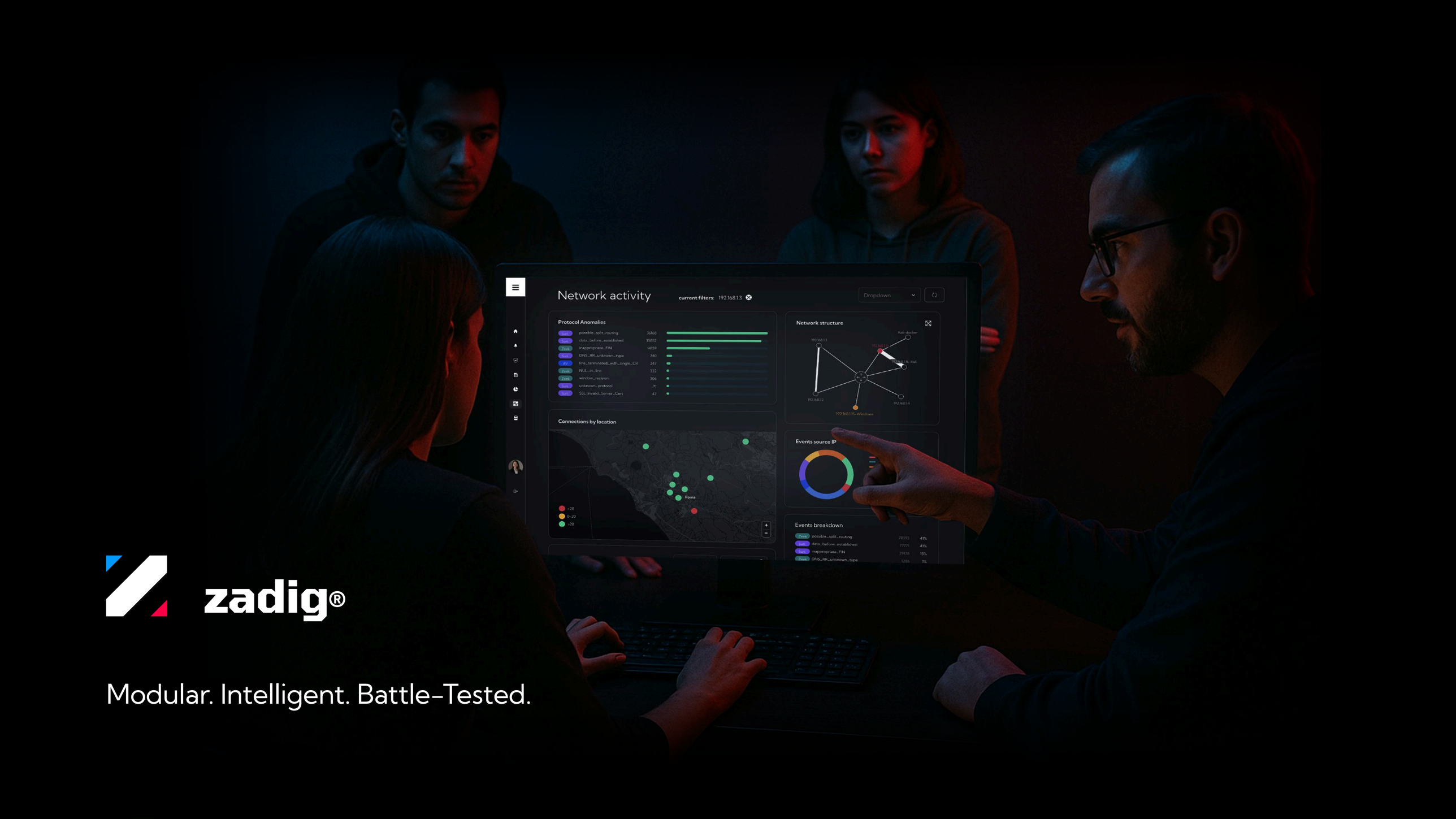


zadig®

Modular. Intelligent. Battle-Tested.

The Next-Gen Cybersecurity & Operational Intelligence Platform

Pioneering Deductive Cybersecurity — Inspired by Voltaire's First Detective

Beyond traditional XDR: Adaptive AI, Seamless Sensor Integration & Open-Source Transparency for True Technological Sovereignty

zadig® is an advanced Extended Detection and Response (XDR) platform developed by bitCorp. Featuring a modular architecture and proprietary AI models, it enables tailored security across diverse enterprise infrastructures. zadig® integrates capabilities typical of EDR, SIEM, NDR, IDS/IPS, and SOAR into a cohesive system with multi-layered protection, log aggregation, threat intelligence, and remediation automation.

The right module, for the right task.

zadig® XDR for mid and large enterprises

Module	Definition
ITD	Intelligent Threat Detector
EDR	Endpoint Detection & Response
NDR	Network Detection & Response
SIEM	Security Information and Event Management

zadig® SMART for micro and small enterprises

Module	Definition
M-IDPS	Modern Intrusion Detection Prevention System

zadig® Gateway	Hardware Support
zadig® Cloud	in Cloud Protection

zadig® ITD

Intelligent Threat Detector

Function: Behavioral and anomaly-based detection powered by self-learning ML models.

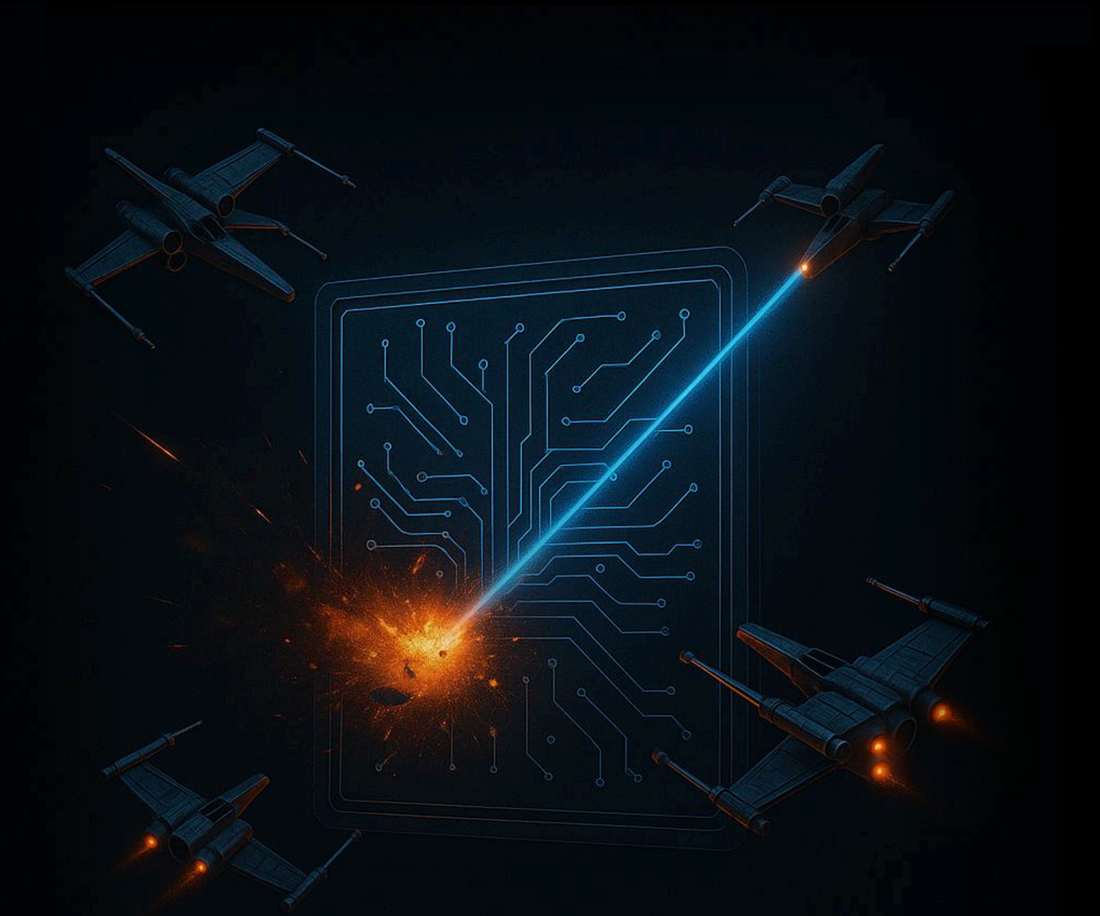
Features:

- AI anomaly detection using proprietary models.
- Continuous monitoring with low false positives.
- Custom model training using client data.
- Scalable performance across environments.
- Tailored model designed to detect threats unique to the customer's business environment

Use Case: Serves as the core for threat modeling and predictive defense.

zadig® NDR

Network Detection & Response



Function: Passive probe-based analysis of real-time network traffic.

Features:

- Coverage of both standard and proprietary/OT protocols.
- Deep network visibility and control through real-time traffic inspection and behavioral analytics.
- Integration with EDR and ITD for layered response.
- Post-event forensic analysis via replayable traffic logs.

Use Case: Ideal for environments with unmanaged devices or complex OT layers.

zadig® EDR

Endpoint Detection & Response

Function: Monitors and protects endpoints (Windows, macOS, Linux, iOS, Android).

Features:

- Agent-based continuous monitoring.
- Cross-platform support via modular architecture.
- Logs file access, process execution, registry changes.
- Integration with ITD and SOAR for real-time correlation and remediation.
- Supports persistent and non-persistent deployments.

Use Case: First-line defense for endpoints and lateral threat movement detection.

zadig® SIEM

Security Information and Event Management

Function: Aggregates and correlates logs across all infrastructure components.

Features:

- Integration with third-party SIEMs and native functions.
- Rule-based and ML-based event correlation.
- Log parsing, BI dashboards, MITRE ATT&CK framework alignment.
- Hot-warm-cold retention policies with Opensearch/Elasticsearch/Azure support.

Use Case: Central analysis point for threat intelligence and SOC operations.

zadig® M-IDPS

Modern Intrusion Detection Prevention System

Function: Deployable IDS/IPS for remote/branch offices and SMEs.

Features:

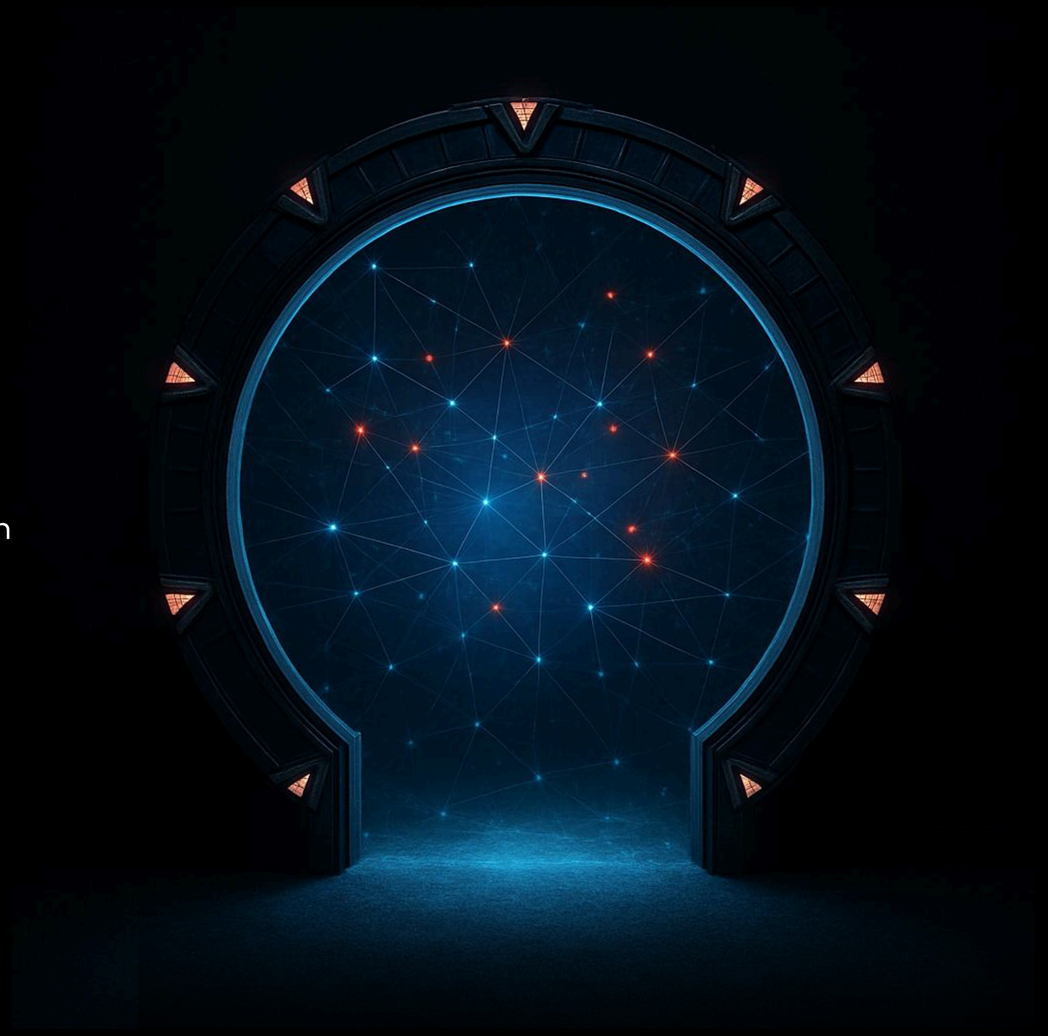
- Plug-and-play hardware/software stack.
- Zero-knowledge install, AI heuristics, and attack isolation.
- VPN, firewall, DNS/AD-block, and anti-ransomware features.

Use Case: Enables small offices to harden perimeters and comply with ISO 27001, NIS2, AgID.

zadig® M-IDPS

Hardware Support Gateway

zadig® Gateway is the one and only edge device needed to protect physical workplaces. It perfectly fits organizations operating from many sites even with lightweight or temporary Infrastructure.



zadig® M-IDPS

Cloud Protection

zadig® Cloud is the innovative SaaS only subscription for enterprise security management that integrates a bundle of cloud services for identity and access management through an advanced, out-of-the-box users and devices directory without the need for any IT expertise.

zadig® SMART

Modern Intrusion Detection Prevention System

bitCorp® has introduced an innovative solution that delivers Intrusion Detection and Prevention System (IDPS) capabilities to organizations that have historically lacked access to such tools due to budget limitations or limited in-house IT expertise.

Recognizing the opportunities presented by the proliferation of Modern Workplaces, bitCorp® has developed the first Modern IDPS (M-IDPS)—a comprehensive platform that provides advanced threat protection. This solution is designed to bridge the cybersecurity gap for companies that have traditionally relied solely on basic antivirus software.

Next-Gen Features

SOAR – Security Orchestration, Automation, and Response

Function: Case and incident management, response playbooks, and automated remediation.

Features:

- Automated triage (phishing, alerts, manual input).
- Remediation playbooks: isolate hosts, disable users, block indicators.
- Metrics (MTTD, MTTR), PDF incident reporting (AAR).
- TI enrichment from multiple providers.

Use Case: Streamlines SOC operations with guided incident lifecycle management.

TEP – Transport Encrypted Protocol

Patent-backed blockchain-based protocol.

Functions:

- Mesh network defense with cold/warm communication modes.
- Federated intelligence exchange between installations.
- Immune to DDoS, MITM, and spoofing attacks.

Use Case: Cyber-resilient infrastructure for defense, utilities, smart grids.

Deployment & Integration

Data ingestion pipeline support
Syslog, Filebeat, Kafka, Windows Event Collector, NetFlow, DB, CSV, FTP.

Storage Backend Support
Elasticsearch, AWS OpenSearch, Azure Log Analytics.

Management UI
Role-based (Admin, Editor, Viewer) with SSO and MFA (OAuth2, SAML).

APIs
Full automation support via RESTful interfaces.

Dashboards
Customizable visual panels, alert priority, MITRE tagging.

Differentiators

1

AI models trained on client infrastructure (no data exfiltration)

2

Behavioral-based detection engine with domain-specific learning

3

High compliance readiness (ISO 27001, NIS2)

4

Efficient for both cloud-native and hybrid deployments

5

Fully European-built, sovereign tech with NATO/ SAM GOV approval

Product Tiers

Product	Target	Description
zadig® XDR	Medium & large orgs	Full-featured XDR suite
zadig® SMART	SMEs, remote offices	Turnkey all-in-one appliance w/ firewall, backup, VPN
zadig® CLOUD	Cloud-first environments	Lightweight agentless security, identity & access control
zadig® GATEWAY	Branch sites	AI-enhanced NGFW with IDPS and AD-blocking

Competitive analysis

Feature / Vendor	bitCorp zadig® XDR	CrowdStrike Falcon XDR	Palo Alto Cortex XDR	Microsoft Defender XDR	SentinelOne Singularity XDR	Trend Micro Vision One	Trellix XDR	Fortinet FortiXDR
Approach	Modular, AI-trained per-client	Threat graph & cloud intel	Unified data model	M365 ecosystem + correlation	Autonomous AI agent	Cross-domain correlated XDR	Threat intelligence & adaptive XDR	Fabric-integrated detection + SOAR
AI / ML	Local, per-client training	Global ML + intel graph	Behavioral ML	ML + heuristics	Behavioral + static ML	AI for email, endpoint, server, etc.	Adaptive threat detection	FortiAI + signature & anomaly models
Custom AI Models	✅ Yes (environment-specific)	❌ No	⚠️ Partial tuning	❌ No	⚠️ Limited tuning	❌ Global models only	✅ Some tuning via Helix	⚠️ Limited – more signature-based
SOAR Integration	✅ Native SOAR + full playbooks	⚠️ Fusion optional	✅ XSOAR native	⚠️ via Microsoft Sentinel	✅ Native automation	⚠️ Optional SOAR via Apex Central	✅ Native Helix SOAR	✅ FortiSOAR optional
Data Ingestion Sources	Broad: Syslog, FTP, DB, NetFlow, Kafka	Falcon agent + connectors	Broad, especially PAN firewalls	Medium (M365, Azure)	Via agent & Ranger	Broad, supports many 3rd parties	Broad (SIEMs, endpoints, cloud)	Fortinet ecosystem + select others
IoT / OT Support	✅ Smart buildings, OT/ IoT devices	❌ Weak	⚠️ Requires integrations	⚠️ Some Defender for IoT	❌ Minimal	⚠️ Limited	✅ Partial via integrations	✅ Native OT support via FortiSwitch

Competitive analysis

Feature / Vendor	bitCorp zadig® XDR	CrowdStrike Falcon XDR	Palo Alto Cortex XDR	Microsoft Defender XDR	SentinelOne Singularity XDR	Trend Micro Vision One	Trellix XDR	Fortinet FortiXDR
EDR Agent Capabilities	Modular, persistent/ non-persistent	Real-time telemetry agent	Deep OS telemetry	Integrated in Windows	Autonomous rollback/ self-healing	Cross-platform agent	Via Trellix Agent	FortiClient EDR
Management Interface	Web UI + RBAC, SSO, MFA	Unified Falcon Console	Cortex console	Microsoft Security Center	Singularity console	Vision One dashboard	Helix platform	FortiAnalyzer/ FortiView
Response Automation	Alerts → isolation, disable users, block IP	Isolation, kill process, IOC block	Custom via XSOAR	Automated via Defender	Yes – full remediation	Block/quarantine + adaptive actions	Integrated into Helix workflows	Yes – with FortiSOAR
Threat Intel Use	Primary TI + verdict scoring	CrowdStrike Intelligence	Wildfire + PAN intel	Microsoft TI feed	SentinelLabs + 3rd-party	Trend Micro Smart Protection Network	Trellix Insights + McAfee legacy	FortiGuard Threat Intelligence
Deployment Model	Hybrid, on-prem first	Cloud-native	Cloud-first	Cloud-first	Cloud-native	SaaS with hybrid options	Cloud-managed or hybrid	On-prem + cloud
Zero Trust Support	RBAC + MFA + encrypted TLS comms	Yes	Yes	Azure AD + Conditional Access	Yes	Yes – supports ZTNA	Supports ZTNA & microsegmentation	FortiNAC + Zero Trust Access
Best For	Regulated, bespoke, hybrid orgs	Enterprise, rapid SOC deployment	Large orgs with PAN ecosystem	M365-heavy enterprises	Mid-large orgs with AI ops	Cross-domain security teams	Large enterprises with legacy overlap	Fortinet users, midsize with OT/IT

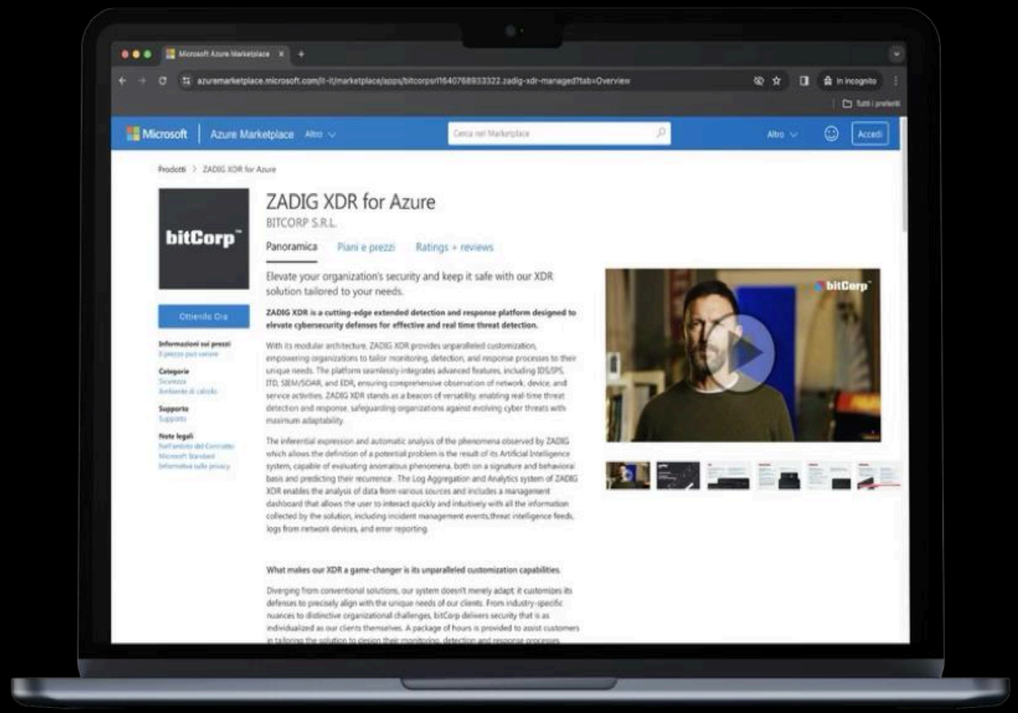
zadig® XDR Microsoft Partnership

The addition of zadig® XDR to the Microsoft Azure Marketplace underscores the innovation and reliability of our platform

This collaboration brings key advantages:

- Reliability and Security: zadig® XDR meets Microsoft's stringent quality standards, ensuring a highly secure and robust cyber defense solution.
- Global Accessibility: As part of the Azure Marketplace, zadig® XDR is easily accessible and seamlessly integrable for companies operating worldwide.
- Seamless Deployment: With fast, flexible configuration, zadig® XDR enables quick and efficient deployment in cloud environments.

With this milestone, we reaffirm our commitment to delivering cutting-edge cybersecurity solutions that safeguard businesses from evolving cyber threats.



The First Line of Defense

We believe that technology is not the only solution

75% of cyber attacks originate through phishing and social engineering campaigns that exploit negligent behavior on the part of affected company personnel.

Technology may not be enough. That's why every product in the zadig® line always includes a basic computer security training video course for all employees.

A course aimed at providing knowledge and skills to defend against the most common cyber attacks and designed to learn how to avoid the most common mistakes that can facilitate cyber attacks.

In addition, thanks to a self-assessment system, you will always have an up-to-date view of the actual state of readiness of your employees.

Summary

zadig® is a scalable, AI-driven cybersecurity framework with specialized modules that address real-time threats, forensic analysis, and organizational resilience.

Its unique AI adaptability, modular design, and federated intelligence capabilities make it ideal for organizations ranging from SMEs to critical infrastructure providers.

zadig®

Modular. Intelligent. Battle-Tested.

www.bitcorp.it

SAM.GOV®

L8QAZ1FWF3K4

Nato

CAGE CODE AU076