amiviz

Four Connected Practices.
One Answer.

The Amiviz Vendor Portfolio:
Security, Data, AI and Infrastructure

A Straight Answer in a Market Full of Vendor Noise

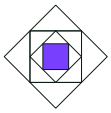
Every vendor says it solves your problem. Few can show you how it behaves inside your estate, under your regulator.

Amiviz is the MEA region's most trusted consultative Value-Added Distributor — the partner organisations call when the technology decision is complex, the stakes are high, and they need an advisor who sees the full picture. A traditional distributor earns its margin through logistics, credit and scale. We earn ours through expertise. We advise on architecture before a purchase is made, and we're compensated to give the right answer.

That's why we've vetted every vendor in this portfolio with a specialist, not added it to a catalogue. Our specialists assess how the technology fits an architecture, which national mandates it helps you meet, and what it delivers once live. Where it matters, we validate it in our Customer Experience Centre before you commit budget.

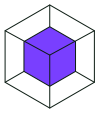
One Advisor. Four Practices. One Answer.

Security is where the conversation starts. It rarely ends there. Security, data, AI and infrastructure have become one conversation, and most distributors answer only one of those questions well. Amiviz answers all four, from a single point of accountability.



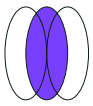
Cybersecurity

The foundation — the operating condition everything else depends on.



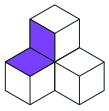
Data & Resilience

The layer that makes AI and cloud investment trustworthy.



Sovereign Cloud & AI

The frontier — where cloud sovereignty and AI governance meet.



Digital Infrastructure

The connective tissue — network, compute and edge, at scale.

Application Delivery, DDoS & AI Security

A10 Networks delivers secure application and network solutions that protect, optimise and scale business-critical systems across on-premises, hybrid cloud and edge environments. Its portfolio spans Thunder ADC for application delivery, Thunder TPS and A10 Defend for automated DDoS protection, carrier-grade networking and firewalls, and centralised management and analytics. A10 has extended this foundation into AI security, with TrojAI guardrails and red teaming for AI models, the A10 AI Gateway for governing LLM traffic, and ThreatX API protection. Service providers and enterprises use A10 to keep applications fast, available and secure as they modernise their infrastructure for the AI era.

Behavioural AI Email Security

Abnormal AI is a behavioural AI security platform that stops the human-targeted attacks traditional defences miss. By understanding identity, behaviour and context, it baselines how every employee and vendor normally communicates and flags the subtle deviations that signal phishing, business email compromise, vendor fraud and account takeover. The platform connects by API to Microsoft 365 and Google Workspace in minutes, with no MX changes, and extends protection to collaboration and cloud apps such as Slack, Zoom, Workday and ServiceNow. AI-driven automation triages user-reported emails and removes threats automatically, reducing manual investigation and easing the load on security teams.

Cyber Deception & Identity Protection

Acalvio is a leader in autonomous cyber deception, helping organisations detect attackers early, before they reach critical assets. Its ShadowPlex platform uses AI to deploy realistic decoys, honeytokens and deceptive credentials at scale across IT, OT, cloud and identity environments. Because legitimate users have no reason to touch these assets, any interaction is a high-fidelity sign of malicious activity, exposing lateral movement, credential misuse, insider threats and ransomware with minimal false positives. ShadowPlex Identity Threat Protection extends this to ITDR, adding a proactive detection layer that complements existing security controls on-premises, in the cloud or through managed service providers.



Network Security Policy Management

AlgoSec helps organisations securely accelerate application delivery by automating application connectivity and security policy across hybrid networks. The AlgoSec Horizon platform uses AI to discover business applications and map their connectivity across multi-cloud, SDN and on-premises environments, then automates policy changes from planning and risk assessment through implementation and validation. It flags risky rules, misconfigurations and compliance gaps, delivers audit-ready reporting and integrates with ITSM, SIEM/SOAR and vulnerability management tools. Security, network and application teams gain a single source of visibility, so they can reduce risk and speed up change without compromising security.



Threat Intelligence & Security Operations

Anomali is an intelligence-native, agentic security operations platform that brings security data, threat intelligence and AI together. The Anomali Data Lake unifies telemetry from cloud, endpoint, network and identity sources at scale, while ThreatStream Next-Gen enriches it with curated global threat context so teams can spot risk earlier. Anomali Copilot and agentic AI guide investigations, recommend next steps and automate repetitive response tasks, with analysts in control. By consolidating SIEM, threat intelligence and SOAR capabilities, Anomali removes the need to stitch together fragmented tools and helps SOC teams detect, investigate and respond to threats faster and with greater confidence.



Data Security, Privacy & AI Governance

BigID is the data intelligence company built for the AI era, helping organisations find, understand, secure and govern their data wherever it lives. Its BigID Next platform uses AI-driven discovery and classification to build a unified view of sensitive and regulated data across cloud, on-premises, SaaS, data lake and AI environments, connecting data to identity, access and lineage for complete context. It combines DSPM, access governance, data cataloguing, retention, privacy automation and AI governance in one platform, helping security, privacy, governance and AI teams reduce data risk, minimise redundant data, automate compliance with global regulations and adopt AI safely with well-governed, trusted data.

Cyber Risk Intelligence & TPRM

Bitsight is a global leader in cyber risk intelligence, helping organisations understand their own risk, the risk posed by their third parties and the threats targeting them. Its platform combines extensive external security data and analytics with deep, dark and clear web threat intelligence, giving real-time visibility across the extended attack surface, including infrastructure, cloud, identities and third- and fourth-party ecosystems. Solutions span Security Performance Management, Third-Party Risk Management and Cyber Threat Intelligence, helping security, GRC and procurement teams benchmark posture, monitor vendors, prioritise exposures and report cyber risk in business terms to executives and boards.

Secure Communications & Endpoint Management

BlackBerry protects the communications, devices and critical operations of governments, defence organisations, critical infrastructure and regulated enterprises. Its Secure Communications portfolio includes SecuSUITE for certified encrypted voice and messaging, BlackBerry UEM and Dynamics for secure endpoint management, Workspaces for secure file sharing and AtHoc for critical event management, with Certicom adding cryptography and PKI expertise. Deployable on-premises, in sovereign cloud or hybrid, BlackBerry keeps organisations in control of their keys, data and infrastructure, helping them protect sensitive information, keep mobile workforces productive and coordinate people during crises.

Enterprise Security, Identity & Data Protectiony

Broadcom's Enterprise Security Group delivers Symantec and Carbon Black solutions that protect users, endpoints, information and identities across hybrid environments. Symantec Endpoint Security and Carbon Black provide layered prevention, EDR, application control and XDR, while Symantec Network Protection and CloudSOC CASB secure web and cloud access. Symantec DLP and Email Security protect sensitive data and defend against phishing and targeted attacks, and Symantec Identity Security secures workforce and privileged access. Backed by global threat intelligence, Broadcom helps large enterprises consolidate controls, enforce consistent policy and reduce risk across complex, mission-critical environments.

API, Bot & Agentic AI Security

Cequence Security is a leader in application, API and agentic AI protection, securing the applications and data that power the agentic enterprise. The Cequence Platform unifies API security, bot management and an AI Gateway, continuously discovering and testing APIs, blocking automated attacks, fraud and abuse, and protecting sensitive data in real time. Agent Trust capabilities verify AI agent identity, uncover shadow AI and govern how agents access enterprise applications and data. Deployable without code changes and delivering value in minutes, Cequence helps organisations run digital services securely at scale, reduce account takeover and API abuse, and adopt agentic AI with confidence.

Network, Cloud & Workspace Security

Check Point Software Technologies is a leading provider of AI-powered, cloud-delivered cyber security, protecting organisations and governments worldwide with a prevention-first approach. The Check Point Infinity Platform spans four pillars: Hybrid Mesh Network Security, Workspace Security, Exposure Management and AI Security. It covers Quantum firewalls, Harmony SASE, Endpoint, Mobile and Email & Collaboration, CloudGuard CNAPP and WAF, and GenAI Protect, all powered by ThreatCloud AI threat intelligence. Unified management gives teams consistent policy and visibility across on-premises, cloud and remote environments, helping organisations prevent sophisticated attacks and secure their AI transformation.

Endpoint, Identity & Cloud Security

CrowdStrike is a global cybersecurity leader whose AI-native Falcon platform stops breaches across endpoints, identities, cloud workloads, data and AI. Built on a single lightweight agent and cloud-native architecture, Falcon unifies endpoint protection and XDR, identity protection, cloud security, exposure management, data protection, SaaS security and Next-Gen SIEM in one platform. Charlotte AI and agentic workflows accelerate detection, investigation and response, while Falcon Complete MDR, incident response and threat intelligence extend the team with elite expertise. CrowdStrike helps organisations consolidate tools, reduce complexity, achieve rapid time-to-value and stay ahead of modern adversaries.

AI Data Security, DLP & Insider Risk

Cyberhaven is a leader in data security for the agentic enterprise, protecting sensitive information as it moves between people, applications, endpoints, browsers and AI tools. Its platform is built on data lineage, tracing data from creation through every copy, edit and share, and linking it with identity and behaviour. This context powers DLP, DSPM, insider risk management and AI security in one solution, including visibility into shadow AI and control over what data reaches AI tools and agents. Agentic AI classifies data, detects risky flows and guides response in real time. Security teams stop data loss and insider threats with far fewer false positives, while employees keep using AI tools productively and safely.

AI-Driven Threat Detection & Response

Darktrace secures the modern enterprise by protecting AI, people and infrastructure with behavioural security. Its Self-Learning AI understands what is normal for each organisation, detecting known, unknown and novel threats that rules- and signature-based tools miss. The platform delivers unified visibility and autonomous response across network, email and collaboration tools, cloud, identity, endpoint and OT, with Darktrace / SECURE AI protecting AI systems and agents. Cyber AI Analyst automates investigations, while proactive exposure management helps teams harden defences before an attack, so they can contain threats at machine speed and build lasting resilience across critical infrastructure and government.

Sovereign Data Security & Key Management

Datashield is a unified enterprise data security platform from SITE (Saudi Information Technology Company), powered by confidential computing. It combines multi-cloud key management, data masking and tokenisation, secure DevOps and secrets protection with a natively integrated FIPS 140-2 Level 3 HSM. A zero-trust architecture with granular role-based access control, quorum approvals and single sign-on keeps keys and data under the organisation's control. Delivered as a service from in-Kingdom infrastructure, Datashield helps government and enterprise organisations meet data sovereignty and regulatory requirements and simplify encryption at scale, without running their own cryptographic infrastructure.



DDI & DNS Security

EfficientIP is a network security and automation company specialising in DNS, DHCP and IP address management (DDI). Its SOLIDserver platform unifies DDI with DNS security, automation and observability across on-premises, hybrid and multi-cloud networks, creating a single, reliable source of truth for IP infrastructure. DNS Guardian and DNS Firewall detect and block DNS-based attacks, data exfiltration and malware communications, while open APIs connect DDI data into IT, security and DevOps workflows, and the DDI Observability Center adds network insight. EfficientIP helps network, security and DevOps teams automate core network services, strengthen their security posture and keep business-critical applications and services available.



PKI & Certificate Lifecycle Management

Evertrust is a European software vendor delivering a sovereign platform for PKI, certificate lifecycle management and cryptographic posture management. Evertrust Stream provides a modern certificate authority, Horizon automates the discovery, issuance, renewal and revocation of certificates at scale, and Evertrust CPM continuously assesses cryptographic assets against regulations such as NIS2, DORA and PCI DSS. Available as SaaS, on-premises or hybrid, the platform integrates with existing IT and DevOps environments, helping organisations prevent certificate-related outages, control machine identities, produce audit-ready evidence and prepare for a smooth transition to post-quantum cryptography.



SIEM, UEBA & Security Operations

Exabeam is a leader in behaviour intelligence for the agentic enterprise, helping security teams detect, investigate and respond to threats from human and non-human insiders. As the pioneer of UEBA, it baselines normal activity for users, devices and AI agents, surfacing insider threats, compromised credentials and anomalous behaviour that other tools miss. Its cloud-native New-Scale Security Operations Platform delivers threat detection, investigation and response (TDIR), complemented by LogRhythm SIEM for self-hosted or hybrid deployments. Exabeam Nova AI agents accelerate triage and investigation, improving SOC productivity and reducing risk across an increasingly AI-driven workforce.

EXTRAHOP

Network Detection & Response (NDR)

ExtraHop is a leader in real-time network intelligence, giving security and IT teams complete visibility across hybrid environments. Its RevealX platform combines network detection and response (NDR), network performance monitoring, intrusion detection and packet forensics in one solution. By decrypting and analysing traffic at scale with behavioural analytics and machine learning, RevealX detects lateral movement, ransomware and advanced attacks that evade endpoint and log-based tools. High-fidelity network context also feeds AI agents and automation, powering the agentic SOC and NOC, so teams can investigate with definitive evidence, respond with confidence and improve application and network performance.

Fidelis Security

XDR, NDR & Cloud Security

Fidelis Security delivers proactive cyber defence for enterprise and government, helping organisations detect, hunt and respond to threats across network, endpoint and cloud environments. Its Fidelis Elevate XDR platform combines network detection and response, endpoint detection and response, deception and Active Directory protection, correlating rich telemetry and context to expose post-breach activity that other tools miss. Fidelis Halo, a cloud-native application protection platform, secures servers, containers and workloads across hybrid and multi-cloud environments. Together, they help security teams shrink attacker dwell time, contain threats faster and strengthen resilience against advanced adversaries.

FLASHPOINT

Threat & Vulnerability Intelligence

Flashpoint is a leading provider of threat data and intelligence, helping businesses and governments protect their people, places and assets from cyber, fraud and physical threats. Its Flashpoint Ignite platform combines data collected from the open, deep and dark web and illicit communities with expert human analysis and AI. Covering cyber threat, vulnerability (VulnDB), fraud, physical and geopolitical intelligence, Flashpoint helps security, fraud and intelligence teams uncover compromised credentials and ransomware activity early, prioritise the vulnerabilities attackers are actively exploiting, and make faster, better-informed decisions that reduce risk, prevent financial loss and strengthen operational resilience.

Credential Management & MFA

Intercede is a cybersecurity software company specialising in digital identity, protecting organisations against compromised credentials, one of the leading causes of data breaches. MyID CMS manages the full lifecycle of high-assurance credentials, including PKI smart cards, virtual smart cards and FIDO2 passkeys, while Authlogics delivers password security, breached password screening, one-time passwords and MFA. Secure registration and identity verification ensure credentials reach the right people. Trusted by government, defence and financial services, Intercede helps organisations move to phishing-resistant, passwordless authentication and meet standards such as FIPS 201 and NIST SP 800-63.

Endpoint Management, ITSM & Secure Access

Ivanti is a global enterprise IT and security software company that helps organisations manage, secure and service every device, user and application. The AI-powered Ivanti Neurons platform connects IT and security data into a unified system of record, giving teams a trusted foundation for autonomous endpoint management. Its portfolio spans unified endpoint management, patching, IT service and asset management, risk-based vulnerability and exposure management, and Zero Trust secure access through Ivanti Connect Secure. Automation and self-healing reduce manual effort and downtime, while giving IT and security teams shared visibility to close exposures faster and deliver a secure, productive employee experience.

Endpoint Security, XDR & Threat Intelligence

Kaspersky is a global cybersecurity and digital privacy company protecting businesses, critical infrastructure and governments with AI-driven security and deep threat expertise. Its Kaspersky Next product line scales with the business, from endpoint protection and EDR to open XDR, while the wider portfolio covers Kaspersky SIEM, threat intelligence, industrial OT security, mail and container security, and automated security awareness training. Managed detection and response and expert SOC services add specialist support. Backed by strong independent test results, Kaspersky helps organisations detect and respond to advanced threats, reduce workloads on security teams, prevent downtime and protect revenue.

Kiteworks

Secure Data Exchange & AI Governance

Kiteworks helps organisations govern and manage risk in every send, share, receive and use of private data. Its Private Data Network unifies secure email, file sharing, managed file transfer, SFTP, web forms and APIs under one policy engine, audit log and encryption model, delivered as a hardened, single-tenant virtual appliance on-premises, in private cloud or as a hosted service. The Kiteworks AI Data Gateway extends the same governance to AI agents and large language models, controlling how they access sensitive content. Kiteworks helps regulated enterprises and government agencies prove compliance, keep full control of where their data lives and adopt AI without exposing sensitive content.

LMNTRIX
BE THE HUNTER | NOT THE PREY

XDR & Managed Detection and Response

LMNTRIX delivers an AI-driven XDR platform, 24/7 managed detection and response and offensive security services. Built on an assume-breach approach, its Active Defense platform brings endpoint, network, cloud, identity, email, mobile, OT and AI security together with deception, threat intelligence and continuous validation. The Artemis agentic AI engine investigates alerts automatically, while the LISA assistant delivers findings to analysts. LMNTRIX Cyber Defense Centers provide round-the-clock monitoring, threat hunting and response, and LMNTRIX Recon adds external attack surface intelligence, helping organisations contain threats rapidly without the cost and complexity of building an in-house SOC.

MENLO SECURITY

Browser Security for People & AI Agents

Menlo Security is the pioneer of the Browser Security Platform, protecting the place where most work now happens. Its cloud-delivered platform secures every browser session for people and AI agents, without endpoint software or impact on the user experience. Built on patented isolation technology, it stops evasive phishing, zero-day and browser-based malware before it reaches the endpoint. Capabilities include HEAT Shield AI-powered phishing prevention, data loss prevention, file security, GenAI usage controls and secure access for unmanaged devices, while Menlo Agent Runtime Security extends governance to autonomous AI agents, securing hybrid human and agentic workforces.

Extended Detection & Response (XDR)

METRAS is a Saudi cybersecurity company formed by SITE and Privafy to localise advanced cybersecurity technology and build national capability. Its MetrasXDR platform uses a single lightweight agent to collect and analyse endpoint telemetry, with behavioural detection, MITRE ATT&CK mapping and AI-generated investigation summaries in one console. Security teams gain clear visibility, faster triage and guided response without juggling multiple tools. Backed by managed detection and response from Saudi-based experts, METRAS helps government and enterprise organisations detect, investigate and contain threats without running their own SOC, while meeting national data sovereignty and regulatory requirements.

SAP Application Security

Onapsis is the global leader in SAP cybersecurity and compliance, protecting the business-critical applications that run finance, supply chain, manufacturing and HR. The SAP-endorsed Onapsis Platform combines vulnerability and compliance management (Assess), real-time threat detection (Defend) and code and transport security (Control) across RISE with SAP, S/4HANA Cloud, SAP BTP and hybrid landscapes. Powered by the Onapsis Research Labs, it gives security and SAP teams a shared view of risk, while agentic AI capabilities automate SAP security workflows, helping organisations prevent breaches, accelerate audits and keep SAP cloud and AI initiatives secure with rapid time to value and measurable risk reduction.

Authentication & Mobile App Security

OneSpan helps banks and other regulated organisations build secure, seamless digital experiences. Its cybersecurity portfolio protects identities, mobile apps and high-value transactions through high-assurance authentication, transaction signing, mobile app shielding, threat intelligence and fraud prevention. The DigipassONE platform brings these capabilities onto one shared foundation, on-premises or in the cloud, in software or hardware form, including trusted Digipass authenticators. Organisations can adopt phishing-resistant methods such as passkeys and FIDO2 while protecting existing investments, helping them reduce fraud, meet regulatory requirements and give customers fast, frictionless access.



Human Risk Management

PhishRod is a human risk management company that helps organisations identify, predict and reduce the cyber threats caused by human behaviour. Its AI-powered platform brings together phishing simulation, security awareness training, phishing incident response, user behaviour monitoring and policy compliance management. By personalising awareness to individual risk, automating the reporting and remediation of suspicious emails and tracking policy acknowledgement across the workforce, PhishRod helps security and compliance teams measure employee readiness, demonstrate regulatory compliance and turn employees into an active line of defence within a lasting, organisation-wide cyber-secure culture.



Security Validation & Breach and Attack Simulation

Picus Security is a leading exposure validation company that helps organisations prove what attackers can actually exploit and whether their defences can stop them. The Picus Platform combines Breach and Attack Simulation, automated penetration testing, attack path validation and detection rule validation to continuously test security controls against real-world threats. Rather than simply listing vulnerabilities, Picus prioritises the exposures that matter, delivers ready-to-apply mitigations and re-validates once fixes are in place. With extensive integrations across leading security technologies, Picus helps security teams measure and improve resilience and get more from existing security investments.



Post-Quantum Cryptography

QuantumGate helps governments, critical infrastructure and enterprises prepare for the quantum era with post-quantum cryptography and secure communication solutions. Built on cryptographic libraries developed at Abu Dhabi's Technology Innovation Institute, its portfolio includes QSphere for quantum-resistant encryption and connectivity, Salina for phishing-resistant identity, Cryptographic Discovery for a complete inventory of cryptographic assets, and Secure VMI for protected mobile work. Advisory and migration services help organisations plan and execute their transition, defend against 'harvest now, decrypt later' threats, achieve crypto-agility and meet national cryptography regulations.

Rakeen
part of Site

Network, Endpoint & XDR Security

Rakeen is a Saudi cybersecurity company and a subsidiary of SITE, developing locally built security products for public and private sector organisations in the Kingdom and the wider region. Its portfolio covers next-generation firewalls, intrusion prevention, endpoint protection with EDR and an AI-driven XDR platform, delivered as SaaS on the SITE Sovereign Cloud. Rakeen XDR correlates telemetry from multiple sources to help teams detect, investigate and respond to complex threats. With in-Kingdom hosting and integration with SITE threat intelligence and managed detection and response, Rakeen helps organisations strengthen cyber resilience, keep sensitive data sovereign and build national cybersecurity capability.

runZero

Exposure Management for IT, OT & IoT

runZero delivers a single source of truth for exposure management across the total attack surface, helping organisations find and secure every asset, including the ones they did not know they had. Its platform combines proprietary active scanning, passive discovery and API integrations to discover and fingerprint IT, OT, IoT, cloud, mobile and external assets in detail, without agents or credentials. runZero identifies unmanaged and rogue devices, unknown networks and missing security controls, then prioritises exposures by risk, giving security and IT teams complete visibility and closing coverage gaps across complex environments. Remediation tracking and reporting help verify that issues are actually fixed.

sectona

Privileged Access Management (PAM)

Sectona is a privileged identity security company that helps organisations control, monitor and secure privileged access across on-premises, cloud and endpoint environments. Its Modern Infrastructure Access Platform unifies privileged access management, endpoint privilege management and cloud access management in one easy-to-deploy solution. Password and secrets management, session monitoring and recording, just-in-time access and least-privilege enforcement remove standing privileges and reduce the risk of account abuse. Secure remote and third-party access and detailed audit trails help security teams protect critical credentials and meet compliance requirements across hybrid and DevOps environments.

Securiti AI
a Veeam company

Data & AI Security, Governance & Privacy

Securiti AI, now part of Veeam, is a leader in data and AI security and governance, helping enterprises find, understand and control sensitive data so they can use it safely with AI. Its unified platform is built on a knowledge graph that maps data, identities, AI models and regulations across cloud, SaaS, data lakes and on-premises environments. On this foundation, it delivers data security posture management, data access governance, data cataloguing, privacy automation and AI governance, while Agent Commander helps secure and govern agentic AI. Organisations use Securiti to reduce data risk, automate compliance with global privacy regulations, lower operational cost and adopt generative and agentic AI safely.

securonix

Agentic AI SIEM & Security Operations

Securonix delivers the industry's first Unified Defense SIEM with agentic AI, helping security teams detect, investigate and respond across the full threat lifecycle. Its cloud-native platform unifies SIEM, UEBA, SOAR and threat intelligence, with Sam, the AI SOC Analyst, supporting triage, investigation and response under human oversight and built-in guardrails. Advanced Behavioral Analytics extends detection beyond users and entities to AI agents, while ThreatQ, now part of Securonix, adds curated external threat intelligence and Data Pipeline Manager helps control data costs. Securonix helps organisations reduce alert noise and run faster, governed security operations at scale, with approvals and audit records retained.

segura®

Privileged Access & Identity Security

Segura, formerly senhasegura, is a global identity and privileged access management company. Its 360° Privilege Platform delivers modern PAM for human, machine and autonomous AI identities, combining privileged access management, endpoint privilege management, cloud entitlements (CIEM), DevOps secrets, certificate management and VPN-less remote access in a single platform. Session recording, automated credential rotation and just-in-time, least-privilege elevation reduce the attack surface and the risk of credential misuse. Designed for fast deployment and a low total cost of ownership, Segura helps organisations enforce least privilege and stay audit-ready across on-premises, cloud and DevOps environments.

sysdig

Cloud & AI Workload Security (CNAPP)

Sysdig delivers cloud security powered by runtime insight, open innovation and agentic AI. Founded by the creators of Falco and Wireshark, it helps security and development teams secure containers, Kubernetes, cloud services and AI workloads. Sysdig Secure is a cloud-native application protection platform (CNAPP) that unifies posture, vulnerability and entitlement management with cloud detection and response, using runtime context to prioritise the risks actually in use. Sysdig Sage, an AI cloud security analyst, speeds investigation, and runtime protection now extends to AI coding agents, helping teams cut through noise, stop attacks in real time and secure hybrid and multi-cloud environments.

tenable®

Exposure Management & Vulnerability Auditing

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. Its AI-powered platform, Tenable One, unifies visibility, insight and action across the attack surface, including IT, OT, cloud, identity, web applications and AI. Built on Tenable's long heritage in vulnerability management, the portfolio spans vulnerability management, cloud security, identity exposure, OT security, attack surface management, web app scanning and AI exposure. Predictive prioritisation and attack path analysis help teams focus on the exposures most likely to be exploited, so organisations can understand their true cyber risk and reduce it continuously and measurably.

utimaco®

HSMs & Key Management

Utimaco provides cybersecurity and compliance solutions that protect sensitive data, cryptographic keys, identities and payment transactions. Its portfolio centres on hardware security modules, including u.trust general-purpose HSMs and Atalla payment HSMs, alongside enterprise key management and file and disk encryption. Available on-premises or through Utimaco's Trust as a Service and cloud HSM offerings, it gives organisations cryptographic control without managing infrastructure. With certified products and support for post-quantum algorithms, Utimaco helps financial institutions, payment providers, governments and enterprises meet compliance requirements and prepare for quantum-safe cryptography.



Data Storage Infrastructure for AI & HPC

VDURA provides high-performance data storage infrastructure for AI factories, neoclouds and high-performance computing. The VDURA Data Platform combines the speed of a parallel file system with the durability and economics of object storage, in a software-defined architecture spanning flash and disk. It keeps GPUs fully utilised with consistent, high-throughput performance, while multi-tenancy, API-first automation, S3 support and intelligent data tiering simplify operations at scale. Built-in data protection keeps clusters online as environments grow, helping organisations accelerate AI and HPC workloads, scale capacity cost-effectively and protect critical data without operational complexity.



Data Resilience, Security & AI Trust

Veeam is the Data and AI Trust Company and a market leader in data resilience, helping organisations protect, recover and secure their data wherever it lives. Following its acquisition of Securiti AI, Veeam connects backup and recovery, cyber and ransomware recovery, data security posture management, privacy and AI governance in one platform. Its portfolio includes Veeam Data Platform, Veeam Data Cloud, Veeam Backup for Microsoft 365, Veeam Kasten and Agent Commander for governing agentic AI. Organisations can recover clean, trusted data quickly after ransomware, outages or AI errors, understand and secure their sensitive data, and adopt AI safely across cloud, virtual, physical, SaaS and Kubernetes environments.



AI Agent Security & Governance

WhiteMatter, formerly Quilr, is an agent-native company that secures and operationalises the agentic enterprise, governing every AI agent across its entire lifecycle. Its platform discovers every agent, model and MCP server an organisation runs or builds, gives each agent its own identity and tests it before it runs, with red teaming and threat modelling that show its blast radius. At runtime, one policy engine decides every action in the browser, on the endpoint, at LLM and MCP gateways and inside the agent runtime, while a dedicated Guardian Agent coaches users and agents in real time. WhiteMatter also tracks what every agent costs and delivers, helping security, platform and engineering teams adopt AI safely and at scale.

ZEROFOX

Digital Risk Protection & Threat Intelligence

ZeroFox delivers actionable intelligence to discover, validate and disrupt external threats at scale. Its platform protects organisations across the public attack surface, beyond the traditional network perimeter, combining cyber threat intelligence, brand and domain protection, executive and VIP protection, physical security intelligence and external attack surface management. By continuously monitoring the surface, deep and dark web, social media and digital channels, ZeroFox uncovers impersonation, phishing domains, leaked credentials, fraud and threats to people, then removes them through automated takedowns, helping security, fraud and brand teams protect revenue, brand reputation and people.

Vendor descriptions are supplied by each vendor.
Territorial coverage varies by product.
Visit www.amiviz.com for details.

When the Decision Is Complicated, Talk to an Advisor

Amiviz secures your technology estate, governs your data, deploys your AI, and builds the infrastructure that holds it all together.

Tell us what you're working on, and we'll bring the right specialist into the room.

Email: info@amiviz.com **Visit: www.amiviz.com**

Our Offices

UAE
2403, Mazaya Business Avenue, BB1 Tower, JLT, Dubai

+971 4 435 7209

Saudi Arabia
Office 5000, 3rd Floor, Olaya View, King Fahd Road, Al Wurud District, Riyadh 12215

+966 50 3100 074

Egypt
Office 601, 6th Floor, Hegaz Grand Plaza, Maadi, Cairo

+20 2 37880485

amiviz