REVEALD®

Epiphany Validation Engine

The future of Breach & Attack Simulation

ABOUT OUR PLATFORM

Epiphany Validation Engine is a cloud-based breach and attack simulation platform that tests the strength of your cybersecurity controls through simulated cyber attacks. Our zero-trust platform enables users to rapidly identify security gaps, address vulnerabilities, and optimize solutions for customers.
More importantly, it allows continuous testing of customer environments to ensure regulatory and data privacy requirements are met, remediated, and provide an audit trail for third-party auditors.

HOW DOES THE EPIPHANY VALIDATION ENGINE COMPARE?

FEATURES	EPIPHANY VALIDATION ENGINE	COMPETITORS
Measure Network & Endpoint Vectors for Traditional Cybersecurity	X	X
Access to known artifacts/samples/ malware	X	X
Execution of samples and/or artifacts in a real and isolated environment	X	
On-demand advanced threat artifacts with specific triggers for IoC and BoC	X	
Modified known artifacts with unknown TTPs	X	
Access to new & unknown artifacts with standardized methodologies that reflect TTPs	X	
Monitoring callbacks, lateral movements, and attack servers (for custom artifacts)	X	
Actual measurement of the investigative skills of response teams under attack	X	

KEY FEATURES

100% Customizable

Customize each attack simulation. Dictate which kill chain phases you want to test, upload your own scripts, and encrypt threat artifacts.

Realistic, Continuous Assessments

Our on-demand method provides security teams a true-to-life assessment to determine if cyber defenses are configured and working properly.

Respond Using Actionable Data

Security can be quantified and measured according to prevention, detection, and response. Teams can prioritize actions and reduce their attack surface.

Measure Response Times

Our platform supplies a view into the response capabilities of security teams to react to threats and mitigate those risks rapidly.

MITRE ATT&CK Framework

Our threat artifacts follow APT standards, are based on the MITRE framework, test across the entire kill chain, and reflect authentic TTPs.

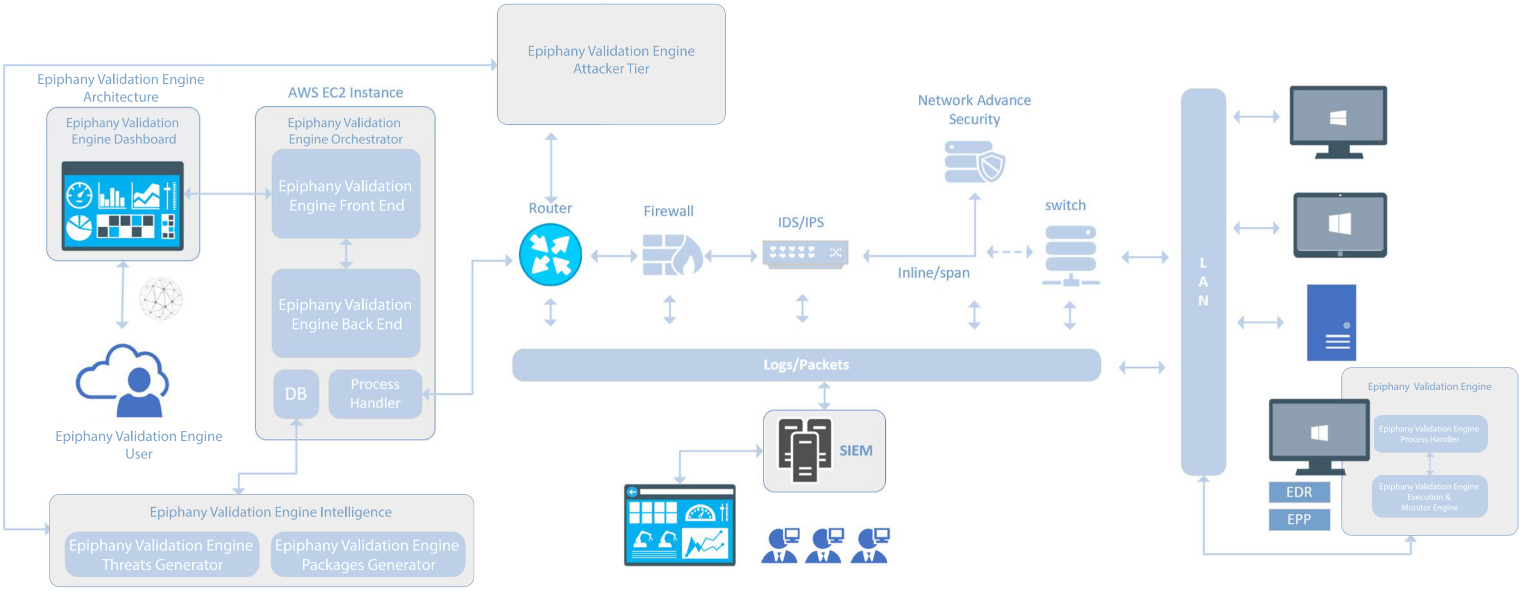
Secure Testing Environment

Tests are carried out through a virtual machine in a controlled testing environment on endpoints that contain your company's gold image. Lateral movements are removed from our threat artifacts.

USE CASES

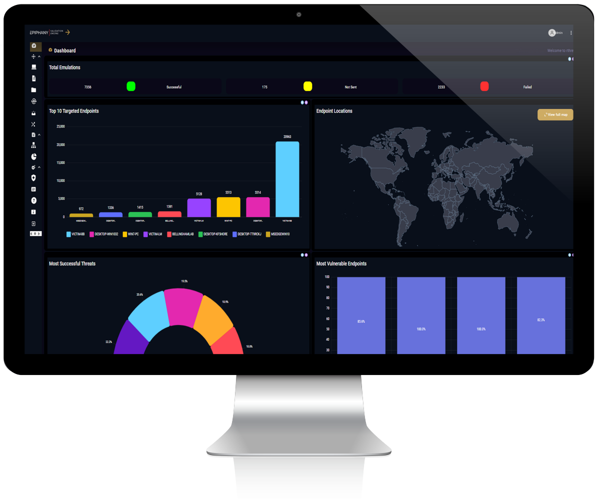
- Vulnerability Management
- Cybersecurity Controls Validation
- Compliance Enablement
- Remote Workforce Validation
- Continuous Evaluations
- Risk Assessment and Reporting
- Operationalize MITRE ATT&CK
- 3rd Party Supply Chain Posture
- Security Investment Optimization

HOW THE PLATFORM WORKS


Epiphany Validation Engine Architecture
AWS EC2 Instance
Epiphany Validation Engine Attacker Tier
Epiphany Validation Engine Dashboard
Epiphany Validation Engine Orchestrator
Epiphany Validation Engine Front End
Epiphany Validation Engine Back End
DB
Process Handler
Epiphany Validation Engine User
Epiphany Validation Engine Intelligence
Epiphany Validation Engine Threats Generator
Epiphany Validation Engine Packages Generator
Router
Firewall
IDS/IPS
Network Advance Security
Inline/span
switch
Logs/Packets
SIEM
L A N
Epiphany Validation Engine
Epiphany Validation Engine Process Handler
Epiphany Validation Engine Execution & Monitor Engine
EDR
EPP

At the network architecture level, Epiphany Validation Engine is installed as an AWS instance on the cloud and is given access to all security controls; the golden image. The image above is the flow that artifacts follow once shipped in a mature cybersecurity environment.

PLATFORM HIGHLIGHTS



Callback monitoring and validation: The Epiphany Validation Engine creates custom callback artifacts that can be a killswitch or malware download. These callbacks are monitored and the orchestrator validates and determines if the callbacks arrive succesfully or not. This functionality allows for the validation of mandatory playbooks that exist in the Security Orchestrator.

Advanced network evasion: The Epiphany Validation Engine can force the evasion of cyber security network elements based on sandboxing and hashes, through a shipping and control algorithm based on asymetric encryption. This forcefully verifies the correct operation of advanced security solutions that validate each artifact that travels throuth the network even when they possess advanced obfuscation and encryption mechanisms.

Execution results: Each package and artifact is aligned to the MITRE framework and the Attack Life Cycle, allowing for greater visibility of the attack sent. It is also possible to validate if the artifacted evaded network security, and if its execution was successful at the endpoint.

REVEALD®

Let us know what your needs are for measuring and evaluating your company's cybersecurity solutions.
Contact us: https://reveald.com/#contact

Call: 800- 884- 6142
Website: reveald.com

**31 HUDSON YARDS,
11TH FLOOR, NEW YORK,
NY 10001**