Bitdefender GravityZone EASM – Frequently Asked Questions (FAQ)

What is GravityZone EASM and how does it work?

Q1: How does GravityZone EASM work?

A: GravityZone EASM continuously scans the internet for assets associated with the organization using publicly available data, DNS records, or SSL certificates. It identifies internet-facing systems, detects vulnerabilities and misconfigurations for these assets.

Q2: What kind of input does GravityZone EASM require?

A: While you can start by entering known assets (like a domain, IPv4 address, IPv6 address, and email addresses), the system is designed to discover additional assets automatically over time. This includes stray assets you might not be aware of. You can:

- Start with minimal input (e.g. a few domains).
- Mark discovered assets as ones you want to monitor and extend the search to, or as assets you want to exclude from scanning.
- Add relevant found assets to the scan seeds for better future visibility.

You don't need to enter all infrastructure for EASM to provide value — it evolves with continuous discovery.

Q3: What is Shadow IT?

A: All the hardware, software, or services used within an organization without the knowledge of the IT security teams are considered Shadow IT. These assets can be a big security risk because they often skip standard security checks and monitoring.

Shadow IT assets, especially those exposed to the internet, pose higher security risks due to the fact that they are usually missing proper security controls and are not monitored by security teams.

GravityZone EASM uncovers these assets and identifies vulnerabilities and misconfigurations, helping organizations reduce risks.

Q4: What kind of Shadow IT can GravityZone EASM identify?

A: GravityZone EASM helps uncover shadow IT by detecting unknown or unmanaged internet-facing assets, such as forgotten test environments, marketing campaign subdomains, cloud services created outside approved processes, and third-party assets tied to the organization brand or infrastructure.

Q5: What is Bitdefender GravityZone External Attack Surface Management (EASM)?
A: GravityZone EASM is a Bitdefender product that is part of the GravityZone XDR Platform. It identifies internet-facing assets, their vulnerabilities, and misconfigurations, enabling risk prioritization and rapid mitigation. It is essential for controlling the expanding attack surface, detecting shadow IT, supporting third-party vendor assessments, and meeting compliance requirements.

Q6: What is the difference between ASM and EASM?
A: ASM (Attack Surface Management) is an umbrella term that covers both internal and external attack surfaces. GravityZone EASM focuses on the external surface, identifying assets that are publicly accessible. Internal risk visibility is provided by capabilities such as Risk Management and solutions such as GravityZone Patch Management and GravityZone PHASR.

How is GravityZone EASM licensed?

Q7: How is GravityZone EASM licensed?
A: It is licensed based on the number of endpoints/devices. A minimum of 50 endpoints is required.

Q8: Can the number of GravityZone EASM licensed endpoints be fewer than the base GravityZone license?
A: No. The number of GravityZone EASM seats must match the number of endpoints on the base GravityZone license.

Q9: Does GravityZone EASM support mixed asset types (e.g., servers, domains, IPv4/IPv6) ?
A: Yes, but licensing is still calculated based on the number of endpoints, not on the number of discovered assets.

Q10: Is GravityZone EASM available for MSPs?
A: Yes. For MSPs, the GravityZone EASM add-on can be activated on top of the GravityZone MSP Security Solutions bundles (Secure, Secure Plus, Secure Extra). It is not available for à la carte offerings.

Q11: Are NFR (Not for Resale) licenses available for GravityZone EASM, including for MSP exclusive partners?
A: Yes, NFR access is available for eligible partners, including MSP-exclusive ones.

Q12: What are the licensing prerequisites for using GravityZone EASM?
A: You must have a license that includes Risk Management. GravityZone EASM is available as an add-on for supported bundles, excluding Small Business Security.

Q13: Can GravityZone EASM function as a standalone product or only with GravityZone bundles?
A: GravityZone EASM is only available as an add-on product to GravityZone packages.

GravityZone EASM use cases and common questions:

Q14: What are the main use cases for GravityZone EASM?
A: There are 3 main use cases:

a. Discovering internet-facing assets (both managed and unmanaged), such as forgotten dev environments or marketing domains.
b. Managing vulnerabilities, misconfigurations, and expired certificates on publicly exposed systems.
c. Prioritization of what needs fixing based on external exposure and context

Q15: What do you mean by continuous scanning?

It has been a common practice for organizations to run periodic scans to identify their external attack surface or update their asset inventories. Due to the speed of modern attacks and the proliferation of new attack surfaces, organizations can no longer rely on yearly scans and need to implement continuous scanning and exposure management programs.

GravityZone EASM enables continuous but not real-time discovery and management of organizations' external attack surface by using scheduled scans. The scans can be scheduled with a weekly frequency, but you can trigger a manual scan once per day if needed.

Q16: Does GravityZone EASM detect vulnerabilities in unpatched operating systems and applications?
A: No. Vulnerabilities in OS and applications are detected by the Risk Management module via agents. GravityZone EASM focuses on publicly exposed assets and their vulnerabilities.

Q17: Can Patch Management be automated based on GravityZone EASM findings?
A: Yes, if the resource is managed and has an agent installed. If the resource is unmanaged, Patch Management cannot apply fixes automatically.

Q18: Can GravityZone EASM replace commercial internet-facing asset discovery tools?
A: GravityZone EASM discovers internet-facing assets and associated vulnerabilities. It can replace siloed EASM solutions, but the functionality overlap is different depending on the particular solution. The key advantage of GravityZone EASM is that it integrates directly with Bitdefender GravityZone, offering centralized visibility, automation, and risk prioritization.

Q19: Can asset discovery be done using other tools instead of GravityZone EASM?
A: Yes, but GravityZone EASM provides seamless integration within the GravityZone console, allowing for centralized visibility, automation, and risk prioritization.

Q20: Which attack surfaces does GravityZone EASM discover/monitor ?
A: GravityZone EASM discovers and monitors internet-facing (external) assets such as:

- Domains (including similar domains that may be used in spoofing attacks)
- Emails
- Expired or soon-to-expire certificates
- Public services (e.g. web servers, applications) and their vulnerabilities and misconfigurations
- DNS records
- Mail servers
- ASN (Autonomous System Numbers)
- IP addresses and IP ranges (IP blocks), including those from cloud providers like Cloudflare

Q21: Does GravityZone EASM overlap with CSPM+ ?
A: GravityZone EASM and CSPM+ complement each other - they focus on different layers (GravityZone EASM on external asset exposure, and CSPM+ on cloud configurations and compliance.)

Q22: How does GravityZone EASM enhance the Risk Management module?
A: Risk Management focuses on known, internal assets within the organization (most of which are not exposed to the public/internet). GravityZone EASM adds a critical external layer by identifying unknown or unmanaged internet-facing assets, providing visibility into potential vulnerabilities that could otherwise be overlooked.