CATCHPROBE™

Empowering The Pursuit of Intelligence

OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE™

CatchProbe is an all-in-one cyber intelligence suite that unifies five AI-driven modules to deliver comprehensive cybersecurity solutions.

Our platform seamlessly integrates web intelligence, threat detection, deception technology, and attack surface management modules – both with each other and to customers' existing security infrastructure – enhancing visibility and delivering actionable intelligence.

OTD BİLİŞİM
GLOBAL VAD

WHY CYBER INTELLIGENCE

Problem

Statistics predict that cybercrime will cost the global economy more than 20 trillion U.S dollars by 2026, a 1.5 times increase compared to figures in 2022 (Source: Statista). Conventional cybersecurity measures often react to threats rather than prevent them, leaving organizations vulnerable. To stay ahead of evolving threats, organizations require advanced threat intelligence that enables them to anticipate and mitigate attacks before they occur.

Solution

We've created a platform to align with the strategic needs and operational demands of national security agencies and the private sector. Each with its own specialized purpose that enhances the capabilities of others, CatchProbe equips businesses with extensive intelligence gathering and preemptive defense strategies.

CATCHPROBE™

WHY CATCHPROBE

Unified Cyber Intelligence:

Integrates deception, dark web intelligence, and attack surface management in one Al-powered platform.

Proactive vs. Reactive Security:

Stops threats before they become incidents, reducing breach response time by over 80%.

Seamless Ecosystem Integration:

Works with firewalls, SIEMs, and SOAR platforms to automate threat mitigation.

Proven Impact:

Trusted by government agencies, private organizations in various sectors, and financial institutions.

Future-Ready:

CatchProbe modules work together, enabling real-time intelligence sharing, automatic remediation, and seamless API integrations with security ecosystems.

OTD BİLİŞİM
GLOBAL VAD

CATCHPROBE™

CATCHPROBE ALL-IN-ONE DIGITAL INTELLIGENCE SUITE

DARKMAP	LEAKMAP	SMARTDECEPTIVE	THREATWAY	RISKROUTE	VENSPECT
					
WEBINT, BRAND PROTECTION	OSINT, CORRELATED LEAKS	DECOY (HONEYPOT) MANAGEMENT	THREAT INTEL SHARING HUB	EXTERNAL ATTACK SURFACE MANAGEMENT	VENDOR RISK ASSESSMENT

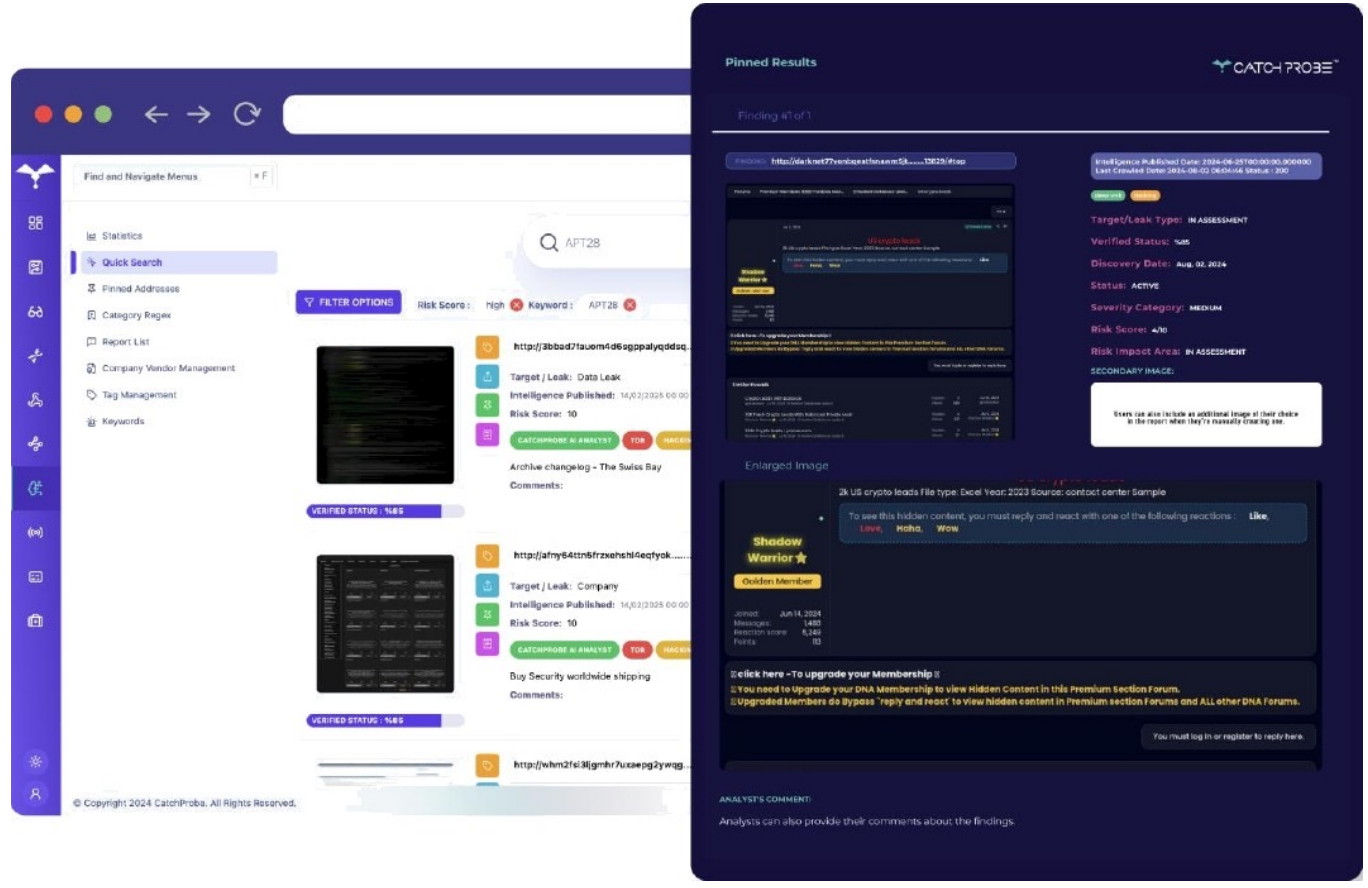
Competitors focus on reactive solutions, responding only after an attack occur.

CatchProbe is built for proactive cyber defense.

OTD BİLİŞİM
GLOBAL VAD

DARKMAP: REDEFINING WEB INTELLIGENCE WITH AI

- Monitors underground forums, marketplaces, and hidden networks.
- Alerts organizations about compromised credentials, leaked financial data, and confidential documents.
- Provides real-time AI-driven threat assessment.
- Automatically translates resources to English, enabling insights across language barriers.
- Allows limitless tracking of vendors to monitor vulnerabilities, without any restrictions tied to license limits.
- Users can configure automated email alerts in PDF format for new findings, specifying when, how (e.g., based on risk score), and who should receive them.
- Automatically acquires leaked data within the pre-set budget allocated by CatchProbe.

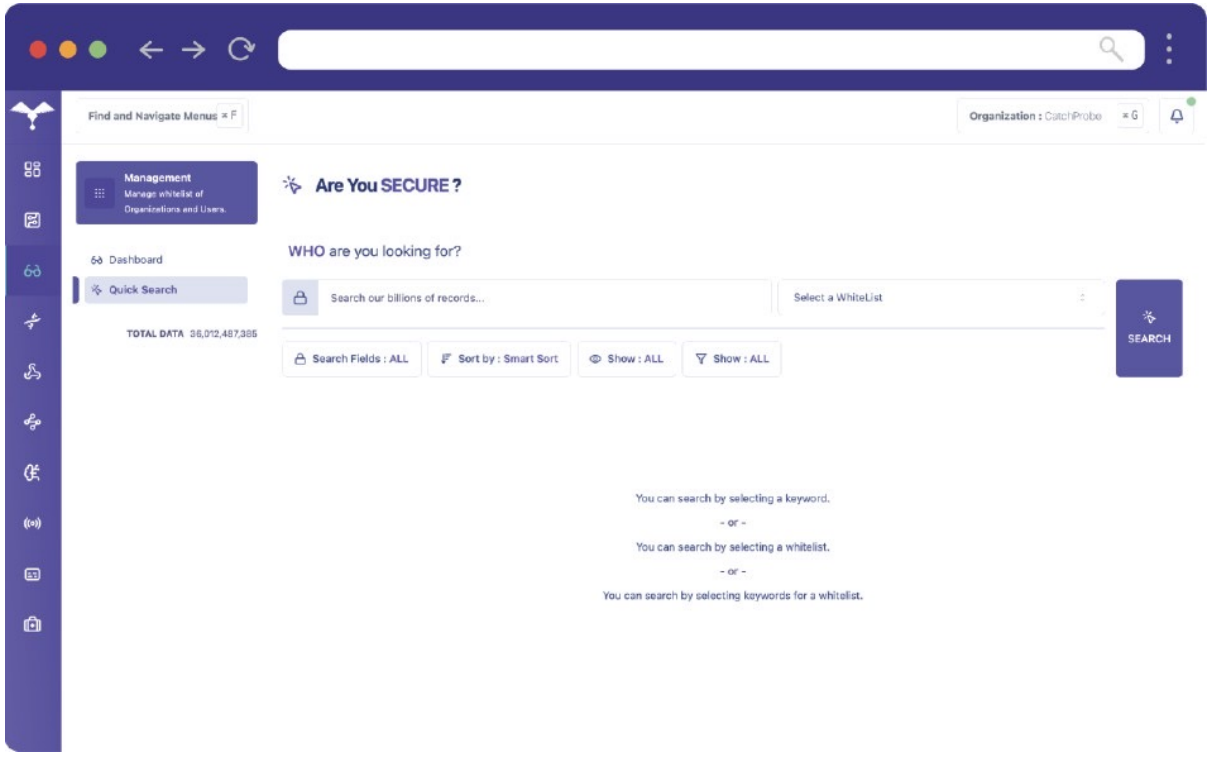


WHY DARKMAP STANDS OUT

- Over 9 Petabytes of ready-to-analyze datasets
- Access to critical internet pages from the last 20 years
- Real-time & hot scans across dark and deep web platforms
- Historical/cold scans for retrospective intelligence
- Coverage of all major dark web infrastructures:
- Yggdrasil, Tor, ZeroNet, 12P, Forums and Messengers
- Instant cloning and downloading of identified sites in seconds
- Regex-based deep search across all collected data
- Keyword-based monitoring: supports IPs, domains, names, etc.
- Keyword permutations & combinations generation
- Alerts based on emerging keywords
- Vulnerability scanning across all digital assets
- Live monitoring of hacker groups and underground activities
- 83 language sources
- Auto-download capability for relevant content
- Predictive intelligence features powered by AI
- AI-based risk analysis with big data correlation
- Cross-platform identity matching (e.g., Telegram avatar & forum alias)
- Monitoring of:
- Telegram & WhatsApp groups
- Encrypted ICQ & IRC chats, prioritized by criticality
- Anonymous access to all darknet and deepnet platforms
- Operator behavior tracking for advanced threat attribution
- Reduce CAPEX to zero, cut OPEX by up to 50%
- Detection & alerts for:
- Live access sales (bank accounts, phone tapping, etc.)

LEAKMAP: MANAGING DATA BREACHES WITH PRECISION

CatchProbe LeakMAP is the largest, continuously expanding database for identifying and analyzing leaked data.



- Maps and analyzes over 1 petabyte of leaked data across dark web sources.
- Automatically validates leaked credentials, filtering out inactive or false entries.
- Alerts organizations to emerging breaches, credential leaks, and financial data exposure.
- Integrates with SmartDECEPTIVE to detect attackers attempting to exploit leaked data.

Current Total Data: + 36 Billion.

CATCHPROBE™

WHY LEAKMAP STANDS OUT

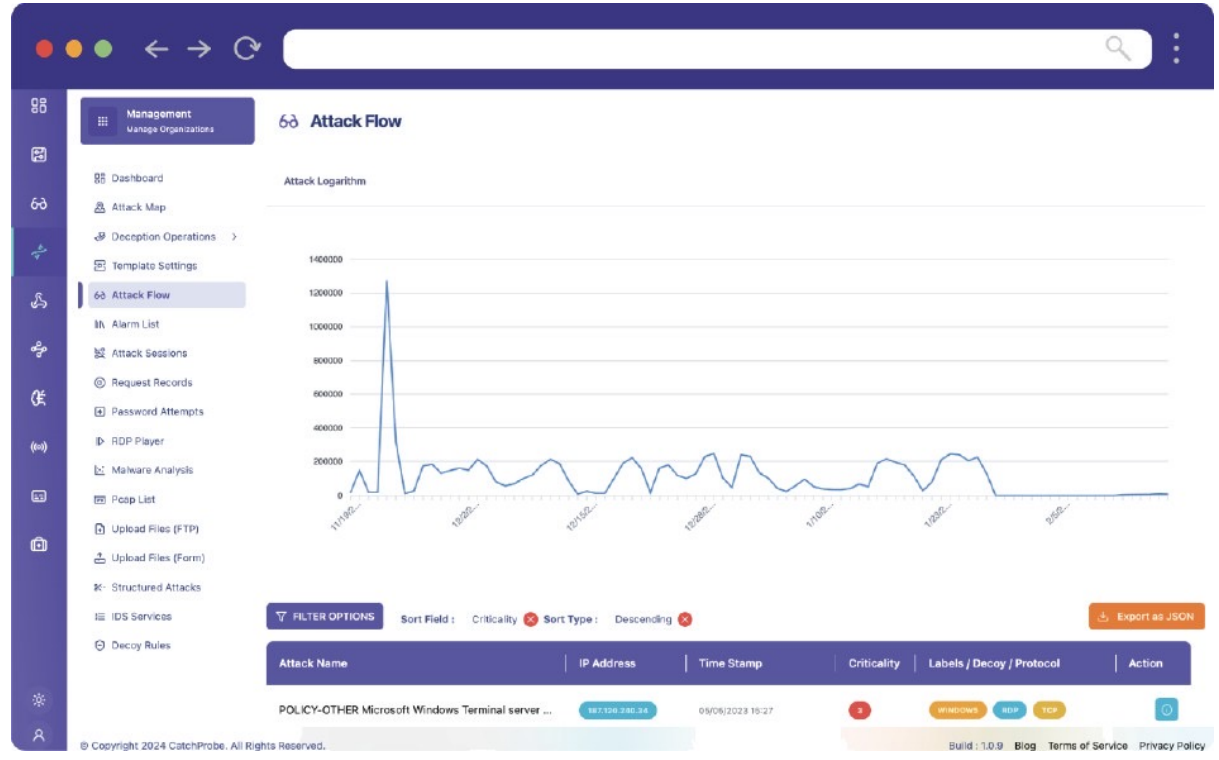
- Comprehensive Breach Analysis across global datasets
- LDAP Integration and Active Directory Security insights
- Enterprise-Based Labeling to classify and prioritize findings
- Access to all leaked databases of the past 20 years worldwide
- Ingestion and analysis of malware logs
- Ability to download malware files for investigation
- Detection of unpublished (yet-to-surface) malware threats
- AI-powered interpretation of all collected data
- Identify employees most vulnerable to targeted attacks
- Use of regex-based correlation across different data types
- Enables advanced data discovery and analysis

OTD BİLİŞİM
GLOBAL VAD

SMARTDECEPTIVE: KEEPING ATTACKERS IN THE DARK

SmartDECEPTIVE transforms traditional honeypots with Al-driven, highly customized decoys that lure attackers.

- Unlike static honeypots, CatchProbe decoys actively analyze attacker behavior in real-time.
- With firewall and SIEM integration, SmartDECEPTIVE ensures that threats are stopped at the perimeter before they reach core systems.
- Additionally, it performs instant malware analysis And cross-references attacker 1oCs with open-source intelligence for deeper insights.
- Integrates with LeakMAP to detect targeted attacks, identifying any attempts to exploit leaked data for malicious purposes.
- With full packet capture (PCAP) capability and Mitre Att&ck integration enables in-depth understanding of attacker behavior.
- This isn't just detection—it's proactive blocking, creating a digital minefield that attackers can't navigate.



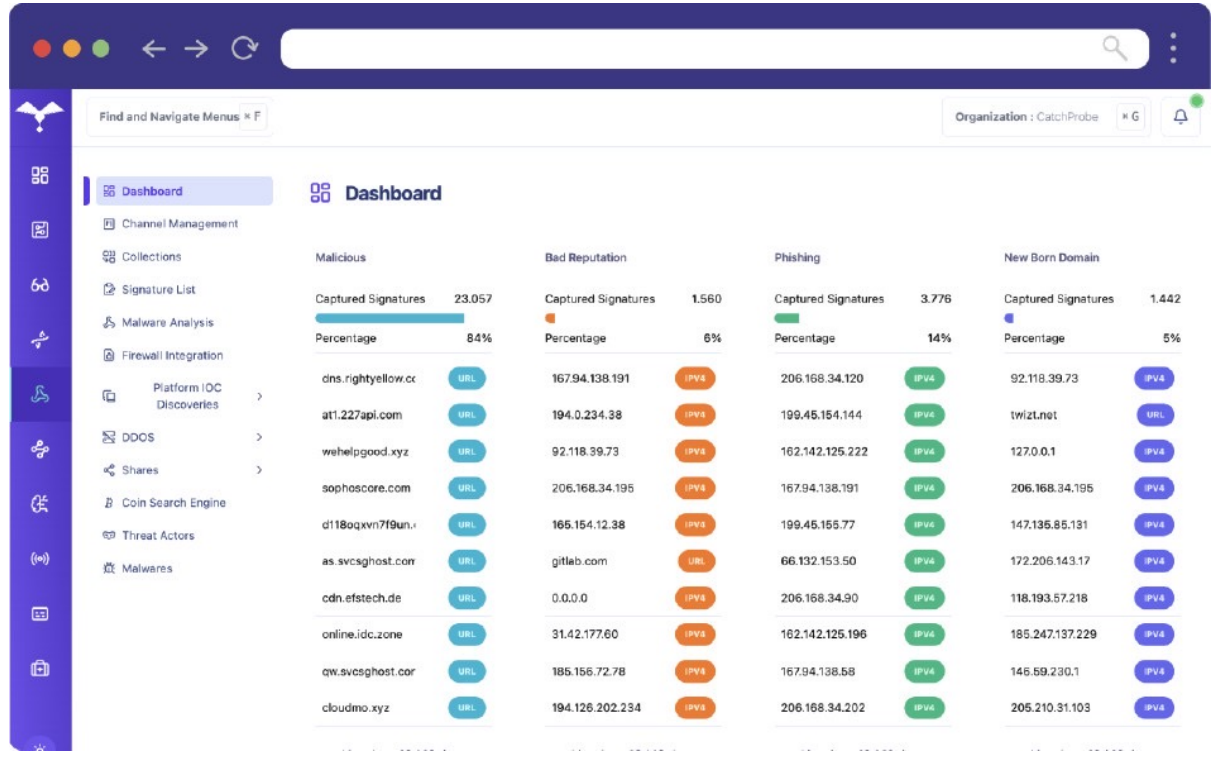
CATCHPROBE™

WHY SMARTDECEPTIVE STANDS OUT

- AI-powered attacker profiling and behavior prediction
- Real-time attack analysis across all decoys
- Instantly deploy hundreds of undetectable decoys within minutes
- Create deception environments on any platform:
- Linux, Windows, SCADA, Android, Kiosk, etc.
- Fully customizable by port and service
- Extensive library of pre-built attack scenario templates
- Run full attack flow (including malware analysis) in seconds:
- No license uploads or manual downloads required
- Automatic PCAP analysis from decoys
- RDP session monitoring capability
- Identify the same attacker across multiple IPs, correlate via AI
- Enable competitive/peer analysis based on attack signatures
- Custom SSL integration for deception environments
- Reverse proxy support for advanced engagement
- Optional on-prem deployment for energy sector infrastructure
- Create unlimited IDS instances, with custom rule sets per IDS
- Reduce CAPEX to zero, lower OPEX by up to 50%
- Flexible response: Auto-contain or alert-only modes

THREATWAY: REAL-TIME CTI THAT FITS SEAMLESSLY INTO YOUR ECOSYSTEM

- Critical Threats First: Focus Protection Where It Matters Most. ThreatWAY analyzes and prioritizes threats, ensuring that your organization is focused on the most critical risks.
- Allows you to share refined intelligence across your intra- and inter-organizational channels in milliseconds.
- Delivers Indicators of Compromise (IoCs) directly to your firewalls, SIEMs, and SOAR.



ThreatWAY offers seamless integration of over 200 platforms through API, alongside DarkMAP's advanced crawling operations and SmartDECEPTIVE's decoys and exposed attacks, while also allowing you to easily add or remove customized data sources to ensure only the most relevant intelligence is available for your specific needs in real-time.

CATCHPROBE™

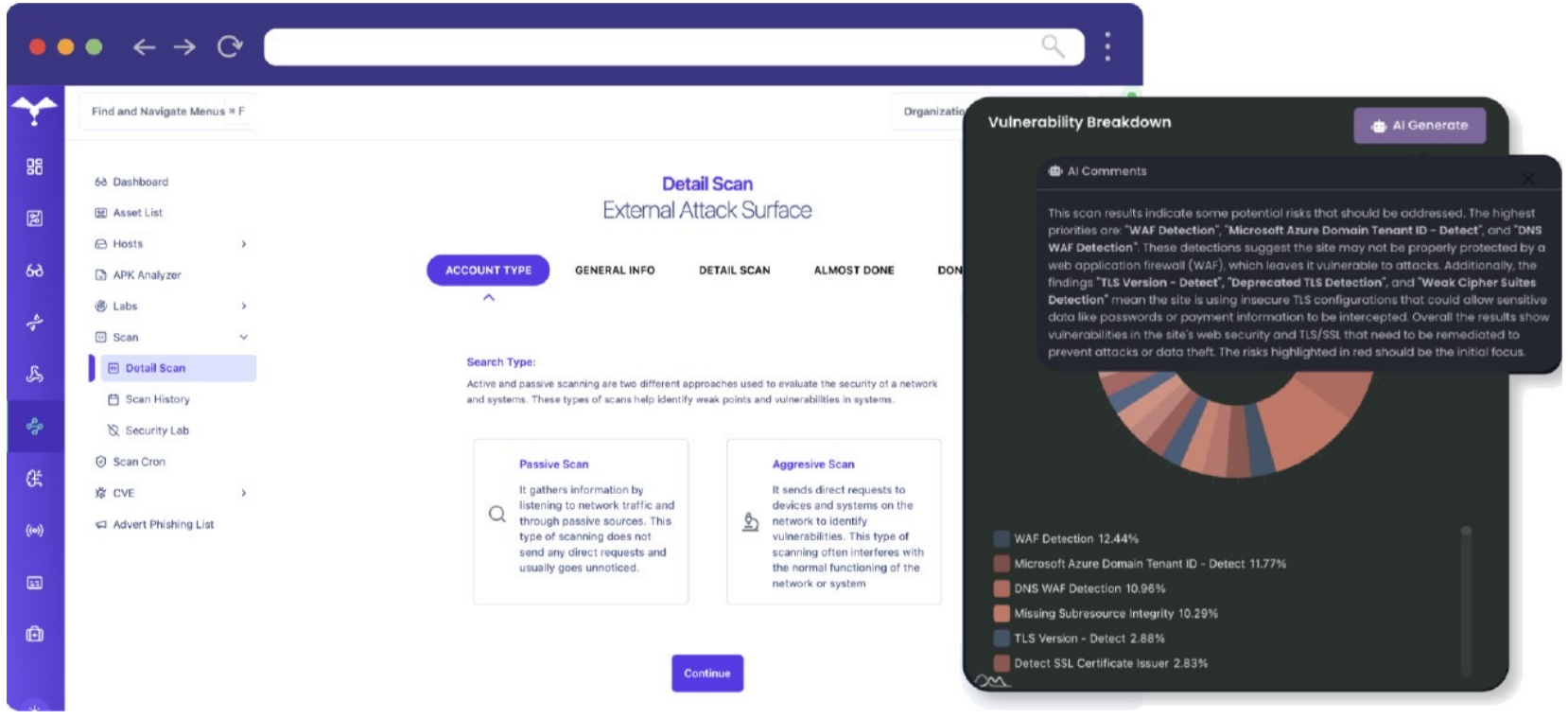
WHY THREATWAY STANDS OUT

- RDP session monitoring capability
- Identify the same attacker across multiple IPs, correlate via Al
- Enable competitive/peer analysis based on attack signatures
- Custom SSL integration for deception environments
- Reverse proxy support for advanced engagement
- Optional on-prem deployment for energy sector infrastructure
- Create unlimited IDS instances, with custom rule sets per IDS
- Reduce CAPEX to zero, lower OPEX by up to 50%
- Flexible response: Auto-contain or alert-only modes
- Information leakage detection
- Social engineering indicators

- Build your own CERT & CSIRT infrastructure in minutes
- Create custom intelligence sharing channels
- Invite other organizations into your threat sharing network
- Push intel or alerts to partners or internal security tools
- Access to 10+ years of scored and enriched dirty IP datasets
- Covers billions of entries across 20+ data types
- Intelligence includes:
- DNS health insights
- Patching status analysis
- Application security assessments

RISKROUTE: COMPREHENSIVE ATTACK SURFACE MANAGEMENT

CatchProbe RiskRoute empowers security teams to monitor, manage, and secure critical systems, identify vulnerabilities, track asset health to reduce the risk of data breaches and cyber attacks.



Provides AI-powered risk analysis with tailored remediation recommendations.

Integrated alerting through Jira, Webhook, and email for efficient incident response.

CATCHPROBE™

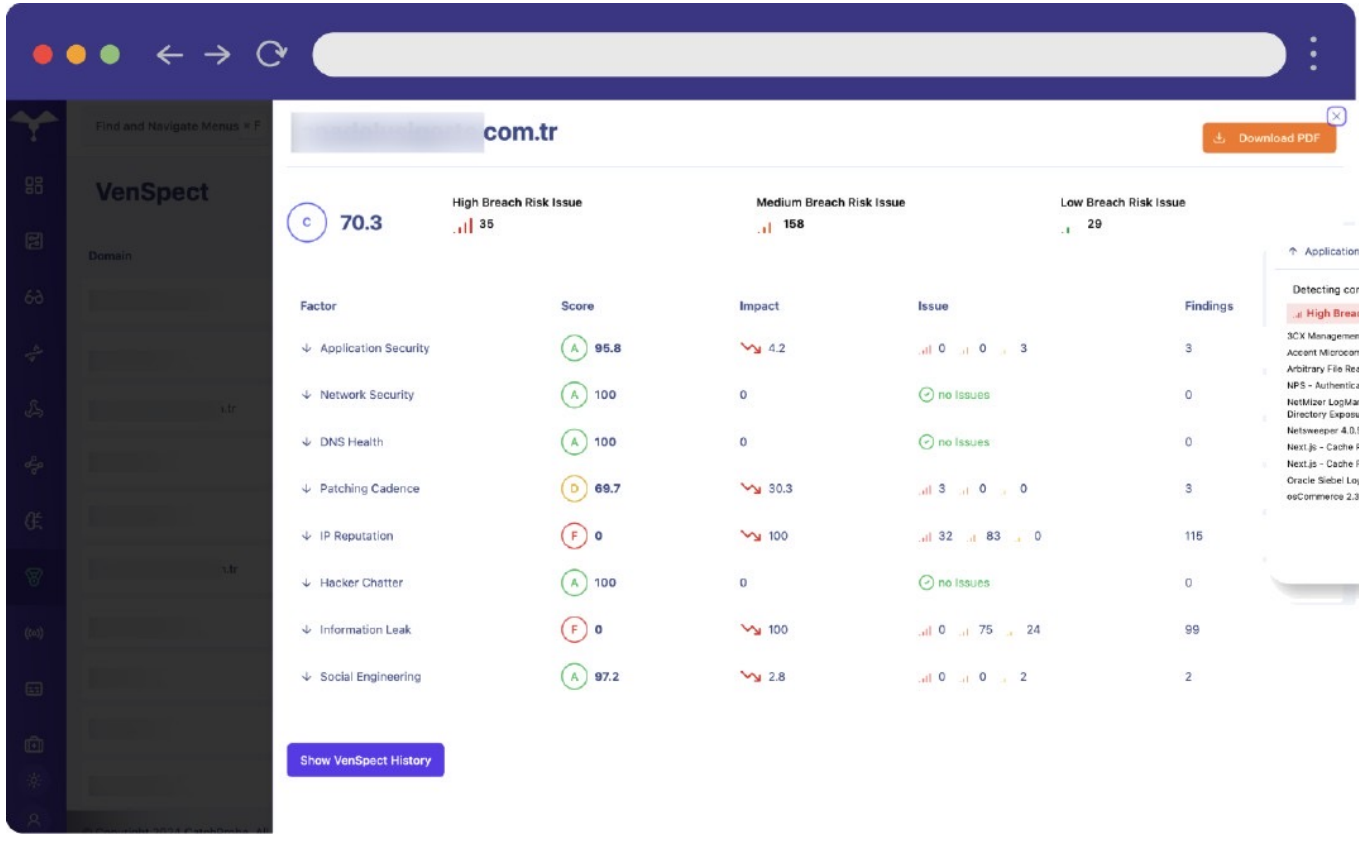
WHY THREATWAY STANDS OUT

- Vulnerability assessment across internal and external assets
- Comprehensive security services for digital infrastructure
- Application security testing and code-level analysis
- Cloud environment security testing
- Cyber-asset Attack Surface Management (CAASM)
- Integrated Digital Risk Protection Services (DRPS)
- Passive DNS scanning for stealthy footprint detection
- Scam detection across digital platforms
- Social media-based scammer analysis
- Ad image-to-text extraction for fraud pattern detection
- Social media account discovery linked to digital threats
- Detect and map Shadow IT within your organization

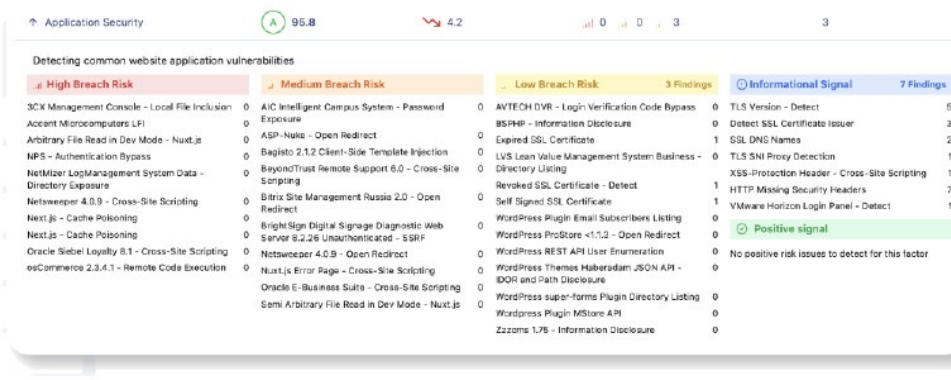
OTD BİLİŞİM
GLOBAL VAD

VENSPECT: THIRD PARTY RISK ASSESSMENT

This one is for monitoring the security posture of your third-party vendors and services. With automated monthly assessments and overtime scoring, VenSPECT helps you stay ahead of external risks and help you make informed decisions without the manual overhead.



- You can trigger assessments manually when a needed, track historical performance, and com.r wj quickly identify risk-carrying partners.



- Download a detailed vendor report with scores, insignts, and risks—perfect for sharing, audits, or due diligence wiLn one click.

CATCHPROBE™

WHY VENSPECT STANDS OUT

- Centralized intelligence orchestration: Combines insights from web, dark web, deception, CTI, and ASM modules
- Correlates data from DarkMAP, LeakMAP, SmartDECEPTIVE, RiskRoute, and ThreatWAY into one unified view
- Enables cross-module pattern detection, exposing links between leaked data, infrastructure weaknesses, and active threat actors
- Delivers prioritized, risk-scored findings with context to accelerate decision-making
- AI-powered engine that supports:
- Entity resolution (e.g., same actor across Telegram, forum, email, etc.)
- Attack chain reconstruction
- Behavioral analysis across multiple attack vectors
- Supports customizable dashboards, filters, and alerts for streamlined analyst workflows
- Ideal for SOC teams, threat hunters, and executive reporting

CATCHPROBE™

CATCHPROBE ALL-IN-ONE DIGITAL INTELLIGENCE SUITE

- **Correlated Leak Detection**

  Identifies compromised credentials across multiple platforms, linking leaks from various sources to prevent credential stuffing attacks.

- **Deep Scraping for Actionable Intelligence:**

  Uses Al-driven scrapers to analyze dark web marketplaces, forums, and hidden networks, providing verified intelligence with risk scores and classifications.

- **Decoy Management:**

  SmartDECEPTIVE deploys realistic decoys to lure attackers, enabling organizations to gather intelligence while ensuring minimal risk to their real infrastructure.

- **Structured Attack Detection:**

  Detects targeted attacks on decoys using leaked credentials, integrating with ThreatWAY for automated incident response.

- **Seamless Integration & Automation:**

  CatchProbe modules work together, enabling real-time intelligence sharing, automatic remediation, and seamless API integrations with security ecosystems.

OTD BİLİŞİM
GLOBAL VAD