Why Take the Old Approach to Pen Testing?

Unparalleled Flexibility

EPIPHANY CAN ANALYZE OVER 35 DIFFERENT ON-PREMISE AND CLOUD BASED PLATFORMS

Including Rapid 7, Tenable, Qualys, CrowdStrike, Cylance, Microsoft ATP, McAfee, Active Directory, Okta, Duo, Azure, GCP, AWS, Ubiquiti, Cisco, Checkpoint, and Palo Alto.

INTRODUCTION

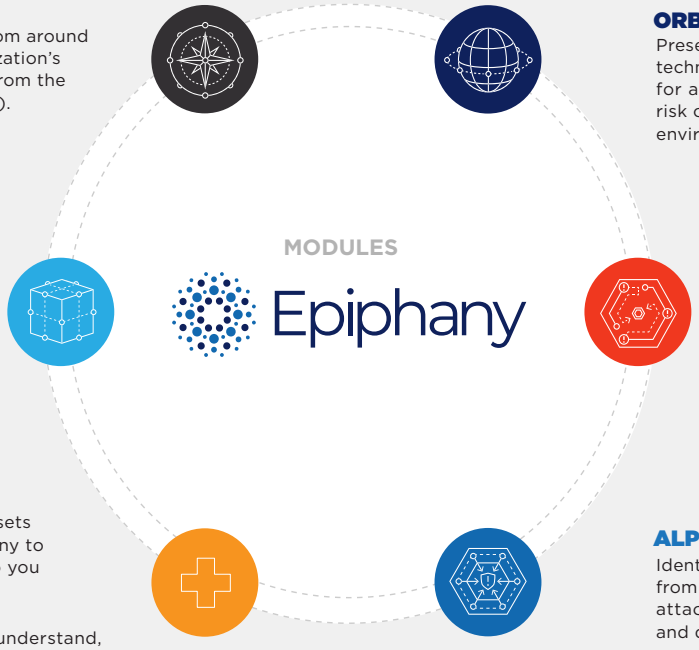
The traditional approach to vulnerability analysis and penetration testing results in pages of overlooked, poorly documented, non-impactful, and unactionable data produced by consultants with a limited view of your environment. Take control of the process to produce actionable intelligence from your penetration tests and understand your environment the way the adversary might. By using the power of the Epiphany Intelligence Platform during your assessment, Digitalware is able to produce the answers that you're often trying to answer while providing the expertise to elaborate further and take action on the areas of concern.

Vulnerabilities and risk conditions can number into the thousands, hundreds of thousands, or even millions in large, complex organizations and it only takes for an attacker to gain a foothold. Epiphany uses a target and prize driven analysis of the environment to determine not only the pathways an attacker has at their disposal, but how well your mitigations could deter and prevent a risk condition from being leveraged.

THE EPIPHANY INTELLIGENCE PLATFORM (EIP)

RECON
Identifies emerging risk conditions from around the world that could affect an organization's environment (with optional support from the Scout team of subject matter experts).

ORBITAL
Presents risks at the strategic, tactical, and technical levels, with insightful visualizations, for a comprehensive understanding of the risk conditions throughout an organization's environment.



LINK
Allows users to verify assumptions about boundaries and transitions across physical and logical security zones.

ALPHA RED
Visualizes an organization's environment from the attacker's perspective, identifying all potential attack paths that could compromise the organization's most valuable assets.

ADD-ON MODULES

Rogue Endpoint: Hunts for rogue assets on your network and enables Epiphany to pinpoint their locations and users, so you can quickly mitigate their risks.

Watchtower ICS: Lets you evaluate, understand, and mitigate risks to your facility management systems and industrial control systems.

ALPHA BLUE
Identifies key data points inside an organization, from a defensive standpoint, to anticipate attack paths, understand transition points, and determine the best places to defend.

As a result of the old penetration testing approach, many organizations struggle to understand the impact and subsequent remediation of a found vulnerability. The even greater challenge is taking those tactical break-fix issues and elevating them to a level where they can be integrated into or prioritized against a business risk management program. The problem is not a lack of information or intent. Rather, the filter that can make sense of all that data is context – the nature of the finding, the context of vulnerability, its impact to the organization, and the priority of its remediation compared to other findings. The Digitalware Epiphany Intelligence Platform solves these challenges by pairing attack intelligence, operational context, vulnerability data, and business knowledge with a team of offensive cyber experts to ensure the client has total awareness of posture, findings, and their prioritization of remediation by impact to the organization.

HOW EPIPHANY ASSESSES YOU

SCOPING
We work with you to identify the objective of the test.

DATA ALIGNMENT
We identify the technologies inside your environment that allow us to answer the questions you care about.

TARGET IDENTIFICATION
Attackers care about what they find inside your environment. So do we.

ATTACK PATH MAPPING
Visualize all the pathways an attacker can take from any entry point to any target.

MANUAL VERIFICATION
For those extra sensitive systems or critical applications our team of experts can manually verify the conditions identified by Epiphany for an added layer of understanding.

REMEDIATION PRIORITIZATION
Armed with the knowledge from Epiphany we can produce a list of remediation and mitigation actions prioritized on minimizing impact to the organization, not just patching random vulnerabilities.

The Epiphany Intelligence Platform allows all key stakeholders within the organization to understand and make quantifiable decisions on the risks behind the findings by helping to answer:

1. Am I exposed?
2. Can an attacker get something of value?
3. What do I fix first?
4. What is the impact of a compromise?
5. What is a tactical issue versus a foundational one?
6. Are my privileged accounts at risk?
7. Where is risk being pooled in my environment?
8. Where are the gaps with my current tool set?
9. Can an attacker get in from the outside?
10. What systems are at risk from phishing attacks?

Stop fighting your security tools.

See what your true risks look like.

Contact us today to start risk hunting with Epiphany.

EPIPHANY@DIGITALWARE.COM

ABOUT DIGITALWARE

Digitalware delivers world-class cybersecurity solutions for enterprises in every sector of government and industry, including the Fortune 500. We are dedicated to reducing technical and business risks through innovative technologies, including artificial intelligence and machine learning.

Our mission is to safeguard our clients' data, assets, and operations across the globe. We assess each client's unique needs and challenges to ensure that their risks are visible, managed, and mitigated. If it's connected, it must be protected.