AGM SOLUTIONS
antifragili per innovazione

PENTERA

Pentera Use Cases

Pentera is a very flexible platform. It provides support to numerous use cases and as time goes on and the platform is both used more and evolved, more use cases arise.
The following list is by no means exhaustive but will help formulate ideas on the art of the possible.

What is Automated Security Validation?

- Automated Security Validation (ASV) refers to the process of continuously testing and validating the effectiveness of security controls against real-life attack scenarios using automated tools and techniques.

  The core objectives and benefits of ASV include:
  - Real-World Security Performance Testing
  - Enabling Continuous Threat Exposure Management
  - Focused Risk Management
  - Speed & Scalability
  - Empowering security teams to get greater visibility of their attack surface.
  - Recommend effective remediation based on impact prioritization
  - Agentless and safe by design

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Example Use Cases

There are quite a few...

C = Challenge that organizations face
S = Solution that Pentera provides
V = The Value Proposition

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Main Use Cases

AGM SOLUTIONS
antifragili per innovazione

PENTERA

CTEM Adoption

C

Organizations are adopting Continuous Threat Exposure Management (CTEM) to achieve ongoing visibility into their attack surface and improve security resilience. However, they face challenges such as:
Complex and fragmented security environments, Lack of actionable insights to prioritize mitigation, Inefficiencies in validating security controls at scale.

S

Pentera aligns with CTEM by emulating real-world attacks, mapping vulnerabilities to MITRE ATT&CK with risk-based prioritization, and providing continuous validation to support CTEM's iterative assessment and improvement process.

V

Pentera enables visibility into the attack surface to identify unknown risks.
It empowers security teams with focused remediation based on criticality and risk impact, reducing the attack surface over time by validating mitigation efforts continuously, aligning seamlessly with the CTEM framework, providing measurable outcomes for management and auditors.

Validation of Ransomware Resiliency

C | Ransomware is one of the most disruptive forms of cyber attacks, targeting individuals, businesses, and organizations. They have become increasingly prevalent and sophisticated in recent years, posing significant threats to organizations across various sectors. Organizations don't know if they are actually protected against ransomware attacks

S | Pentera has the ability to run emulated ransomware attacks against endpoint and server infrastructure (if the customer purchases the RansomwareReady module).
Pentera allows you to choose specific ransomware families like Lockbit, Conti, REvil and Maze and test the breadth of detection across the estate

V | Pentera Testing Scenarios can be scheduled and run on demand as often as required, enabling continuous validation to ensure that detection and response mechanisms are always effective against ransomware.

SOC Optimization: Validating SOC & Incident Response Protocols

C | Incident Response (IR) and Security Operations Center (SOC) teams aim to detect, investigate, and mitigate cybersecurity threats to minimize damage and restore operations quickly. They face challenges like managing overwhelming alerts, detecting sophisticated threats, addressing understaffing, and ensuring visibility across hybrid environments while balancing compliance and rapid threat response.

S | Pentera helps customers test and improve their Incident Response protocols and SOC capabilities by tuning alerting systems and reducing detection and response times (MTTD and MTTR). It identifies weaknesses in playbooks that might inadvertently escalate an attack and allows for safe tabletop exercises with real yet benign attacks to validate SOC and IR team effectiveness.

V | Pentera can find where the detection and response capabilities are lacking and provide recommendations on what and how to fix.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Improve Penetration Testing Efficiency & Cadence

C

A challenge which many organizations have, mainly due to budget reasons, is the cadence of testing. Manual testing is expensive, doesn't cover the entire estate, takes quite a long time and due to differing levels of talent, is not always comparable.

S

Pentera enables continuous security validation, offering faster and more comprehensive visibility into exploitable vulnerabilities compared to traditional penetration testing. Grey Box and Targeted Tests focus on specific scenarios, with machine-speed and machine-scale testing delivering results quickly. Pentera also supports immediate validation of remediations, enhancing organizational security efficiency.

V

Pentera improve testing efficiency and cadence by providing rapid, automated testing and immediate remediation validation, enabling organizations to efficiently improve their security posture.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Vulnerability Prioritization

C

Organizations struggle to manage overwhelming volumes of vulnerabilities due to limited resources to address all findings and Inefficient prioritization, leading to wasted effort on low-risk vulnerabilities. Traditional methods also focus on severity without considering exploitability..

S

Pentera streamlines vulnerability prioritization by assessing risks based on real-world exploitability and business impact, providing clear remediation recommendations to focus efforts where they are most needed. It ensures that prioritized vulnerabilities are effectively remediated and links vulnerabilities to attack techniques using the MITRE ATT&CK framework, offering a deeper understanding of their potential impact.

V

Pentera delivers continuous attack surface visibility, minimizing missed vulnerabilities and unprotected assets. By combining automated attack emulation with actionable insights, it helps organizations address critical risks efficiently while securing known and unknown assets to maintain a resilient external security posture.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Enhancing Red Team Operations with Pentera

C | Red teams face challenges such as - Limited time and resources to conduct thorough testing across large environments, difficulty in performing advanced, real-world attack techniques consistently and inefficiencies in scaling operations while maintaining effectiveness.

S | Pentera amplifies red team capabilities by: Emulating advanced attack scenarios, leveraging real-world tactics, techniques, and procedures (TTPs), providing end-to-end visibility of attack paths, enabling efficient, large-scale testing without compromising depth or accuracy while mapping findings to the MITRE ATT&CK framework, enhancing reporting and communication with stakeholders.

V | Pentera frees up red team resources to focus on strategic, creative operations by automating repetitive tasks and providing comprehensive attack surface insights, ensuring no critical gaps are overlooked. Pentera also enhances collaboration between red teams and SOCs with clear, actionable reports, while allowing for scaling seamlessly across diverse environments, increasing operational efficiency and effectiveness.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Attack Surface Monitoring

C

Organizations often struggle to manage their attack surface effectively due to constantly evolving IT environments, including new assets, shadow IT, and cloud expansions. This dynamic nature makes it difficult to identify exposed vulnerabilities. Compounding the issue is the lack of continuous monitoring tools that provide actionable insights into external-facing assets.

S

Pentera streamlines attack surface monitoring by mapping and validating external-facing assets, identifying vulnerabilities like misconfigurations and shadow IT, and prioritizing them by their actual risk. It emulates real-world attacks to validate asset attractiveness and exploitation potential, providing clear insights for security teams to address critical risks efficiently.

V

Pentera frees up red team resources to focus on strategic, creative operations by automating repetitive tasks and providing comprehensive attack surface insights, ensuring no critical gaps are overlooked. Pentera also enhances collaboration between red teams and SOCs with clear, actionable reports, while allowing for scaling seamlessly across diverse environments, increasing operational efficiency and effectiveness.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Additional Use Cases

Cloud environment validation use cases

C

Cloud environments face many risks, including misconfigured resources, exposed sensitive data, vulnerabilities, weak access controls, leading to unauthorized access and more. Cloud environments are also prone to lateral movement, insecure APIs, and potential risks from shadow IT and unvetted third-party applications. These challenges are compounded by limited visibility and difficulty in ensuring compliance across dynamic and hybrid infrastructures.

S

Pentera offers multiple testing approaches to assess Cloud risk exposure: black box testing evaluates risks without prior knowledge of the cloud environment, while grey box testing examines the impact of a compromised user account. It also includes cloud configuration reviews to ensure resources are secure and compliant and uniquely identifies risks from lateral movement between cloud and on-premises environments, a capability not offered by other vendors.

V

Pentera enhances organizations cloud security by identifying vulnerabilities, validating controls, and addressing risks like misconfigurations and lateral movement, ensuring a stronger and more resilient cloud environment.

New infrastructure or third-party security validation

C | Change introduces risk. Whether a new network is being added, an organizational change is taking place such as a merger, or business data/network access is provided to third parties such as service providers, penetration testing allows visibility of the security posture and risk to be assessed.

S | Pentera automated penetration testing can be carried out as often as needed to meet requirements. This provides the flexibility to run tests on third party infrastructure as well as on internal change events. Immediate reporting provides speedy visibility allowing for gap analysis and remediation guidance.

V | Pentera helps organizations measure security posture on change and identify gaps against policy

Legacy Systems and Infrastructure

C | Many organizations utilize legacy systems and infrastructure which are inherently vulnerable

S | When running Pentera across multiple networks the discovery process can help identify assets that may be vulnerable to attack, forgotten about or in need of updating.
Common findings include legacy SD infrastructure, third party systems and rogue systems.

V | Pentera attack vectors are a powerful way to identify mitigation steps or hardening recommendations to shut down those gaps.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Consolidation of Controls - Zombie Renewals

C | Over time organizations accumulate various security controls. This can result in tooling duplication and redundancy of security controls

S | Pentera can help identify what is currently fit for purpose. Security teams can measure what works best during an emulated attack and retire the duplicate/unneeded tools. For example - multiple EDR and Anti-virus solutions spread across the estate, where not all perform as needed.

V | Evidence of performance can help make decisions on tools and controls that can be deprecated at the time of contract renewal.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Misconfiguration Validation

C | Policies evolve over time, and misconfigurations can undermine effective detection and response. This may involve issues like nested privileges in Active Directory, password reuse, missing security controls, and SOC blind spots in log collection. These factors significantly affect evaluations of cyber resilience.

S | Pentera looks for misconfigurations that may occur and will exploit them, to show the actual impact of the misconfigurations found.

V | Misconfigurations are dynamic vulnerabilities which most VM tools don’t even look for, but which attackers love to exploit

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Efficacy of Security controls like EDRs

C | EDR stands for Endpoint Detection and Response, which is a cybersecurity solution designed to detect, investigate, and respond to threats on endpoint devices like laptops, desktops, servers, and mobile devices. Organizations don't always know if the EDRs are operating as designed.

S | Pentera has multiple types of payloads, all safe, ranging from ones with known malicious signatures to others which were developed by R&D and would probably not be picked up from a hash or signature perspective. These payloads emulate true zero-day attacks and test the behavioral defenses of organizational endpoint detection and response mechanisms.

V | EDRs, AVs and other types of EPP tools efficacy can be validated with Pentera (i.e., are they working as intended)

Malware injection/detection

C

Malware poses risks such as data breaches, leading to the theft of sensitive information, regulatory fines, and reputational damage. It can cause system downtime, financial loss, and compromise intellectual property. Additionally, malware can spread to other systems, eroding trust with customers and partners while escalating recovery costs. Are the organizations securing themselves correctly against them?

S

Pentera will attempt to download payloads (malware) to test whether the endpoint protection blocks them or not, thus, validating if the organization is defending properly against malware attacks, starting with detection of such attacks, through preventing injection of malware (and combined with SOC/IR validation – validation of how the organization responds to such attacks)

V

Pentera provides immediate visibility on where malware injection/attacks are possible, allowing for focused and efficient remediation.

Validation of Lateral Movement & Segmentation Validation

C

After the initial breach, attackers use lateral movement techniques to escalate privileges, identify critical assets, and ultimately achieve their objectives, such as accessing sensitive systems, exfiltrating data, and disrupting operations while remaining undetected for extended periods. By mimicking legitimate user behavior, it evades traditional security tools, enabling attackers to target critical assets or deploy ransomware for greater damage.

S

Pentera can validate whether network segmentation is effectively preventing access between segments by employing the same tactics, techniques, and procedures (TTPs) as real-world attackers to identify exploitable hosts, services, and critical "pivot machines" with multiple interfaces that attackers could leverage for lateral movement.

V

Pentera can validate whether lateral movement or pivoting are possible and provide recommendations how to prevent them. This helps organizations uncover potential pathways attackers could use to breach secure networks or transition from on-premises to cloud environments.

Rogue Asset/Shadow IT Detection = Minimizing the unknown Attack Surface

C | Rogue IT or Shadow IT refers to unauthorized use of hardware, software, or IT resources within an organization, often bypassing IT policies and controls. While it may stem from employees seeking productivity solutions, it poses significant cybersecurity risks, especially since the organization did not know they were there.

S | Pentera Core, Cloud, and Surface can test entire subnets, cloud accounts, and thousands of external-facing assets, often uncovering unknown devices such as unsanctioned IoT devices, vulnerable systems, or unmanaged vendor equipment like printers or ATMs. These devices, often running outdated software, create entry points for attackers to infiltrate the network and move laterally to critical assets.

V | Pentera can detect rogue assets and shadow IT, reducing exposure and providing visibility into the real attack surface

Active Directory Weaknesses

C

Active Directory (AD) weaknesses include misconfigurations like excessive permissions, outdated protocols, and unprotected privileged accounts, which attackers can exploit to gain access or escalate privileges. Vulnerabilities such as weak password policies, exposed credentials, and insufficient monitoring make AD a frequent target for lateral movement and ransomware attacks

S

Manual penetration testers often lack the time and resources to fully analyze Active Directory (AD) environments for all weaknesses, but this is a task perfectly suited for Pentera. Pentera identifies misconfigurations like anonymous enumeration, circular nested groups, shadow admins, and privilege abuse while testing for vulnerabilities and if relaying to a domain controller is possible over LDAP/LDAPS.

V

Pentera's goal is to maintain a secure user repository and minimize administrative privileges to reduce overall risk by validating AD weaknesses

Password Hygiene

C

Poor password hygiene risks include weak or reused passwords, shared or default credentials, a lack of complexity and more, making accounts vulnerable to brute force and credential stuffing attacks. Storing passwords insecurely, failing to update them after breaches, and not using multi-factor authentication further increase the risk of unauthorized access. Although organizations follow best practices, they don't usually know if their passwords are secure

S

Pentera addresses password hygiene risks by measuring password strength in Active Directory or Azure, identifying bad practices, validating service account accessibility and more. It detects password reuse, tests for credential sniffing, and dumping, while allowing customization of password dictionaries for organization-specific terms. Additionally, it assesses the impact of leaked credentials both externally and internally

V

Using Pentera, organizations can continuously validate their password and credentials hygiene , both externally and internally

SIEM Integration = Detection Readiness

C

Many organizations utilize SIEM platforms to collect all the security data in their estate and based on that data to make decisions (to respond, mitigate, etc.). But validating that the SIEMs are performing as designed is not an easy task

S

Pentera integrates with SIEM platforms to validate detection capabilities, ensuring EDRs, Avs and other controls trigger alerts and log attack data for SOC teams to review. This also supports training the teams by emulating attackers and validating Incident Response protocols, using SIEM logs to confirm comprehensive detection and response capabilities.

V

With the SIEM integration, organizations can validate that their detection and response capabilities are up to par.

Critical Assets Validation – The Crown Jewels

C

Critical assets are the systems, data, and resources essential to an organization's operations, security, and reputation. These assets, if compromised, could cause significant damage, disrupt services, or lead to financial and reputational losses.

S

With Pentera, organizations can define critical assets such as **accounts**, **machines**, **IP ranges**, or **web services**, ensuring issues there are addressed first to reduce risk efficiently. Exploitation of a critical asset triggers a **9.9 achievement** with remediation recommendations to close security gaps quickly.

V

Pentera allows organizations to test and prioritize critical assets, helping them focus security efforts on areas with the greatest impact

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Critical Windows Vulnerability Scanning = Find those vulnerabilities that are **really** putting you at risk

C The main challenges of vulnerability assessment include managing the overwhelming volume of vulnerabilities discovered, which can make prioritization difficult. Traditional methods often lack context, focusing on severity rather than exploitability, leading to wasted resources

S Pentera offers Targeted Critical Vulnerability scans, focusing on the most critical vulnerabilities attackers actually exploit, allowing organizations to quickly and minimally invasively assess tens of thousands of machines or validate new networks.

V Pentera provides essential insights without the overload of traditional vulnerability management

Validate New Networks, Cloud Accounts or M&A activity

C

Adding new networks introduces security challenges such as ensuring proper configuration and segmentation to prevent unauthorized access or lateral movement. These networks may lack visibility initially, increasing the risk of undetected vulnerabilities or misconfigurations. Additionally, integrating new networks with existing security controls can be complex, creating potential gaps that attackers could exploit.

S

Pentera's on-demand testing helps validate new areas in an organization's estate, establishing a baseline for new networks, guiding remediation, and enabling periodic retests. During mergers and acquisitions, Pentera quickly assesses the security of the acquired company's network, identifies business risks, and ensures continuous security during and after integration.

V

Pentera enables organizations to validate and secure new networks or merged estates by providing rapid and on-demand validation, guiding remediation, and ensuring ongoing security.

Attack behaviors mapped to MITRE ATT&CK

C

Organizations use the MITRE ATT&CK Framework to improve threat detection, guide red team simulations, and identify security gaps by mapping attacker tactics and techniques. It supports incident response by linking observed behaviors to known attack patterns and evaluates the effectiveness of security tools. Organizations attempt to map their security capabilities against this framework.

S

Pentera's attack vectors provide end-to-end visibility into attack paths, showing how vulnerabilities can be chained together for greater impact, helping prioritize mitigation and root cause fixes. Pentera maps each attack stage and technique to MITRE, color-coded by criticality, offering insights into weak passwords, misconfigurations, and security control effectiveness.

V

By aligning with the MITRE ATT&CK Framework, Pentera helps organizations identify defensive gaps and strengths.

Upskilling and training Cyber Security Teams

C

Training cybersecurity teams is challenging due to the rapidly evolving threat landscape, which requires keeping up with new attack techniques and tools. Limited access to realistic, hands-on training environments and the need to balance ongoing operations with training efforts further complicate skill development. Also, varying expertise levels within teams make it difficult to standardize and scale effective training programs.

S

Pentera provides cybersecurity teams with hands-on experience in stress-testing defenses, tuning controls, and improving policies through safe, controlled attack emulations that don't disrupt business operations. This enables teams to understand attack impacts, evaluate security controls more effectively, and develop new skills in a low-pressure environment, enhancing organizational resilience.

V

Pentera empowers teams to safely test and improve security controls while gaining valuable skills and insights to strengthen organizational resilience without disrupting operations.

IPS/IDS Alert Threshold Tuning

C Due to the dynamic nature of attacks, Intrusion Detection and Prevention tools require continuous “tuning”, to ensure they are performing as designed.

S Pentera allows organizations to validate their IPS/IDS tools by testing increasing stealth levels, starting from "Noisy” up to the stealthiest. This helps assure that the IDS/IPS tools are utilizing their true detection capabilities and ensure they are properly configured. The process provides an accurate picture of what the organization can detect, addressing gaps in vendor claims.

V Pentera enables organizations to validate and optimize their detection capabilities by revealing the true effectiveness of their IPS/IDS tools.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Web Attack Surface enumeration and validation

C

Internal and external websites and services are a valuable source of information for exploiting vulnerabilities and weaknesses and gathering essential information on the organization itself. Organizations don't always know if they are sufficiently protected (and sometimes aren't even aware they exist)

S

Pentera identifies and validates vulnerabilities in both internal and publicly accessible assets like services, websites, APIs, and cloud services. By testing for common vulnerabilities and mapping findings to frameworks like MITRE ATT&CK, it prioritizes high-impact issues and ensures ongoing security. This provides organizations with enhanced visibility and actionable insights to protect their attack surface effectively.

V

Pentera Core & Surface help to identify what is present and potential issues in the Web Attack Surface that might need to be remediated, also providing useful intel on what exists and identifying if sensitive information is exposed to an attacker.

Tech Bake-off

C Security controls and tools are expensive. Organizations invest millions, if not more, into their security stack, without always knowing how these controls will hold up in the moment of truth

S Pentera helps organizations evaluate new security controls during tech bake-offs or PoVs, assessing their effectiveness, configuration, and tuning. This enables security teams to identify standout technologies, optimize tool performance, and evaluate factors like time-to-value, ease of use, and support capabilities. It ensures informed decisions about future security investments.

V Pentera enables organizations to thoroughly evaluate and optimize new security tools, ensuring they select effective solutions that align with their needs and deliver maximum value.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Building and validating security roadmap investment programs

C | This use case is critical for shaping short and long-term cybersecurity investment strategies. Beyond implementing new controls, it ensures that resources allocated to policies and configurations are effectively utilized to achieve optimal cyber resilience, instead of building upon historical data.

S | Pentera provides insights into adversarial behavior through MITRE ATT&CK mapping and detailed reporting, including resilience trends and scorecards, to help management identify and address areas for improvement. Using Pentera, organizations can prioritize security investments and measure improvements through incremental changes or tech evaluations. This ensures targeted and effective enhancement of the organization’s security posture.

V | Pentera helps organizations identify and prioritize security gaps, guiding targeted investments and measuring improvements to help build their security roadmap.

Vendor Accountability and Value

C

Many organizations are supported by 3rd parties and vendors. But who watches the watchers? How can the organization tell if they are receiving what they are paying for?

S

Pentera facilitates validation exercises by identifying gaps and providing actionable feedback for third-party suppliers. This fosters discussions on current performance, leading to potential product updates, configuration changes, or control tuning to address identified gaps effectively.

V

Pentera helps organizations hold vendors and 3rd party providers accountable, by enabling actionable feedback, driving improvements and optimizations to address identified security gaps.

AGM SOLUTIONS
antifragili per innovazione

PENTERA

Use Cases Summary

EXPOSURE MANAGEMENT Attack surface discovery and exposure reduction	**CONTROL VALIDATION** Evaluate in production	**PENETRATION TESTING** Move beyond compliance	**M&A ASSESSMENT** Validate security of acquisition target	**CYBERSECURITY INSURANCE** Improved insurance eligibility and premiums
VULNERABILITY PRIORITIZATION Remediate based on real risk impact	**RED TEAMING** Power tool for red teams and IT security	**SOC OPTIMIZATION** Test SOC / response procedures	**CREDENTIAL EXPOSURE** Validate stolen and weak credentials	**RANSOMWARE ASSESSMENT** Safely test full attacks

AGM SOLUTIONS
antifragili per innovazione

Contact

Mauro Zini
mauro.zini@agmsolutions.net
www.agmsolutions.net