KNIGHTGUARD

Gambit cyber

Unified Vulnerability Management (UVM)

OVERVIEW

In today's hyper-connected landscape, where AI Agents are finding zero-day vulnerabilities daily, traditional vulnerability management doesn't scale and is failing.

The definition of vulnerability is getting an upgrade. Vulnerabilities are not just software flaws anymore, they are also policy misconfigurations, your exposed workflows and assets that act as entry points into the interconnected network. This definition helps organisations shift left.

Security teams are drowning in a "sea of red" alerts, hampered by siloed tools that provide data without context. The shift to **Unified Vulnerability Management (UVM)** is no longer optional; it is a strategic necessity to bridge the gap between **Visibility** (finding the flaw), **Prioritization** (understanding the risk), and **Remediation** (fixing the problem).

Modern enterprises require a platform that doesn't just aggregate CVEs but unifies the entire exposure lifecycle incorporating Asset Surface Management (ASM), Threat Intelligence, and automated validation to ensure that the most critical "choke points" are addressed first.

The "Scan-and-Patch" Trap

The gap between discovering a flaw and its actual exploitation has shrunk dramatically, yet the manual effort to validate and remediate has not. The result is alert fatigue: critical exposures remain unaddressed, buried under mountains of non-exploitable noise.

HOW KNIGHTGUARD UVM HELPS

KnightGuard shifts focus from individual bugs to systemic risk. It unifies Attack Surface Management, Cloud Misconfigurations, and Dark Web Monitoring into a 360° exposure view. By integrating multiple VM scanners into a single source of truth and applying **AI-Driven Choke Point Analysis**, it fixes the one path that blocks ten possible attacks.

KEY UVM CAPABILITIES

Attack Surface Management (Internal & External)

Continuous outside-in discovery of your digital footprint domains, subdomains, shadow IT, exposed services, SSL certificates, etc.

Cloud Misconfigurations NEW

Real-time agentless auditing across AWS, GCP, Azure, GitHub, and Kubernetes. Drift detection identifies deviations from Standard Benchmarks. Auto-tags against SOC2, HIPAA, GDPR.

Multi-Scanner Normalization

Ingests all leading VM scanners (commercial and open source). De-duplication merges redundant findings, reducing data noise by up to 60% one clean record per unique vulnerability.

AI-Driven Vulnerability Prioritization

Beyond CVSS: integrates KEV, EPSS, dark web intel, exploit probability, threat actor activity, and asset value into a dynamic multi-factor risk score contextualized to your specific environment.

Vulnerability Remediation AI Agent

Transforms "what is wrong" into "how to fix it" providing exact PowerShell scripts, GPO settings, and tool-specific instructions. Contextual guidance avoids breaking business dependencies.

Bidirectional ITSM Integration

Real-time sync with Jira, ServiceNow, Slack, etc. When a ticket is updated, KnightGuard reflects the status instantly shifting from "alerting" to "executing."

95%
of "Critical" vulns are not reachable by an attacker

40%
of EDR/SIEM/firewall controls fail silently due to misconfiguration

60%
reduction in MTTR achievable through AI-driven agentic workflows

23%
annual growth rate of the enterprise attack surface in 2026

UVM VS. TRADITIONAL VM: THE DIFFERENTIATORS

CAPABILITY	SUPPORTED FRAMEWORKS	KNIGHTGUARD UVM
Intel Operationalization	Reliant on public feeds (CISA KEV) or static vendor data. Slow to adapt.	AI pipeline ingests unstructured BYO-Intel (PDFs, blogs, advisories) into actionable logic in minutes.
Remediation Effort	High-level "Apply Patch" recommendations. Technical how-to left to IT team.	ITOps AI Agent generates tool-specific, executable playbooks tailored to your exact OS and security stack.
Risk Scoring	Linear CVSS + manual asset tagging. Fails to reflect dynamic threat landscape.	Proprietary algorithm dynamically weights scores using real-world simulation outcomes and validated control status.
Tool Agnosticism	Creates vendor lock-in, pushing users toward proprietary scanner ecosystems.	Fully agnostic mesh layer consolidates ROI of existing scanners without rip-and-replace.

KNIGHTGUARD

Gambit cyber

Unified Vulnerability Management (UVM)

THE 360-DEGREE EXPOSURE INTELLIGENCE LAYER

- **Attack Surface Management** (Internal & External)
- **Cloud Providers (AWS/ GCP/Azure, etc.)**
- **VM Scanners (Tenable, Qualys, Rapid 7, etc.)**
- **Dark Web Intelligence**
- **Identity & EDR**
- **Threat Intel (KEV, EPSS, OSINT)**

AI UNIFICATION LAYER

KNIGHTGUARD

- De-Duplication
- Normalization
- Correlation
- Prioritization

60%
reduction in data noise

THE SHIFT KNIGHTGUARD ENABLES

Reactive	Preemptive
Siloed Alerts	Unified Risk View
CVSS Scores	Business impact
Patch Counts	Measurable Resilience
Assumed Security	Validated defence

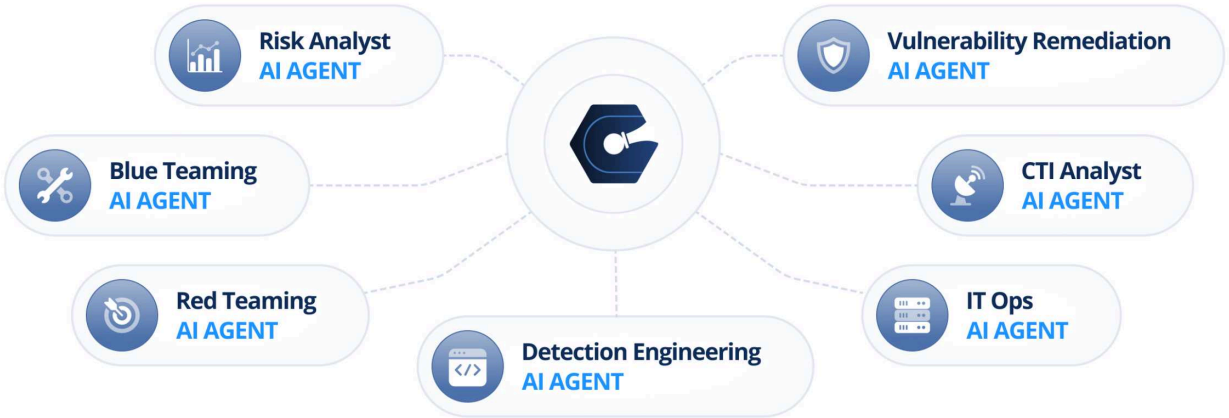
Measurable Risk Reduction	Business-Aligned
Faster MTTD & MTTR	AI-Accelerated
Tools consolidation	Lower TCO
Improved team efficiency	More from Existing Tools

The KnightGuard Agentic Layer

Unlike static platforms, KnightGuard deploys a Mesh of AI Agents CTI Analyst, SOC Analyst, Red & Blue Team, and ITOps that possess Reasoning and Action (ReAct) capabilities. They query your SIEM, update tickets, generate detections, and write remediation playbooks autonomously, operating as a 24/7 force multiplier for your security team.

AGENTIC AI

A MESH OF AI AGENTS - ALWAYS WORKING



Reduced TCO
Consolidate fragmented tools into one vendor-agnostic platform.

Faster Identification
Discover hidden gaps across cloud, on-prem, and the dark web.

Lower MTTR & MTTD
Autonomous agents accelerate both finding and fixing.

Swift Prioritization
Use AI to rank exposures based on actual exploitability.

Outcome-Based Remediation
Focus on the 5% of gaps that represent 90% of your risk.

KNIGHTGUARD

Gambit cyber

Unified Vulnerability Management (UVM)

SUBSCRIPTION MODULES

KnightGuard Unified Vulnerability Management

- Attack Surface Management
- Unified Asset Intelligence & Prioritization
- Unified Asset Exposure Scoring
- Cloud Misconfigurations NEW
- Dark Web Monitoring
- Unified Vulnerability Prioritization (based on Threat Intelligence, Dark Web, Exploit Availability, Ease of Exploitation, Risk score from security tools, etc.)
- Vulnerability Attack Paths NEW
- Asset Exploitability Attack Paths NEW
- Unified Vulnerability Management Metrics (Team Velocity, Critical Trends, Open/in-progress/fixed Trends, Resurfaced Vulnerabilities, etc.)
- Native Integrations
  - VM Scanners (Tenable, Qualys, OpenVAS, etc.)
  - Cloud Providers & Repositories (AWS, Azure, GCP, GitHub, M365 etc.)
  - Firewalls (Fortinet, Cloudflare, Palo Alto, Cisco, etc.)
  - Identity Solutions (Microsoft EntraID, Okta, etc.)
  - ITSM (ServiceNow, Jira, Slack, Teams, etc)
  - EDR (CrowdStrike, SentinelOne, Defender, etc.)
- Named Customer Success Manager

Vulnerability Remediation AI AGENT

KnightGuard Threat Informed Defense

- MITRE Aligned Threat Intelligence + OSINT
- GIR (General Intelligence Requirements) based Threat Intelligence Prioritization
- Threat Intelligence Operationalization (BYO Threat Intelligence)
- SIEM agnostic Detection Analytics
- Threat Monitoring
- ATT&CK-mapped Adversary Playbooks NEW
- Threat-Based Risk Scoring NEW
- Threat-aligned Logs Prioritisation
- Campaign Intelligence (TTP evolution, tooling, timelines, etc.)
- Top Techniques & Controls Identification
- Controls Mapping & Prioritization (NIST 800-53, MITRE Mitigation, MITRE Defend) NEW
- NIST & MITRE-Based Remediation Guidance
- MITRE Aligned Detection Analytics
- Multi-SIEM Detections NEW
- NIST CSF 2.0 Controls Remediation Mapping
- Threat Coverage & GAP Analysis NEW
- Board Reporting NEW
- Named Customer Success Manager

CTI Analyst AI AGENT

IT Ops AI AGENT

KnightGuard Unified Exposure Validation

- MITRE Aligned Detection Engineering
- Threat Hunting
- Breach Attack Emulation
- 1500+ Ready-to-deploy Emulation Campaigns
- Seamless Purple Teaming
- Detection As Code NEW
- Multi-SIEM Detection Management NEW
- Multi-SIEM Unification NEW
- Native Integrations with SIEM (Sentinel, Splunk, Elastic, etc.)

Vulnerability Remediation AI AGENT

Red Teaming AI AGENT

Blue Teaming AI AGENT

KnightGuard Unified Risk Management/Quantification

- Cyber Risk Prioritization (MITRE, NIST, etc.)
- Ready to Quantify Risk Scenarios (BEC, Ransomware, Dataloss, etc.) NEW
- Cyber Risk Quantification (based on NIST RMF, NIST 800-30, NIST 800-39, NIST 800-53)
- Risk Gap Analysis NEW
- Risk Reduction Guidance Mapped to Organizational Controls
- Organization Context-Based Quantification NEW
- Organization Specific Risk Profiles
- Use case specific Risk Profiles (for DORA, OT, Ransomware, etc.)
- Automated Compliance Coverage (for AWS, GCP, AZURE, etc.)
- CISO Dashboards

Risk Analyst AI AGENT

Notes:

KnightGuard Unified Exposure Validation

KnightGuard Unified Exposure Validation is an add-on module to KnightGuard Threat Informed Defense or KnightGuard Unified Vulnerability Management.

KnightGuard Unified Risk Management & Quantification

KnightGuard Unified Risk Management & Quantification is an add-on module to KnightGuard Threat Informed Defense + KnightGuard Unified Vulnerability Management + KnightGuard Unified Exposure Management.

KNIGHTGUARD

Gambit cyber

Unified Vulnerability Management (UVM)

ABOUT GAMBIT CYBER

Gambit Cyber B.V. is a Netherlands-headquartered cybersecurity company pioneering AI-driven, risk-centric Continuous Threat Exposure Management (CTEM). Through its AI-native and risk-centric Preemptive threat exposure management platform, **KnightGuard,** Gambit Cyber helps enterprises move from reactive, alert-driven security to continuous, validated, and threat-informed defence that reduces real-world cyber risk.

The company's core leadership team brings over 100 years of combined experience in cybersecurity across global technology organizations, having built and scaled large-scale security programs in complex, regulated environments. Gambit Cyber was recently recognized as one of **Europe's Top Cybersecurity Startups** by the **European Cyber Security Organization (ECSO).**

Gambit Cyber is backed by a strong investor base including **Expeditions, Bitdefender Voyager Ventures,** and seasoned angel investors. Their confidence in our vision not only fuels our growth but also brings invaluable expertise and strategic support to accelerate our journey.

OUR INVESTORS

Expeditions

Bitdefender VOYAGER VENTURES

TRIDENT HORIZON

START WITH ONE MODULE. GROW AT YOUR PACE.

Complete flexibility to begin modestly and expand your CTEM program step by step - no big-bang deployment required.

1. START HERE - PHASE 1
   Unified Vulnerability Management
2. PHASE 2
   Threat Informed Defense
3. PHASE 3
   Unified Exposure Validation
4. PHASE 4
   Unified Risk Management & Quantification

COMPREHENSIVE FRAMEWORK ALIGNMENT

FRAMEWORK CATEGORY	SUPPORTED FRAMEWORKS	KNIGHTGUARD APPLICATION
Security Governance	NIST 800-53 & NIST-CSF 2.0	Automatically maps identified exposures to NIST control families, prioritizing fixes that satisfy regulatory audits.
Intelligence Planning	GIR (General Intelligence Requirements)	Uses GIR framework to categorize threat intelligence.
Adversary Behavior	MITRE ATT&CK®	Operationalize, defences aligned to adversary behaviours across ITOps and SecOps
Defensive Mapping	MITRE D3FEND™ MITRE MITIGATION	Suggests specific technical countermeasures (File Analysis, Decoy Environment) to neutralize identified threats.
Risk Quantification	NIST RMF, NIST 800-30, NIST 800-39	Prebuilt quantification modules for 9+ risk scenarios like BEC, Ransomware, Data Loss, and Insider Threat scenarios.

WHY KNIGHTGUARD WINS

Vendor-Agnostic "Agentic Layer"

Sits on top of existing tools - no rip-and-replace. Operationalizes intelligence in real-time to answer: "Are we actually protected against this specific threat right now?"

Evidence-Based Defense

Replaces "we think we are secure" with "we have validated that our controls work against these specific threat scenarios."

Rapid Time-to-Value

Zero-infrastructure SaaS deployment. Agentic onboarding go from Zero to Visibility in under 60 minutes.

Operational Harmony

Aligns SecOps, ITOps, and GRC under a single source of truth - eliminating silo fatigue permanently.

GET IN TOUCH

Visit Our Website
www.gambitcyber.org

Chat to Sales
sales@gambitcyber.org

Chat to support
support@gambitcyber.org

Our Locations
The Netherlands | India