Digitalware | **Epiphany Intelligence Platform™**
Find, prioritize, and master risk—with eye-opening speed and insight.

Epiphany Facility Systems Security

PROTECT YOUR FACILITY BETTER: IDENTIFY, QUANTIFY, PRIORITIZE & MITIGATE RISKS

See where your technical vulnerabilities meet your true business risks — before an attack

Defending your facility against cyber attacks can be complex, time-consuming, and costly. Vulnerability and risk management programs can give you data overload. And they may only react after an attack has occurred. Plus, they can't tell you if, or how much, a technical issue poses a true risk to your critical operations.

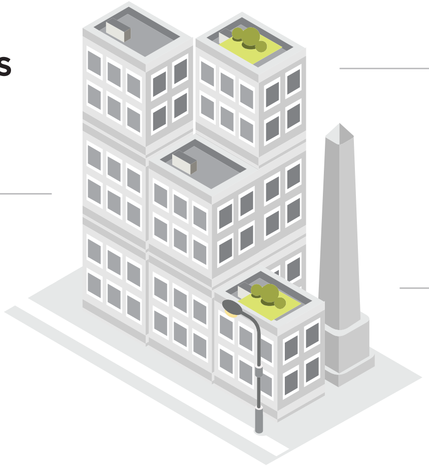
Epiphany is different. It gives you complete visibility of strategic business risks, not just technical issues and vulnerabilities. And it prioritizes the most important risks, so you know where—and how—to focus your mitigation efforts. There's no data overload. No wasted time chasing false alarms.

Best of all, Epiphany is proactive—it goes risk hunting before there's an attack on your facility. And it works invisibly in the background, while your facility operations run normally.

KEY VALUES:

1. Identifies risks 3x faster than traditional vulnerability assessment tools.
2. Provides complete visibility of key business risks, not just technical issues.
3. Shows all potential attack paths—and the best ways to stop them.
4. Prioritizes business risks over technical issues, to eliminate data overload and streamline the patch process.
5. Eliminates the need to manually cross-reference multiple tactical tools.
6. Eliminates time wasted on false-positive alerts from point solutions.
7. Provides a simple visualization of risk, so all stakeholders can speak a common language using a common data set.
8. Consumes data quickly as agentless overlay to existing security tools—no agents or heavy infrastructure to deploy.
9. Delivers immediate results at any scale, accelerating any organization's risk maturity.

CRITICAL BUILDING RISK AREAS



Physical Systems

- HVAC
- Camera
- Access control
- Common area tech (Wi-Fi, displays)

Information Technology

- Computer systems
- Infrastructure (networking)
- Vulnerability management
- Configuration control

Building Technology

- Building orchestration
- Building automation
- IoT/sensors (occupancy)
- Resiliency (back-up systems)

The Epiphany Intelligence Platform improves how building owners/managers see, understand, and control risks in their facilities. Specifically, Epiphany:

1. Identifies and quantifies technical risks.
2. Catalogs connections into facility.
3. Assesses networked devices.
4. Prioritizes business risks in context with technical issues.
5. Maps potential impacts of compromised assets.
6. Holds third-party vendors accountable for cyber security.

Integrated into your facility operations

Epiphany overlays existing systems without affecting their normal operation, so your facility processes will continue to run smoothly. In addition, Epiphany can tie into work order systems to turn detected risks into specific remediation tasks—automatically.

Key capabilities

Epiphany lets you hunt for—and mitigate—business risks more effectively than traditional vulnerability and risk management applications ever could. Epiphany also optimizes your investment in your existing tools infrastructure—by showing you which systems are most effective…and which are not.

EPIPHANY MODULES

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.

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.

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.

Link

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

Watch Tower

Evaluates and understands risks present in the environment that impact facility management systems and industrial controls. (Required for facility management; optional for other applications.)

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).

EYE-OPENING INSIGHT

Complete Risk Visibility
Epiphany sees, understands, and displays technical issues in context with business risks—on servers, desktops, IoT devices, and ICS devices. And it uses only the data already present in your environment.

Model Disconnected Systems
Epiphany can even model the state of systems that are disconnected from the facility and corporate network.

Comprehensive Attack Prevention
Epiphany gathers organizational data and metadata to calculate all the ways attackers could find sensitive areas, vulnerable systems, or privileged credentials. Then it shows you where and how to protect your most valuable business assets, processes, and systems.

Insight Beyond Vulnerabilities
Event-based tactical tools, alone, can't give you a full understanding of your strategic, organizational risk. Epiphany goes far beyond vulnerability management, to expand awareness of your entire system state—and prioritize true business risks.

SPEED TO BENEFIT

Simple to Deploy
Epiphany is completely agentless. You don't have to manage any additional services. The platform gets all the data it needs from your existing security tools and technologies. And Epiphany works no matter what environment you have—Cloud, local, or hybrid. That means Epiphany is easy to implement—often in just a few days.

Immediate, Meaningful Results
Since Epiphany overlays your security infrastructure—harvesting data from all your existing systems—there are no data silos. And the platform starts producing results instantly after it starts ingesting data. So not only is Epiphany quick to deploy, it can deliver actionable information within hours of deployment.

Zero Impact on Environment
Because Epiphany is agentless and requires only data already in your environment, it won't disrupt your systems or operations.

TIME AND MONEY SAVED

Faster, More Cost-Effective Penetration Testing
By understanding every potential attack path, Epiphany eliminates the need for meaningless, non-targeted penetration tests. And when you do run pen tests on your environment, Epiphany will cut the time it takes by up to 75% while maximizing the output.

More Efficient Security Teams (and Fewer Consultants)
Epiphany enables security professionals to focus on what matters most, prioritizing the most impactful actions to mitigate the greatest risks. That means more bang for the buck from your internal security team, and less reliance on costly outside consultants.

Optimized Security Tools
Most organizations have many security tools and technologies, from multiple vendors. By gathering data from all these sources, and assessing how risks can best be mitigated, Epiphany can reveal which tools are most—and least—effective.

Lower Risk of Catastrophic Loss
With deep insights, fast reactions, and prioritized remediation, Epiphany can significantly reduce risks to critical business assets, processes, and systems. That translates into revenue protection, cost avoidance, and reputation preservation.

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.