EPIPHANY SYSTEMS

USE CASE

# Understanding the Implications of Compromise

**CUSTOMER INDUSTRY**
Public Sector

**ATTACK SURFACE**
Over 30K endpoints

**PLATFORM COMPONENTS**
Epiphany Intelligence Platform™

## Summary

A third-party security assessment found that a customer's employees were susceptible to social engineering and phishing attempts. The customer's executive leaders wanted to understand the impact that a successful phishing attack could have on the organization. To quantify the answer, the security team considered two approaches:

- Conduct traditional penetration testing to phish network users and try to reach assets of value.
- Use the Epiphany context search engine to look across their enterprise data, run a series of queries, and contextualize "how bad could it be?"

While pen testing might seem routine for security practitioners, it poses both practical and operational challenges. Errors in pen testing can cause unanticipated impacts to the production environment.

Epiphany, on the other hand, offers a way to detect risk conditions and visualize how attacks could transition across a network, without affecting the environment at all.

### KEY BENEFITS

- Quickly derive impacts of social engineering and technical risk
- Analyze outcomes from attacker's perspective
- Connect data across the enterprise to answer risk-related questions
- Ask state-related questions about the environment with nearly limitless flexibility
- Reduce time to get answers, identify mitigations, and reduce risk

### WHY EPIPHANY?

- Built to answer the questions "What if?" and "Is this a risk we currently have?"
- Ingests nearly any data source or enterprise platform to measurably increase risk awareness and visibility
- Identifies and prioritizes business risks with correlated, quantifiable data
- Deploys rapidly to organizations of any size in cloud, hybrid, and on-premise modes
- Operates without agents and causes zero disruption to the operational environment

## Challenge

The customer had 40,000 employees spread across multiple physical locations, including the homes of remote workers. Users were organized into hundreds of Active Directory groups, AWS permission groups, and groups with unique application privileges, all gated via Single Sign-on.

To try to gauge the risk of a phishing breach, the customer's security team entered data manually into spreadsheets. They had no automated system to correlate the silos of IT data, security data, and identity data. So each test (on a single system user) took over 30 hours of analyst time. As a result, they could test only a small set of administrative users.

The manual process to harvest data included: searching for user and administrative identities and permissions across multiple identity providers; finding that user's machine to determine the potential vulnerabilities that could be leveraged by a phishing attack; and estimating what could happen if that any of that user's identities were compromised.

Adding to this complexity, they had no way to know if the defensive technology on a user's machine was effectively detecting and blocking an exploit. So although they had many security tools and their own pen testing team, they could not confidently or quickly define the potential impacts of a phishing attack.

The security team needed a better, faster way to query data from multiple on-prem and cloud-based tools across their enterprise. Ideally, they wanted one unified platform to answer the executives' questions about "What could happen?"

## Solution

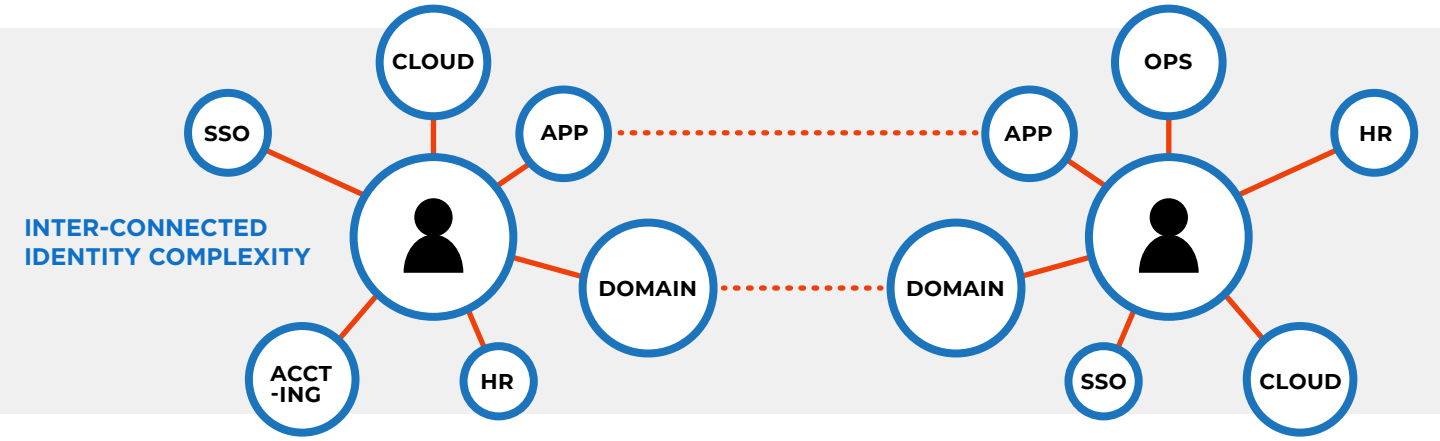
The customer looked at multiple vendors and enterprise toolsets for vulnerability management, breach simulation, and endpoint management. But the only solution that provided exactly what they needed was Epiphany.

### Epiphany was able to produce a map of attack paths that showed executives what a phishing breach could do. And it did it in less than 60 seconds.

The platform analyzed a complex set of questions about user identities, systems, operational context, and probability of outcomes. It absorbed data from both manual assessments and automated sources, including endpoint protection suites, vulnerability scans, Active Directory data, Okta, Duo, AWS, Azure, GCP, and user session data.

**EPIPHANY WAS ABLE TO ANSWER QUESTIONS LIKE:**

1. Who of my users within a known list are working on a system with critical phishing vulnerabilities?
   a. Which of those users have administrative privileges of any level?
   b. Which of those users have access to critical applications in the environment?
2. Do I know how many and what types of vulnerabilities are associated with the attack and how effective are they against my AV/EDR?
3. Are the vulnerabilities being currently leveraged by any known groups targeting my organization?
4. What are the resulting attack pathways available after compromise?
   a. Are they domain-based, cloud-based, application-based, or computer to computer attacks?
5. Would my network and cloud systems effective prevent migration along these attack pathways?
6. What is the expected outcome of these attack chains? Would the attacker be able to reach a critical asset, application, or database?
7. Are there any other risks associated to these systems and what is their priority to the business?
8. Where do I start first to reduce risk of these potential phishing attacks?




## Outcome

Epiphany's ability to ask "what if" questions allowed the customer's analysts to quantify the effectiveness of their security posture and strategy against phishing attempts. It eliminated the old, cumbersome testing process, saving hundreds of work-hours. And Epiphany's scope dwarfed the limited reach of the prior testing—the platform provided risk visibility across the entire network.

By deploying Epiphany, the customer achieved unprecedented awareness of risks, new and old, that could impact their environment. And the platform gave the security team the confidence to act on the results immediately.

In short, Epiphany became the central source of security knowledge and "truth" in the organization.

# Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us