analyzet

activehacks

Intelligent Adversary Simulation Platform

Strengthen your defenses by validating how well your systems detect, block, and respond to real-world attacks.

activehacks

ActiveHacks

Intelligent Adversary Simulation Platform

Strengthen your defenses by validating how well your systems detect, block, and respond to real-world attacks.

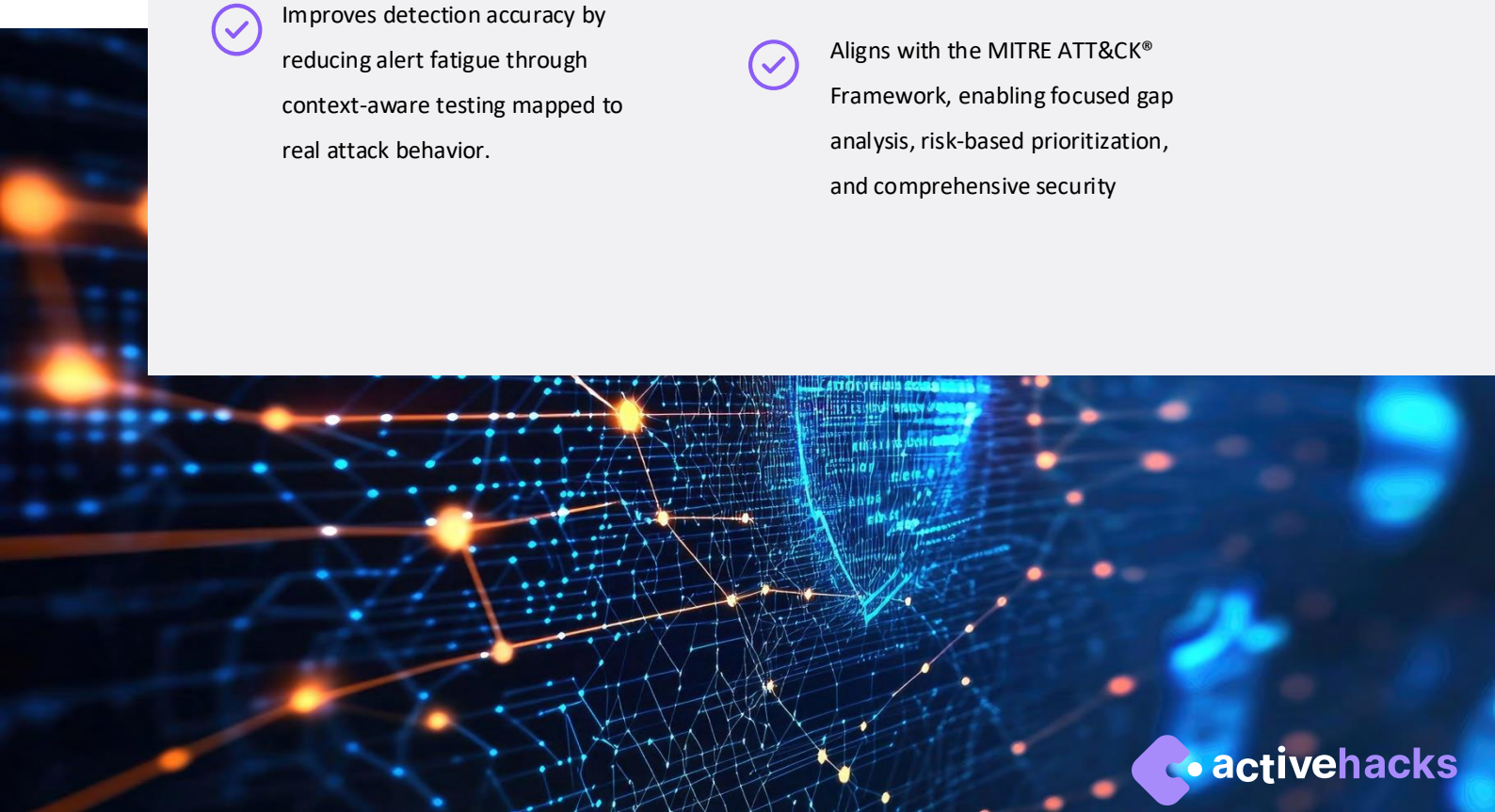
In today's ever-changing threat landscape, It is increasingly challenging for organizations to pinpoint which cyber threats could most impact their business operations. ActiveHacks helps solve this problem with a powerful platform that simulates real-world attacks and checks how well existing security controls work. With coverage across web applications, endpoints, networks, email systems, databases, and Active Directory, ActiveHacks gives security teams a complete view of their defenses. By continuously testing detection and prevention capabilities, it helps teams find security gaps, fix them faster, and stay ahead of critical threats—improving overall cyber resilience.

What ActiveHacks platform does

Validate. Detect. Strengthen.

ActiveHacks is a high-performance Attack Simulation and Security Control Validation platform that:

- Identifies gaps in your cyber defenses by simulating real-world attacks across web applications, endpoints, networks, email systems, databases, and Active Directory.
- Validates the effectiveness of existing security controls with safe, controlled, and customizable threat scenarios.
- Provides actionable, tool-specific remediation guidance to help security teams resolve weaknesses faster and more effectively.
- Improves detection accuracy by reducing alert fatigue through context-aware testing mapped to real attack behavior.
- Integrates with leading SIEM, EDR, and NDR solutions, verifying alert generation, log visibility, and incident response flow.
- Enables continuous posture monitoring with automated or on-demand testing to detect misconfigurations, network changes, and control drift.
- Leverages a rich Threat Simulation Library featuring techniques from malware, ransomware, insider threats, and APT campaigns.
- Aligns with the MITRE ATT&CK® Framework, enabling focused gap analysis, risk-based prioritization, and comprehensive security



Product highlights

Focus on what matters most

Prioritize critical threats and high-impact security gaps while minimizing distractions from low-risk issues.

Simulate real-world threats with actionable insights

Run realistic attack scenarios to uncover context-based vulnerabilities and receive tailored mitigation guidance aligned with your environment.

Streamline SecOps workflows

Enable security teams to focus their efforts on validated threats, reducing investigation fatigue and response delays.

Maximize ROI from security tools

Continuously test and measure the effectiveness of your existing security tools—SIEM, EDR, NDR, WAF, IAM, and more—to ensure optimal

Track security posture improvements over time

Use automated, repeatable, and on-demand simulations to monitor changes, detect control drift, and ensure consistent defense readiness.

Security Framework Alignment

- MITRE ATT&CK Tactics & Techniques
- OWASP Top 10 (Web Application Module)
- Custom control validation (via Threat Builder)

Why Activehacks matters

Proactive Threat Validation:

Automatically assesses control effectiveness against the latest adversarial TTPs.

Security Stack Optimization:

Identifies misconfigurations and tuning opportunities for EDR, SIEM, NDR, IAM, DB logs, and more.

Continuous Assessment:

Offers scheduled and on-demand simulations to detect environmental drift and emerging threats.

Attack Framework Alignment:

All simulations are mapped to MITRE

Customizable Attack Scenarios:

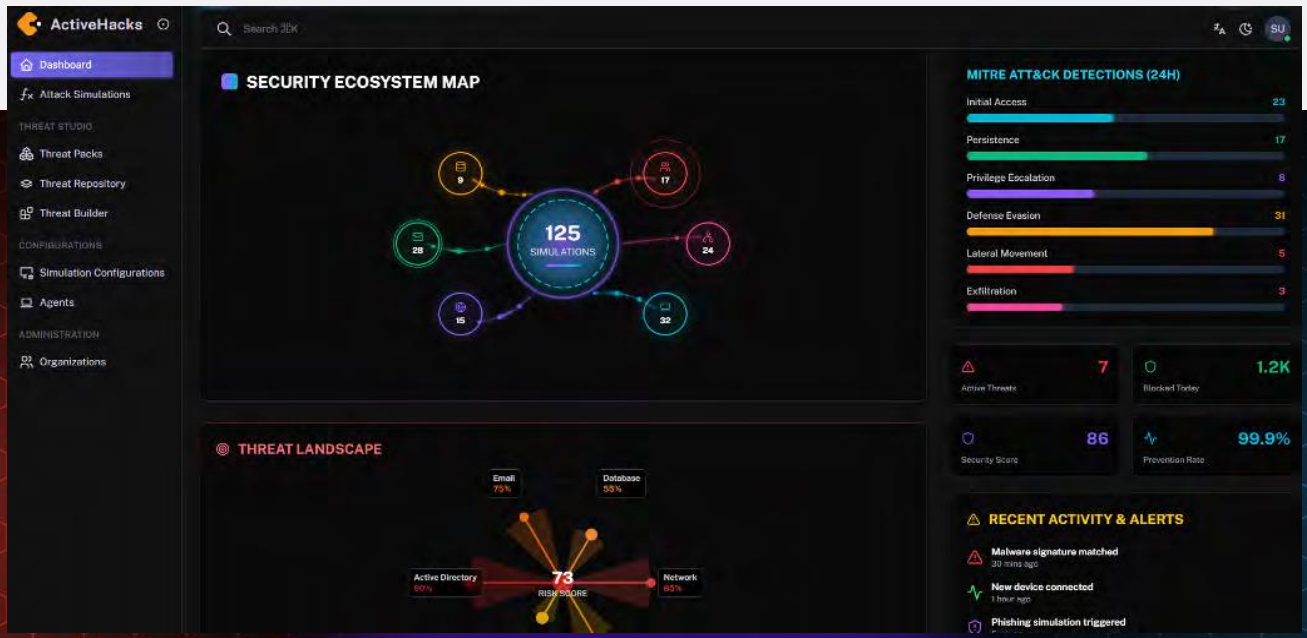
Create targeted simulations tailored to your environment and threat landscape.

Business Impact Visibility:

Translate technical gaps into risk metrics tied to critical assets and operations.

Compliance & Audit Support:

Simulate control effectiveness to support ISO/NIST audits and reduce compliance friction.



activehacks

Key features of ActiveHacks

Multi-vector simulation

Simulate threats across endpoints, networks, email, web apps, Active Directory, and databases.

ATT&CK-Aligned Coverage

Every technique is mapped to MITRE ATT&CK & OWASP Top10 for strategic alignment and coverage visibility.

Agent-Based Execution

Lightweight agents deployed across hosts simulate attack behavior without risk to production systems.

Red Team / Blue Team Modes

Provides realistic offensive emulation and defensive validation workflows.

Cloud-Based Analytics Dashboard

Real-time reporting, heatmaps, and visualizations of detection gaps and attack execution status.

Supports cross-platform operating systems

Windows, MacOS, and Linux

Safe Payload Execution

Executes non-destructive payloads that mimic real malware or adversary behaviors while maintaining environment integrity.

Custom Simulation Profiles

Define reusable TTPs, asset groups, timing controls, and complexity levels to tailor tests.

Integration-Ready

Compatible with SIEM, EDR, SOAR, CMDB, and ticketing platforms for automated response and tracking.

activehacks

MITRE ATT&CK® Mapping

ActiveHack helps organizations strengthen their security posture by mapping simulated attack techniques directly to the MITRE ATT&CK® framework. This allows teams to clearly understand which threat behaviors are detected, missed, or weakly monitored across their environment.

Threat Landscape Mapping

6500+
Real World Attack Scenarios

35K+
Actions

10000 +
Malware Samples

1700 +
Malware Families

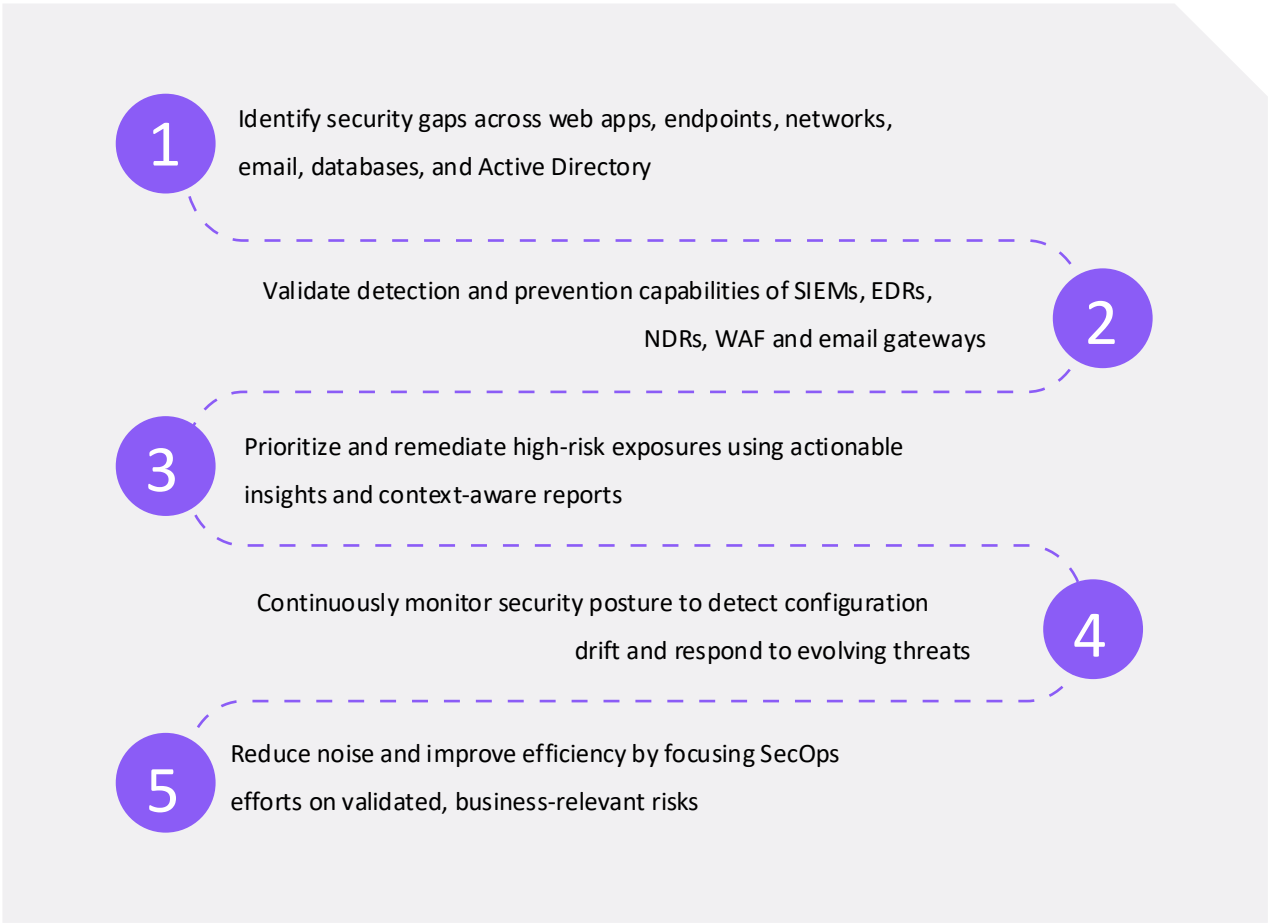
150+
Different Threat Actor Groups

20+
Malware Categories

How ActiveHacks solves the problem

Security teams often struggle to validate whether their controls can detect, block, and respond to today's complex threats. ActiveHacks addresses this challenge with a comprehensive simulation platform that safely emulates real-world cyberattacks across your environment.

By simulating techniques used by modern threat actors—mapped to the MITRE ATT&CK® framework—ActiveHacks helps organizations:



ActiveHacks empowers organizations to take a proactive approach to cybersecurity—ensuring defenses work as intended before a real attack occurs.

activehacks

Core modules and capabilities

Our platform offers a comprehensive suite of attack simulations across network, endpoint, email, web application, Active Directory, and database layers—helping organizations identify vulnerabilities, validate defenses, and strengthen their overall security posture.

Network Infiltration Attack Simulation

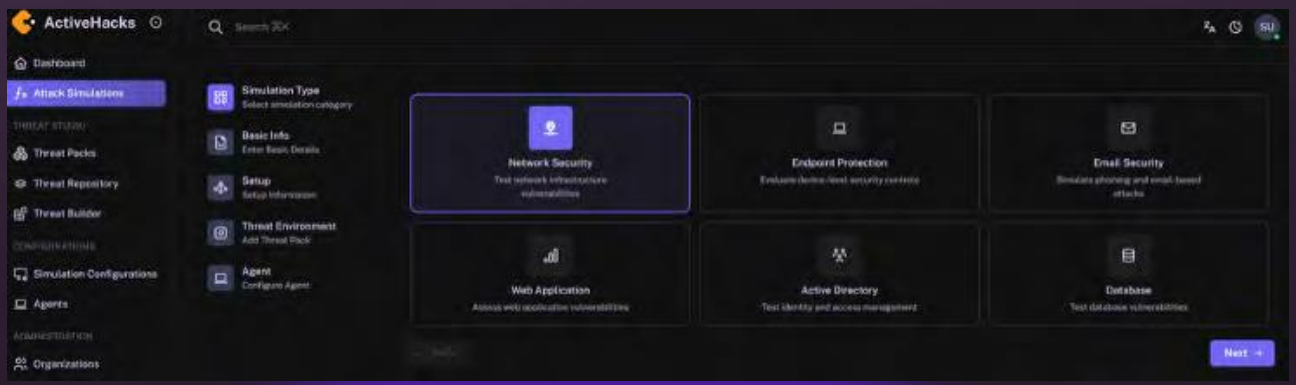
Endpoint Attack Simulation

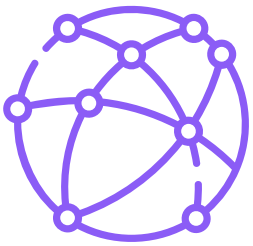
Email Attack Simulation

Web Application Attack Simulation

Active Directory Simulation

Database Attack Simulation





Network Infiltration Attack Simulation

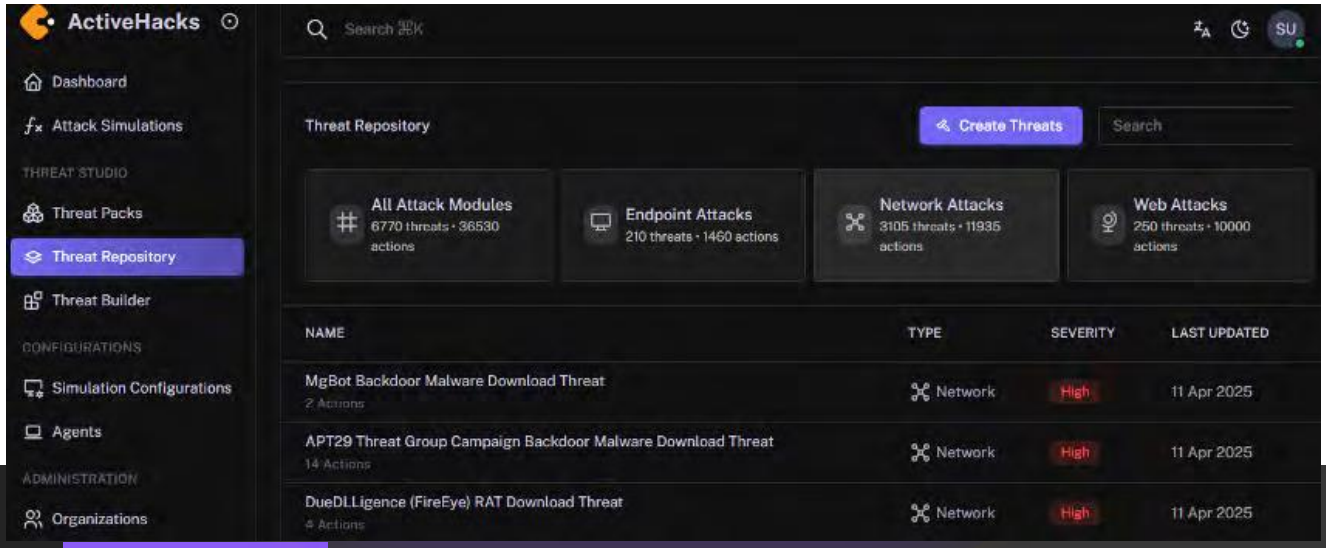
Safely replicates real-world attack paths to validate detections, test segmentation, and strengthen defenses with customizable, MITRE-aligned scenarios.

Network Infiltration Simulation module

The Network Infiltration Simulation Module safely replicates sophisticated, real-world attack paths—enabling you to validate detection controls, verify network segmentation, and reinforce internal defenses with fully customizable, MITRE-aligned threat scenarios.

3000+
Real-world Network Threats

11,000+
Network Simulation Actions



Key Benefits

1. Validates Segmentation Controls
2. Improves Detection & Response Readiness
3. Uncovers Internal Attack Paths
4. Safe Testing in Live Environments
5. Supports MITRE ATT&CK-Based Risk Mapping

Core Capabilities

1. Customizable threat Templates
2. Zero-Impact Execution
3. Encrypted Telemetry
4. Compliance Reporting

activehacks

Endpoint Attack Simulation

Emulates real-world endpoint attacks to test detections, validate EDRs, identify blind spots, and enhance endpoint security.

Endpoint Attack Simulation

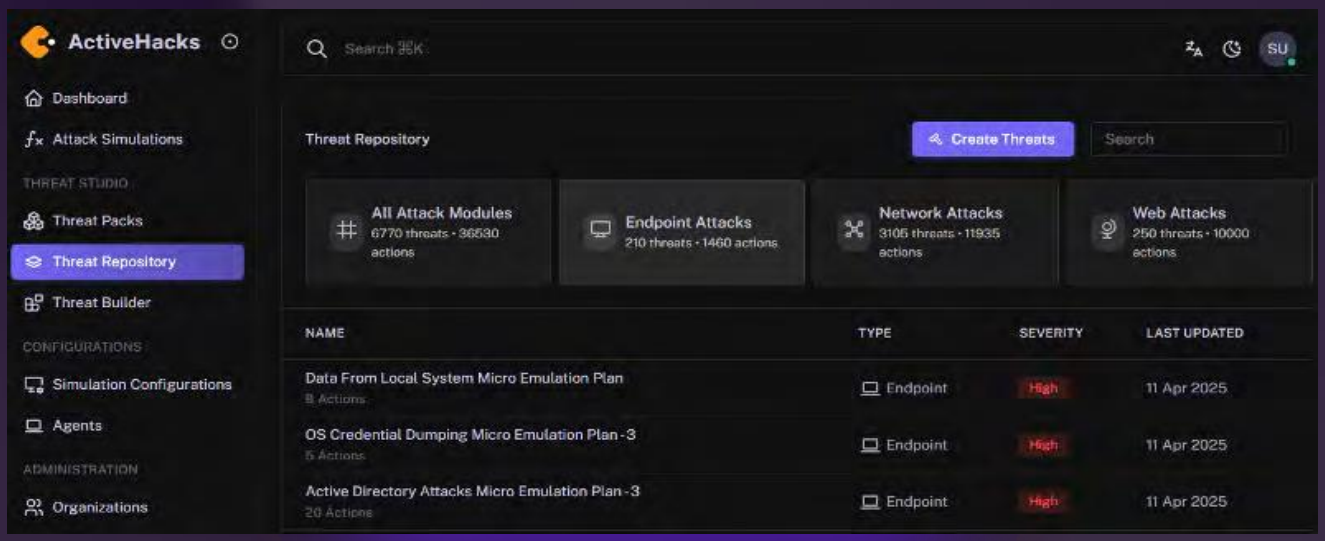
The Network Infiltration Simulation Module safely replicates sophisticated, real-world attack paths—enabling you to validate detection controls, verify network segmentation, and reinforce internal defenses with fully customizable, MITRE-aligned threat scenarios.

200+

Total Endpoint Threats

1400+

Total Endpoint Actions

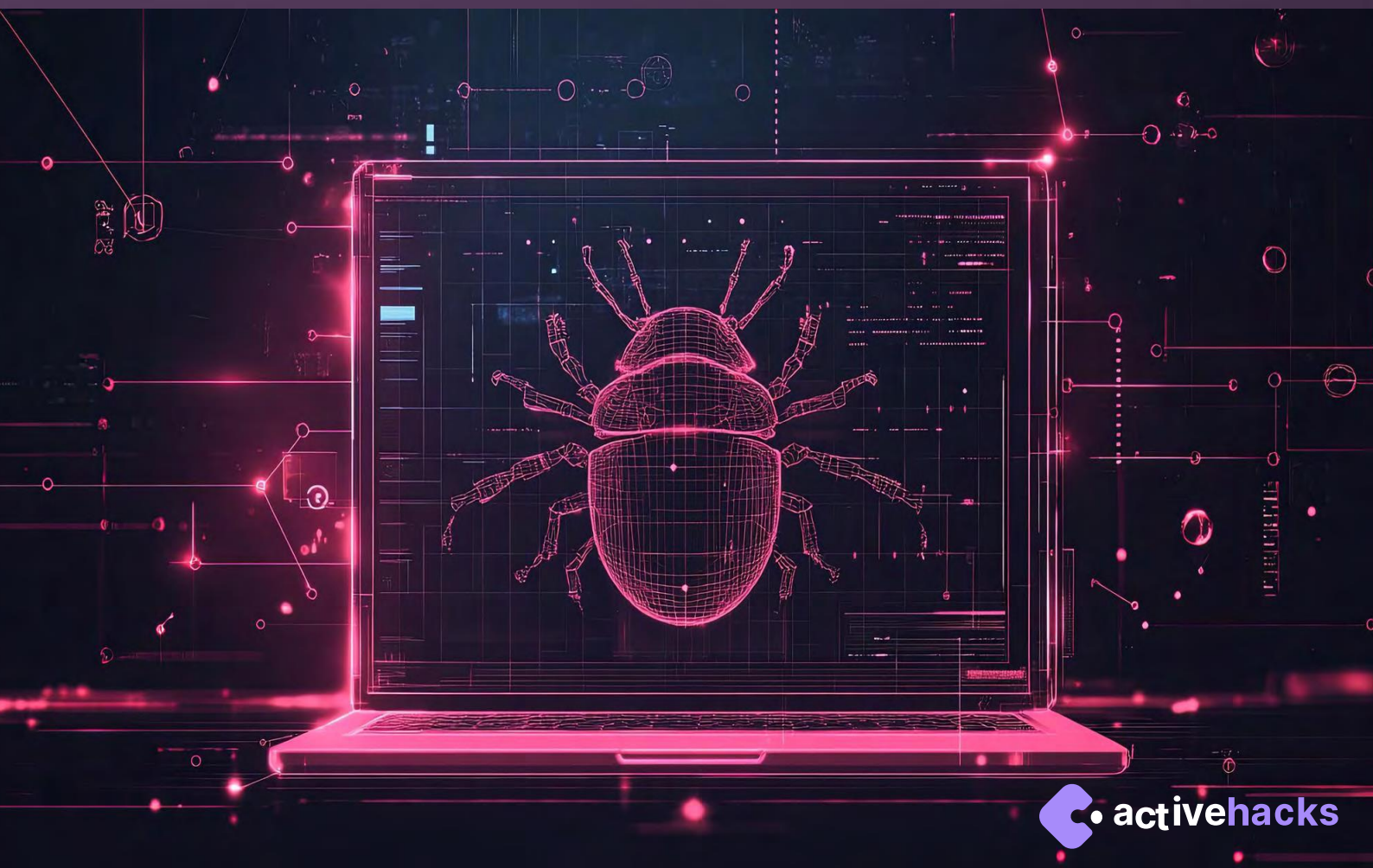


Key Benefits

1. Enhanced Detection Validation:
   Confirms that antivirus and EDR solutions correctly identify and alert on simulated malicious behaviors.
2. Blind-Spot Identification:
   Uncovers unseen vulnerabilities in endpoint configurations, privilege settings, and security policies.
3. EDR Efficacy Assessment:
   Measures the real-world effectiveness of endpoint protection platforms in detecting and blocking threats.
4. Proactive Risk Reduction:
   Enables security teams to remediate endpoint weaknesses before adversaries exploit them.
5. Continuous Posture Improvement:
   Automates recurring tests to track endpoint security enhancements and prove compliance over time.

Core Capabilities

1. Malware Behavior Emulation
2. Command & Control (C2) Behavior Simulation
3. Multi-Platform Support (Supports simulation on Windows, Linux, and macOS endpoints, with OS-specific TTP variations.)
4. EDR/XDR Visibility Mapping



activehacks

Email Attack Simulation

Safely tests your email security by replaying real-world attacks to assess filters, detections, and blocking of malicious links and attachments—no user action required.

Email Attack Simulation

The Email Attack Simulation Module evaluates your email security stack by safely replaying real-world attack vectors—testing filters, detection engines, and blocking controls for malicious links and weaponized attachments, all without user involvement.

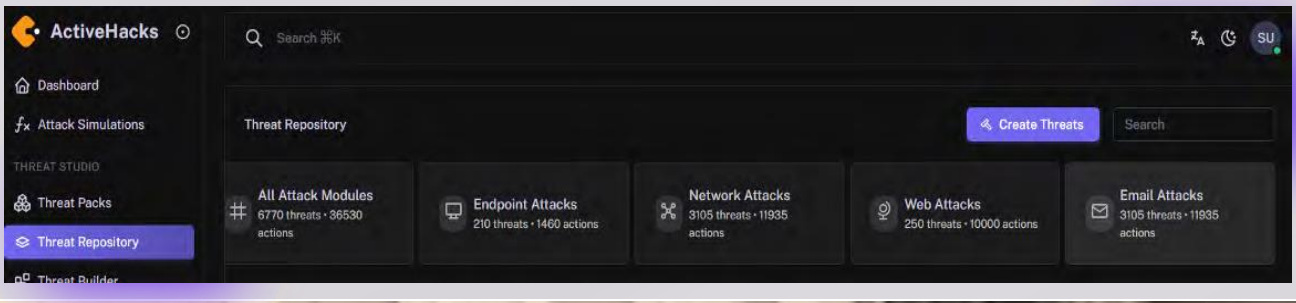
Metric	Value
Total Endpoint Threats	181 threats
Total Endpoint Actions	1294 actions

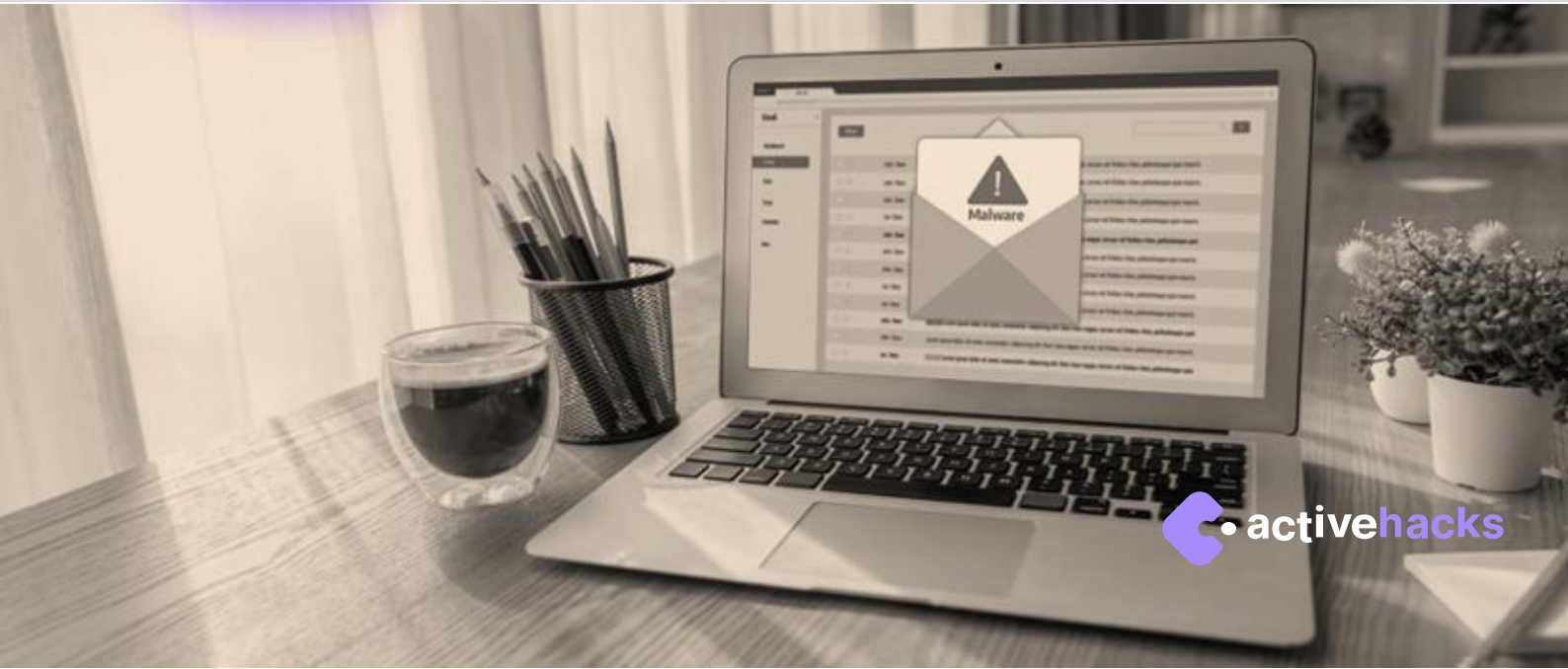
Key Benefits

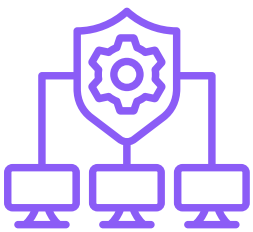
This module enables security teams to proactively identify blind spots in their email threat detection stack—without relying on end-user actions—ensuring that email filtering technologies are effective against evolving malware delivery

Core Capabilities

1. Malicious Attachment Simulations
2. Phishing Link Testing
3. Spoofed Sender & Domain Simulation
4. Delivery & Execution Tracking







Web Application Attack Simulation

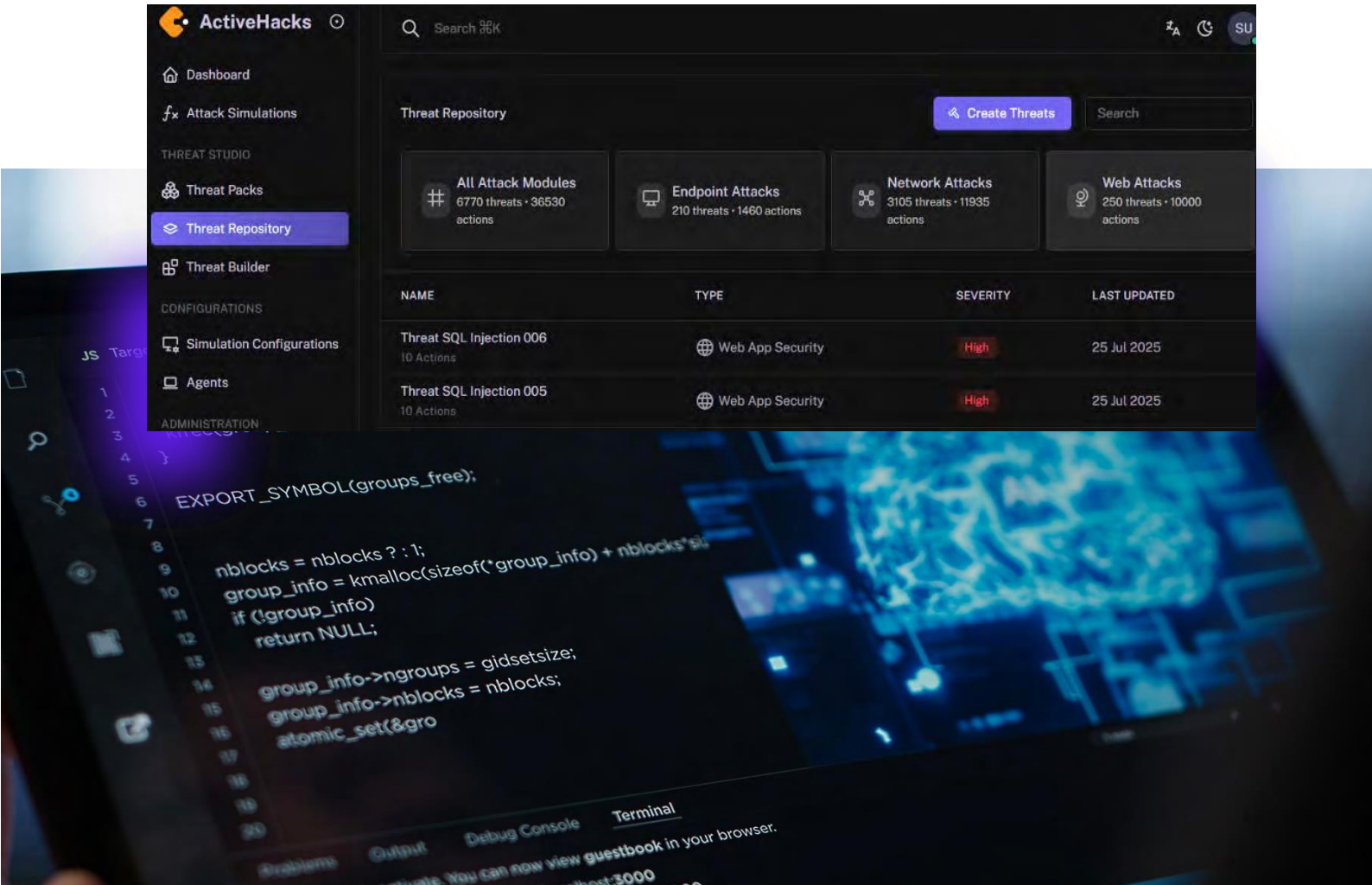
Emulates real-world web attacks to uncover OWASP vulnerabilities, validate detections, and test response workflows—strengthening your app security posture.

Web Application Attack Simulation

The Web Application Attack Simulation Module emulates real-world attacks against web applications—identifying critical OWASP vulnerabilities by replaying malicious payloads, validating detection controls, and testing response workflows to proactively fortify your application security

ActiveHacks covers a wide range of web application attack vectors

SQL Injection (SQLi)	Server-Side Request Forgery (SSRF)
Cross-Site Scripting (XSS)	Open Redirects
Command Injection	Remote Code Execution (RCE)
Path Traversal	File Inclusion (LFI/RFI)
File Upload Exploits	Security Misconfiguration
Cross-Site Request Forgery	Insecure Deserialization
Directory Traversal	

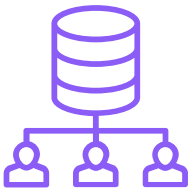


Key Benefits

- Comprehensive Vulnerability Coverage: Identify critical flaws across OWASP Top 10, SANS Top 25 —SQLi, XSS, XXE, and more—before adversaries exploit them.
- Detection Control Validation: Ensure WAFs, IDS/IPS, and SIEM rules correctly flag malicious payloads and anomalous traffic.
- Response Workflow Testing: Verify incident response playbooks and automated mitigation actions trigger as expected.
- Proactive Risk Reduction: Remediate high-risk web application weaknesses to prevent data breaches and compliance gaps.
- Continuous Assurance: Schedule recurring simulations with historical trend reporting to demonstrate ongoing security improvements.

Core Capabilities

- Customizable Attack Scenarios: Drag-and-drop builder with prebuilt payloads for injection, authentication bypass, file inclusion, and logic flaws.
- Zero-Impact Execution: Safe, read-only request replay and payload injection without disrupting production services.
- Real-Time Orchestration & Monitoring: Cloud dashboard coordinates tests, streams live results and visualizes attack paths and control failures.



Active Directory Simulation

Performs advanced, non-intrusive AD assessments to detect vulnerabilities, validate controls, and reveal privilege escalation risks.

Active Directory Attack Simulation

The AD Attack Simulation Module delivers advanced, non-intrusive assessments of your Active Directory environment—empowering organizations to detect vulnerabilities, validate controls, and understand privilege escalation risks from multiple vantage points.

Why AD Attack Simulation Matters

A successful AD compromise can grant attackers domain-wide access, leading to data exfiltration, ransomware deployment, or full network takeover. Simulating AD attacks validates your defenses, ensuring critical identity and access controls are effective against advanced threats.

Core Activities

1. AD Threat Simulation

Simulate a broad spectrum of Active Directory attacks using prebuilt and customizable scenarios mapped to the MITRE ATT&CK® framework. The platform offers flexible scenario creation, enabling you to model real-world adversary tactics, techniques, and procedures (TTPs), and tailor simulations to your organization's unique AD structure. Results include contextualized findings and prioritized remediation guidance—helping teams proactively close security gaps.

- MITRE-Aligned Testing: Assess detection and response capabilities for credential theft, privilege escalation, replication abuse, and more.
- Custom Scenario Design: Easily modify or create new attack chains to suit your unique operational environment or compliance goals.
- Safe, Non-Disruptive Execution: All actions are read-only/API-driven, ensuring zero impact on production data or AD schema.

2. Advanced Path Analysis

Go beyond single attack scenarios with automated path analysis—mapping and visualizing all feasible attack paths from various privileged (and non-privileged) user accounts to high-value targets, such as Domain Admins. The platform identifies each step required for escalation, highlights chokepoints and risky configurations, and offers actionable options to disrupt or remediate these lateral movement paths.

- Privilege Escalation Mapping: Identify and visualize all possible privilege escalation routes to Domain Admins from any user or group in your directory.
- Step-by-Step Path Details: Receive granular breakdowns of each action, abuse point, and misconfiguration an attacker could

Key Benefits

1. Comprehensive Exposure Assessment
2. Actionable Intelligence
3. Continuous Assurance:
4. Zero Impact

Database Attack Simulation

A lightweight, non-intrusive tool that helps identify misconfigurations, privilege escalation paths, and exploitable vulnerabilities in critical databases—before attackers do.

Database Attack Simulation

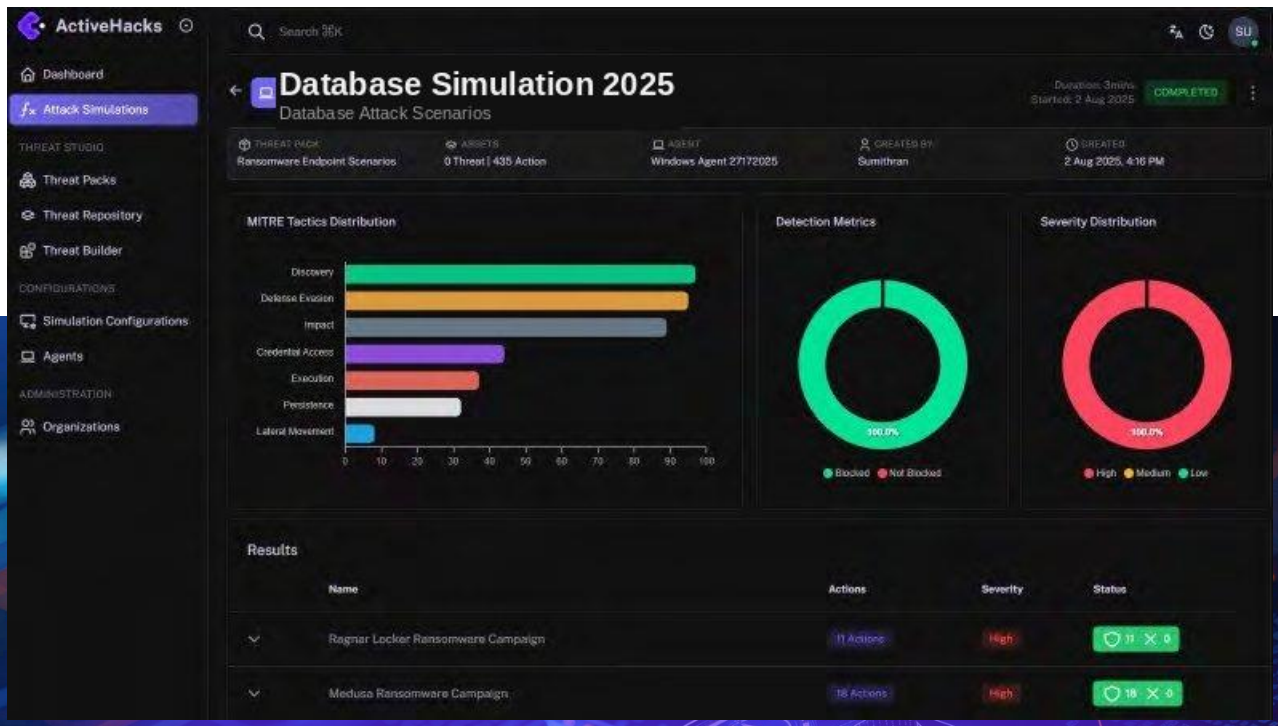
The Database Attack Simulation Module provides targeted, non-intrusive assessments of your organization's critical databases—enabling teams to automatically surface misconfigurations, privilege escalation risks, and exploitable weaknesses that could lead to severe security breaches.

How it Works

1. Choose from prebuilt threat packs
2. Safe, Read-Only Testing
3. Real-Time Monitoring
4. Security Stack Validation
5. Actionable Reporting

Key Benefits

1. Critical Weakness Discovery
2. Actionable Remediation Steps
3. Continuous Improvement
4. Zero Disruption



activehacks

Notice

This document contains information about the proprietary property of Analyzet Innovations. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Analyzet.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. Analyzet disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of Analyzet; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed herein and is advised to seek the advice of competent legal counsel, without obligation of Analyzet.

Analyzet retains the right to make changes to this document at any time, without notice. Analyzet makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owner’s benefit, without any intent to infringe.

Contact Us

Analyzet

Dubai Silicon Oasis, Dubai, United Arab Emirates +971 50 513 3973
analyzet.com