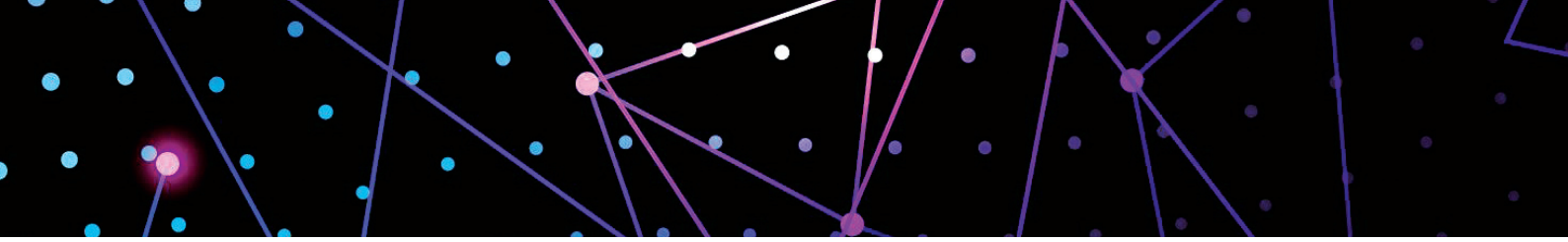
AI-Powered Threat Exposure Management

The Evolving Threat Landscape

In today's hyper-connected world, the cyber threat environment is more volatile than ever. The traditional perimeter has dissolved as organizations expand into cloud, mobile, remote work, and third-party ecosystems. This shift has created a constantly growing attack surface, exposing enterprises to vulnerabilities they often don't even know exist.

ATTACK METRICX



Threat actors are evolving at the same pace — if not faster. From **nation-state adversaries and organized ransomware syndicates** to **hacktivists and financially motivated groups,** attackers are leveraging automation, AI, and underground economies to accelerate their campaigns.

- **Expanding Attack Surfaces:** Misconfigured cloud assets, shadow IT, and third-party integrations are now prime entry points.
- **Underground Economies:** The dark web is thriving with marketplaces selling stolen credentials, zero-days, and insider access.
- **Brand Abuse & Impersonation:** Fake domains, phishing kits, and fraudulent apps erode trust and siphon customers.
- **Ransomware as a Service (RaaS):** Criminal groups are commercializing ransomware, creating supply chains for attacks.
- **AI-Powered Threats:** Deepfakes, generative phishing, and autonomous malware campaigns are redefining speed and scale.
- **Targeted Executive Attacks:** High-profile leaders and VIPs are increasingly targeted for social engineering and reputational damage.

The result? Traditional tools that focus only on patching or scanning are no longer sufficient. Organizations need a **holistic Threat Exposure Management solution** — one that continuously discovers, monitors, and mitigates risks across the **entire threat spectrum**.

Why AttackMetricX?

AttackMetricX is not just an Attack Surface Management (ASM) tool. It is a **comprehensive AI Threat Exposure Management platform** that combines **attack surface intelligence, threat intelligence, brand protection, and executive monitoring** into a unified, scalable solution.

By leveraging **AI-driven analytics, global threat feeds, OWASP and MITRE ATT&CK mapping, and automated remediation workflows**, AttackMetricX empowers organizations to:

- Gain **total visibility** over their digital footprint.
- Detect threats **before they escalate.**
- Customize **countermeasures tailored** to their unique risk profile.
- **Automate remediation** and streamline response processes.
- Enable MSSPs to deliver **scalable, multi-tenant protection** to their customers.

Core Features

1. Attack Surface Intelligence

Your digital footprint is constantly changing — new cloud instances, domains, APIs, and third-party integrations appear every day. AttackMetricX provides:

- Continuous discovery of **domains, subdomains, IP ranges, APIs, cloud services, and SaaS applications.**
- **AI-driven vulnerability prioritization** based on exploitability and business impact.
- Real-time monitoring of **SSL certificates, DNS misconfigurations, exposed services, and shadow IT.**
- Visual **attack surface maps** and intelligence dashboards to simplify risk oversight for CISOs and SOC teams.

2. Dark Web Monitoring

The dark web is where stolen data, credentials, and access points are traded — often before an organization is even aware of a breach. AttackMetricX provides:

- Continuous scanning of **darknet forums, marketplaces, encrypted chats, and illicit data exchanges.**
- Detection of **compromised accounts, leaked databases, stolen files, or insider sales.**
- Alerts when your **company name, brand, customers, or executives** are mentioned in underground chatter.
- Early identification of **ransomware affiliates selling access** to your infrastructure.

3. Brand Protection

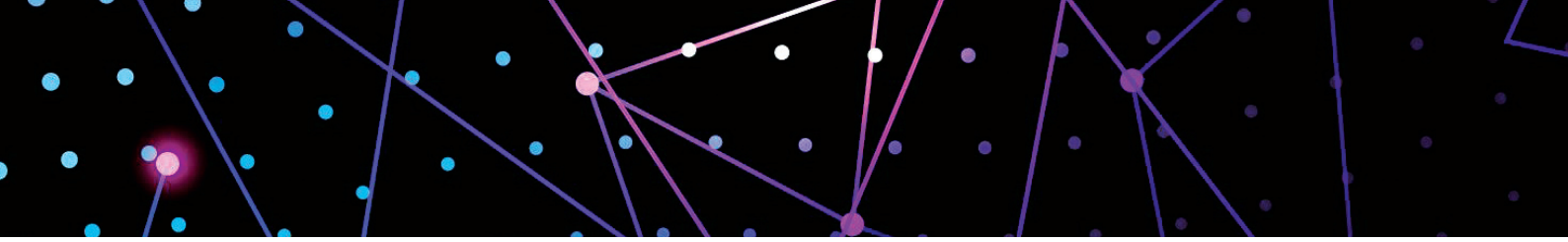
Your reputation is your first line of trust with customers. AttackMetricX actively protects it by:

- Identifying **impersonating domains, typosquatted URLs, cloned websites, and fake apps.**
- Detecting **phishing kits and fraudulent campaigns** in real time.
- Offering support for **takedown operations** across hosting providers, registrars, and social platforms.
- Preserving **customer trust** and reducing exposure to fraud, phishing, and scams.

4. Threat Actor Profiling

Attackers are not anonymous. They leave digital fingerprints in the tools, tactics, and chatter they use. AttackMetricX delivers:

- **Detailed profiles of adversaries** including threat groups, ransomware gangs, and APT actors.
- Mapping of their **TTPs (Tactics, Techniques, Procedures)** against **MITRE ATT&CK.**
- Early warnings on campaigns targeting your sector, region, or supply chain.
- Actionable insights that allow defenders to prepare **counter-strategies aligned with attacker behaviors.**



5. Executive & VIP Threat Monitoring

High-profile individuals within an organization are prime targets for **whaling, spear phishing, and social engineering**. AttackMetricX helps safeguard executives by:

- Monitoring dark web chatter, leaks, and impersonation attempts tied to named individuals.
- Protecting against **personalized phishing lures** and reputation-based attacks.
- Offering alerts on exposed personal data, enabling **preventive action** before exploitation occurs.

6. Threat Intelligence Feeds & Ransomware Watch

AttackMetricX enriches its analysis with **real-time, AI-curated threat intelligence**:

- Feeds of IOCs, malware signatures, phishing indicators, and industry-specific intelligence.
- **A dedicated Ransomware Watch module** that tracks active ransomware families, affiliates, and negotiation tactics.
- Alerts when **ransomware groups announce new victims** or plan sector-specific campaigns.

7. ClearNet (Dorks) Monitoring

Data exposure doesn't just happen in the dark web — it leaks into the open internet too. AttackMetricX:

- Continuously runs **Google Dorking techniques** and other advanced queries to find indexed sensitive data.
- Detects exposed cloud storage buckets, misconfigured collaboration tools, and leaked source code.
- Provides instant alerts so exposures can be contained **before they're weaponized.**

8. Advanced Reporting

AttackMetricX produces reports tailored for every audience:

- **Executive Summaries** for boards and decision-makers, highlighting trends and risk levels.
- **Technical Deep-Dives** for SOC teams, complete with mapped vulnerabilities and exploits.
- **Compliance Reports** automatically aligned with **OWASP Top 10, MITRE ATT&CK, ISO 27001, PCI DSS, and NIST.**
- Export-ready reports for regulators, auditors, and governance bodies.

9. Open API Integrations

AttackMetricX seamlessly integrates into your existing security stack:

- **SIEM & SOAR integrations** for correlation, orchestration, and automated playbooks.
- **ITSM connectors** to ticketing and workflow platforms.
- Flexible APIs for MSSPs to embed intelligence into their service offerings.

10. Advanced Role-Based Access Control (RBAC)

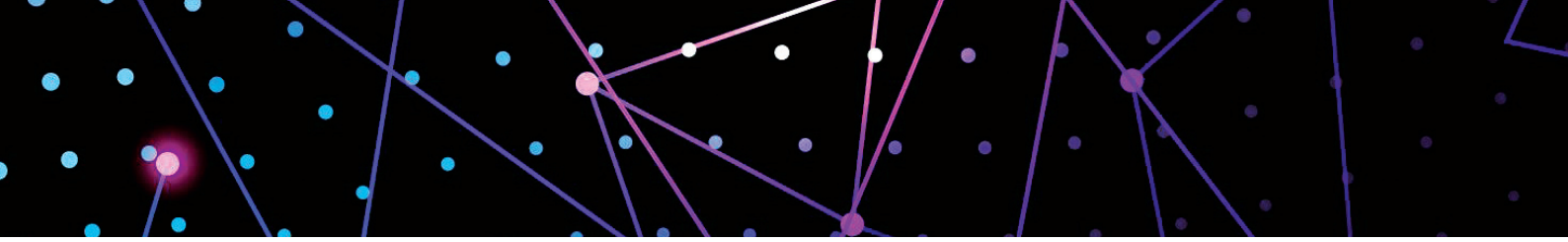
Security is also about governance. AttackMetricX provides:

- **Granular user access policies,** mapped to organizational structures.
- Multi-factor authentication, least privilege enforcement, and audit trails.
- Delegated access for **regional offices, subsidiaries, or business units.**

11. Multitenant MSSP Platform

Designed with **service providers and large enterprises** in mind:

- True multi-tenant architecture with **segregated customer environments.**
- Unified **"single pane of glass" dashboard** for SOC analysts managing multiple clients.
- **Scalable intelligence sharing and reporting** across hundreds of customer tenants.
- Intuitive UI that reduces analyst fatigue and improves operational efficiency.



Why Choose AttackMetricX?

- **AI-Driven Analytics**: Detects, prioritizes, and responds to threats with intelligence that evolves.
- **Full-Spectrum Coverage:** From attack surface to dark web to executive protection.
- **Strategic Framework Alignment:** Integrated with **OWASP, MITRE ATT&CK, PCI, ISO, and NIST.**
- **Actionable Defense:** Countermeasure profiles, remediation wizard, and automated plans reduce MTTR.
- **Enterprise & MSSP Ready:** Scales for banks, governments, and service providers.

CYSTACK ATTACK METRICX CYMETRICX CYSAFE

ELEVATE YOUR **CYBER DEFENSES**

CYSTACK TECHNOLOGY L.L.C

info@attackmetricx.com