eventus™

PRODUCT DATASHEET

RedArc CTEM AGENTIC

Continuous Threat Exposure Management Platform

See more of your attack surface. Understand what matters. Validate exposure with control.

Connect attack-surface visibility with business context to prioritise exposure and guide action.

RedArc is Eventus Security's agentic CTEM platform. It brings asset signals together to help teams understand what is exposed, why it matters and who needs to act.

RedArc's External Attack Surface Management (EASM) offering is commercially available. Planned expansion covers cloud posture, vulnerability context and risk quantification; internal attack surface and identity; and controlled adversarial validation.

> **The primary object is an exposure, not a CVE.**
> Each exposure brings together the affected asset, supporting evidence, business importance, ownership and remediation state. CVEs are signals, not the whole decision model.

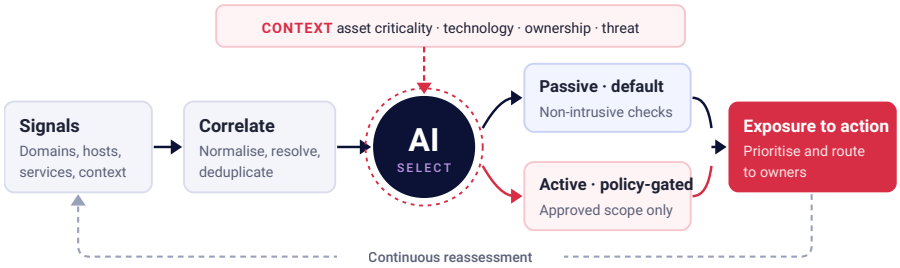
PLATFORM APPROACH

Continuous visibility
Internet-facing assets, applications, APIs, services, certificates, DNS and technology fingerprints.

Contextual assessment
Passive signals by default; active verification gated by policy, confidence and risk.

Risk-based action
Correlate, deduplicate, prioritise and route exposures with evidence and ownership.

HOW REDARC WORKS



What "agentic" means in RedArc. AI assists discovery, correlation and assessment planning. Explicit authorisation and deterministic policy rules decide what actually runs.

USE CASES

Find unknown assets
Surface forgotten domains, shadow IT and orphaned cloud assets before they fall outside assessment coverage.

Cut exposure noise
Deduplicate findings and focus effort on exposures that are reachable and business-critical.

Assurance between pentests
Continuous discovery and change detection keep coverage current as the footprint changes.

Evidence-backed reporting
Exposure trends and remediation progress for leadership, supported by technical evidence.

PLATFORM

Core platform capabilities

01 Asset intelligence
Domain and subdomain relationships, internet-facing hosts, ports and protocols, web and API surfaces.

02 Technology-aware scanning
Observed stacks and services guide relevant checks, rather than exhaustive testing on every asset.

03 Exposure intelligence
Scanner and source findings normalised into a consistent exposure record with supporting evidence.

04 Safe orchestration
Scope, scan profile, rate limits, target sensitivity, approvals and audit history govern active checks.

05 Continuous change detection
Newly exposed services, changed technologies, drift and recurring weaknesses.

06 Actionable reporting
Tenant-level dashboards, asset and exposure views, prioritisation queues and remediation tracking.

hello@eventussecurity.com | www.eventussecurity.com
© 2026 Eventus Security. All rights reserved.

02 / ASSESSMENT METHOD AND OUTPUTS

How RedArc assesses exposure

An evidence-led pipeline gathers signals, adds asset context and chooses passive or active checks according to the target and a defined safety policy.

SIGNAL SOURCES

EXTERNAL SIGNALS · available now (EASM)

External telemetry: DNS, certificates, registration metadata and public internet observations.

Application surface: websites, APIs, URLs, exposed content and fingerprint signals.

Infrastructure: IP ranges, ports, services, TLS and cloud endpoints.

ENTERPRISE AND SECURITY CONTEXT · roadmap integrations

Security systems: vulnerability scanners, EDR / XDR, SIEM and security alerts.

Enterprise context: CMDB, ownership, business tier, environment and exceptions.

Threat context: threat intelligence, active exploitation and relevant attack techniques.

AI-assisted context engine. Correlates asset identity, technology, service behaviour, exposure history, business criticality, threat relevance and scope policies, then recommends assessments with rationale and confidence. Deterministic policy rules keep final control over execution.

PASSIVE BY DEFAULT, ACTIVE BY POLICY

DEFAULT **Passive assessment**

Enrichment and correlation, configuration and metadata analysis, risk inference and non-intrusive revalidation.

POLICY-GATED **Active assessment**

Service-aware checks, approved safe probes, targeted vulnerability validation and authenticated assessment, only where approved.

WHAT DECIDES THE CHECK

- Technology match
- Source confidence
- Asset criticality
- Test invasiveness
- Authorisation
- Rate limit
- Change window

Unknown or sensitive targets remain passive until active testing is permitted.

PASSIVE	LOW-IMPACT	SCOPED ACTIVE
New unknown host	**Known web stack**	**Approved critical API**
Discovery and technology identification; intrusive checks deferred.	Low-impact validation checks matched to the detected stack.	Scoped, authenticated testing under explicit guardrails.

Illustrative decisions.

OUTPUTS

- **Exposure records:** affected assets, supporting evidence and verification status.
- **Prioritised views:** business context and assessment rationale.
- **Remediation support:** ownership, guidance and status tracking.
- **Leadership reporting:** exposure trends and risk context.

CONTROLS AND ENTERPRISE READINESS

- **Guardrails:** approved scope, permissions, scan profiles and throttling.
- **Traceability:** provenance, timestamps and audit trail; no exploitability claimed without evidence.
- **Tenant-aware:** separate inventories, policies and reporting per tenant.
- **Integration first:** open ingestion for scanner outputs, telemetry and business context.

NEXT STEP

Discuss RedArc architecture, evaluation scope, integration requirements and phased adoption with Eventus Security.

hello@eventussecurity.com
www.eventussecurity.com
India · Middle East · SEA · USA

Roadmap capabilities describe intended product direction, not a commitment to release dates or feature availability. Supported features and integrations are specified for each evaluation. Testing requires authorised scope and agreed controls.

© 2026 Eventus Security. All rights reserved.