THREAT-NG

Cloud & SaaS Security Assessment Unlike Any Other

Requires No Agents, No Credentials, and No APIs

ThreatNG extends External Attack Surface Management (EASM), Digital Risk Protection, and Security Rating capabilities to discover and assess the cloud (Amazon AWS, Microsoft Azure, and Google GCP), a spectrum of SaaS vendors, and uncover open buckets **without using agents**, **credentials**, **API connections**, **browser plugins**, and any other means that require prior knowledge.

Requiring only a domain and organization name, ThreatNG users can perform Outside-In Discovery, Assessment, Reporting, and Monitoring of their Cloud and SaaS Footprint, Exposed Open Buckets, Unsanctioned Implementations (Shadow IT), and Brand Impersonations (Cybersquats).

Cloud

Amazon Web Services (AWS)

Microsoft Azure

Google Cloud Platform (GCP)

SaaS Applications

Analytics

Business Intelligence (BI)

Customer Relationship Management (CRM)

File Sharing

Human Resources

Security

Video Telephony

CONTACT US FOR A FREE EVALUATION

External Attack Surface Management (EASM), Digital Risk Protection, & Security Ratings for Cloud & SaaS

ThreatNG brings Cloud and SaaS into Asset Inventory, Security & Governance, Subsidiary Security Monitoring, Brand Protection, and Third-Party Security Assessments.

External Attack Surface Management

Asset Inventory | Data Leakage Detection | Due Diligence | Cloud & Security Governance | Subsidiary Security Monitoring

- External Cloud & SaaS Footprint Discovery for Asset Inventory
- Bolster Cloud Security & Governance with Reporting & Monitoring for Sanctioned/Unsanctioned Cloud & SaaS Implementations, Open Cloud Buckets, and Exposed Files
- Cloud & SaaS Visibility of Your Organization, Subsidiaries, Partners, Third Parties, and entire Supply Chain

Digital Risk Protection

Brand Protection | Data Leakage Detection | Digital Asset Discovery

- Ensure that All Cloud and SaaS Assets are Properly Accounted for, Branded, and Secured
- Uncover Impersonations (Cybersquats) of Cloud & SaaS implementations
- Highlight Cloudsquats with Exposed Storage Buckets Containing Reputational Damaging Material
- Thwart phishing attacks leveraging SaaS platforms by proactively uncovering SaaSquats

Security Ratings

Due Diligence | Third-Party Risk Assessment | Third-Party Security Monitoring

- Discover, Assess, and Monitor the Cloud and SaaS Footprint of any organization for Third-Party Security Assessments
- Cloud & SaaS Cybersecurity Risk Appetite Customization and Assessment Scoring
- Auto-Generated Substantiated Questionnaire to Facilitate Cloud & SaaS Security Investigations

About ThreatNG

ThreatNG is redefining digital risk protection and external attack surface management with a platform of unmatched breadth, depth, and capabilities in managing technical and business threats across the dark, deep, and open web. Living up to the company mantra ("Security Centric; Not Security Exclusive"), ThreatNG provides a configurable solution to target, discover, and assess digital assets across a definable ecosystem of organizations, subsidiaries, partners, third parties, supply chain, and customers. Bolstered and maintained by the open source intelligence (OSINT) experts at DarcSight Labs, ThreatNG empowers organizations of all types and sizes to uncover, understand, and manage their external digital threats