attempts, advanced attacks can escalate quickly.

Solution: ESET Cloud Workload Protection extends full XDR capabilities to cloud-based virtual machines. It provides deep visibility by continuously collecting rich, low-level telemetry and security signals, enabling security teams to detect and investigate advanced malware, fileless attacks, misuse of legitimate tools, and suspicious user or application behavior in real time.

PROTECTION APPLIED:

- Host Intrusion Prevention System (HIPS)
- XDR correlation of login attempts and privilege changes
- Network Attack Protection to block suspicious outbound traffic

Losing visibility and control?

Hybrid environments add complexity. Securing on-premises endpoints and cloud VMs without the right tools leaves gaps in monitoring and management, making it harder to stop threats before they strike.

Problem: SMBs often lack centralized visibility across on-premises and cloud workloads, leaving blind spots that attackers exploit. Fragmented security tools make it impossible to assess the full attack surface.

Solution: ESET CWP integrates with ESET PROTECT to provide a single console for complete visibility and control over all workloads (on-premises and cloud). Automated policies ensure consistent protection across environments.

PROTECTION APPLIED:

- Centralized security management of all VMs and endpoints
- Policy-based automated deployment
- XDR telemetry for threat detection

Key features

MANAGED FROM A UNIFIED CONSOLE

All ESET cloud VMs, endpoints, and mobiles can be managed from ESET PROTECT, our cloud-based or on-prem unified management console.

RANSOMWARE SHIELD & REMEDIATION

An additional layer of defense protecting users from ransomware, fused with a comprehensive rollback through seamless, automated file restoration from secure backups.

BLOCK TARGETED ATTACKS

ESET's protection uses threat intelligence based on its global presence to prioritize and effectively block the newest threats before their delivery anywhere else in the world.

PREVENTION-FIRST MULTILAYERED TECHNOLOGY

Developed over decades, ESET's AI-powered technology delivers an award-winning detection engine and protection core validated by customers worldwide.

ADVANCED THREAT DEFENSE

Cloud-based technology that uses advanced scanning, cutting-edge Machine learning, cloud sandboxing and in-depth behavioral analysis to prevent targeted attacks and new, never-before-seen threats. ESET LiveGuard Advanced provides proactive threat prevention against zero-day attacks with autonomous remediation.

SEAMLESS INTEGRATION

1-2-3-click activation of the security offering on your selected cloud VMs. Simply connect to the ESET PROTECT integration with Amazon Web Services, Microsoft Azure or Google Cloud Platform.

EXTENDED VISIBILITY AND XDR

Cloud telemetry from VMs and the cloud itself is ingested into the ESET PROTECT XDR module of the platform for admins to control and automate incident response actions and threat hunting.

ADD-ON MDR SERVICE

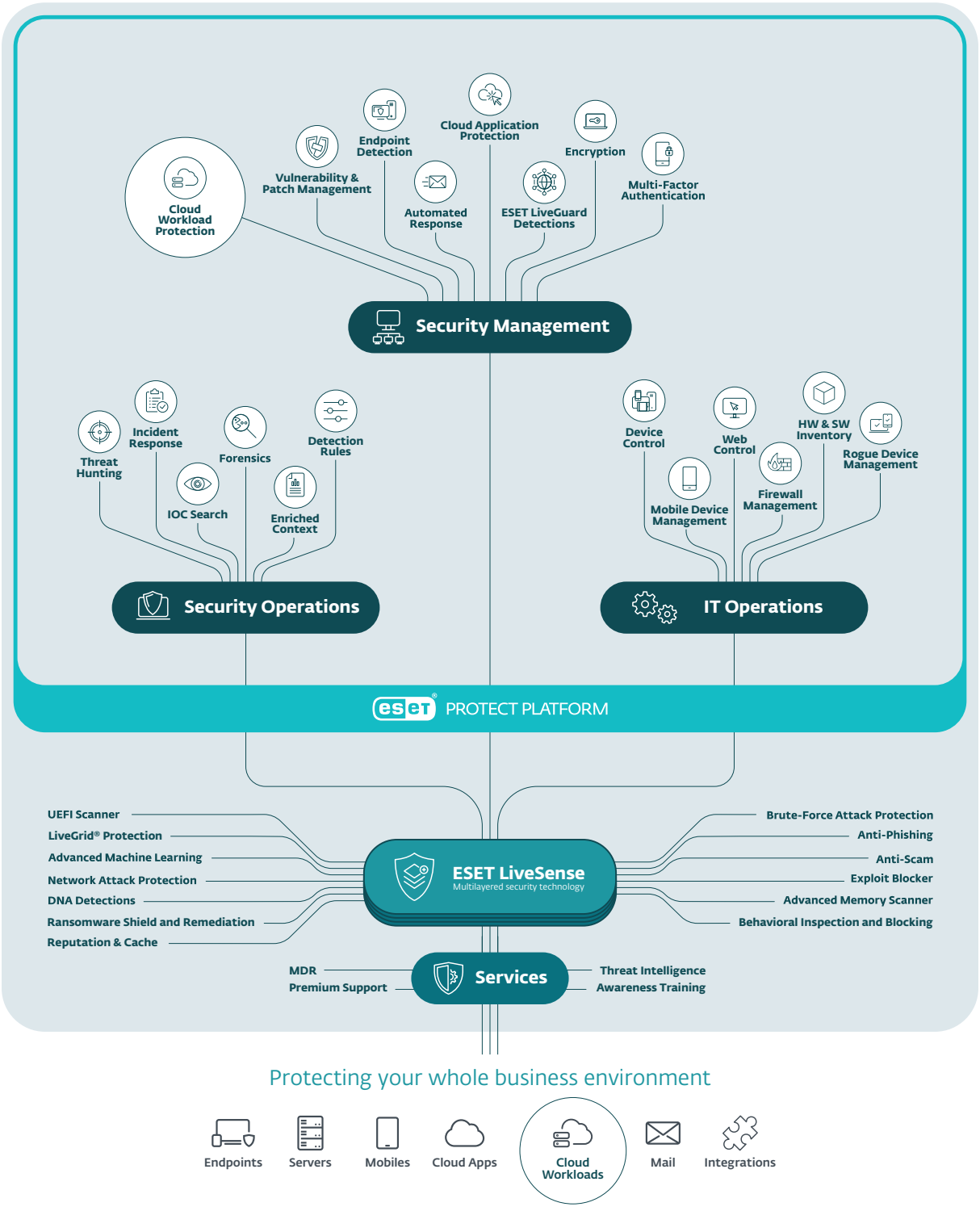
MANAGED DETECTION AND RESPONSE FOR CLOUD

Rely on the ESET experts who monitor your hybrid or cloud environment 24/7 and provide the incident response service, stopping threats or malicious activity almost instantly. Mitigate cybersecurity skill gaps and free up your IT resources to focus on your core business.



ESET PROTECT Platform ecosystem

How Cloud Workload Protection fits into the security ecosystem and what cybersecurity needs the platform can address.



Cybersecurity
Progress. Protected.

TRY BEFORE YOU BUY

Test our advanced Cloud Workload Protection for virtual machines on AWS, Azure, or GCP and see how quick and easy it is to deploy. Experience its reliability, convenience, and ease of management. Contact our experts to request a free trial of an ESET PROTECT tier listed below.

Included in:

- ✓ **ESET PROTECT Advanced**
- ✓ **ESET PROTECT Complete**
- ✓ **ESET PROTECT Enterprise**
- ✓ **ESET PROTECT Elite**
- ✓ **ESET PROTECT MDR**
- ✓ **ESET PROTECT MDR Ultimate**

eset Cybersecurity
Progress. Protected.

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 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Canon Marketing Japan Group

protected by ESET since 2016
more than 23,000 endpoints

ISP security partner 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

Gartner and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.