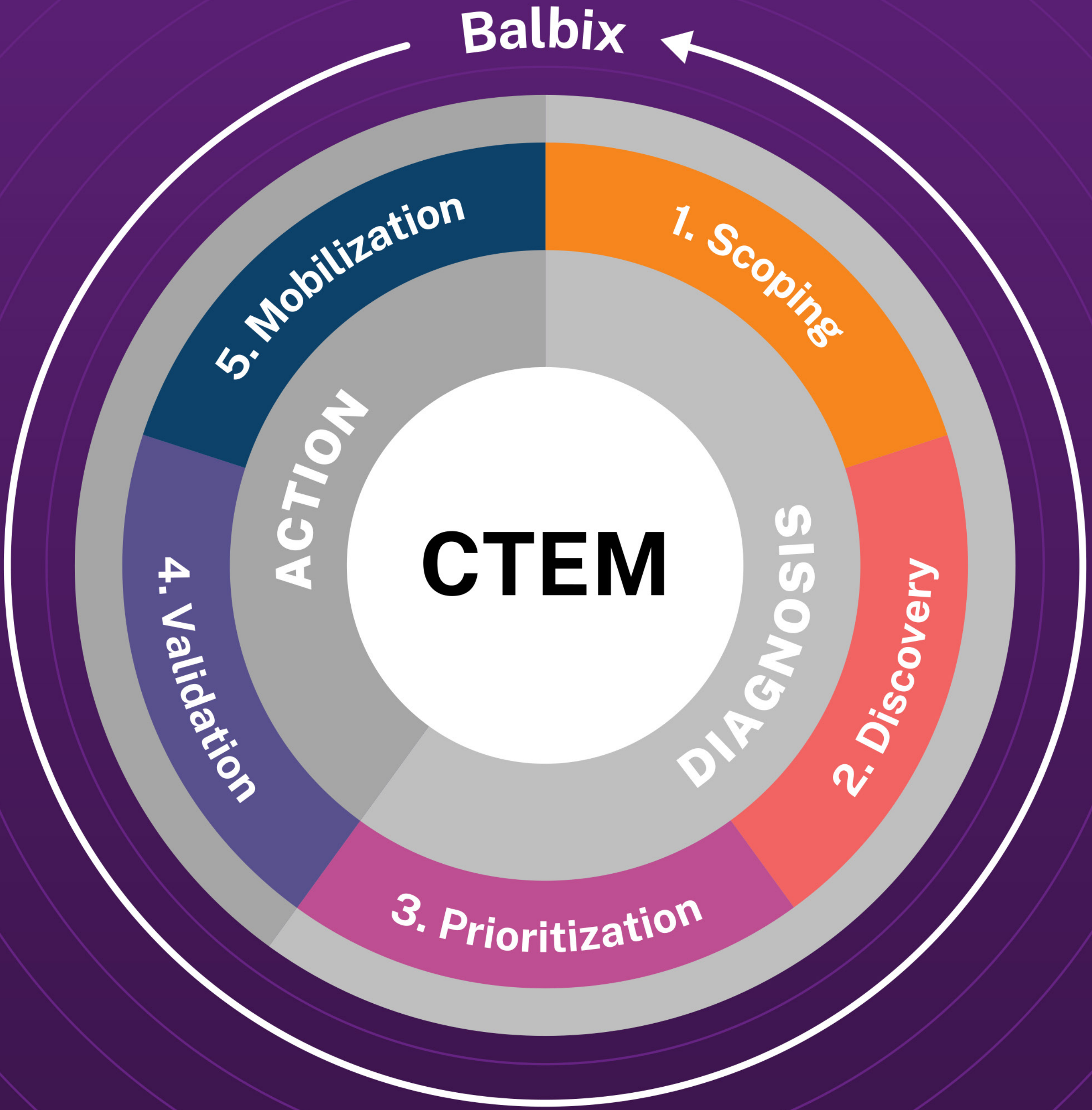
# Discover why CTEM is a top 10 security trend and why CISOs are adopting it.

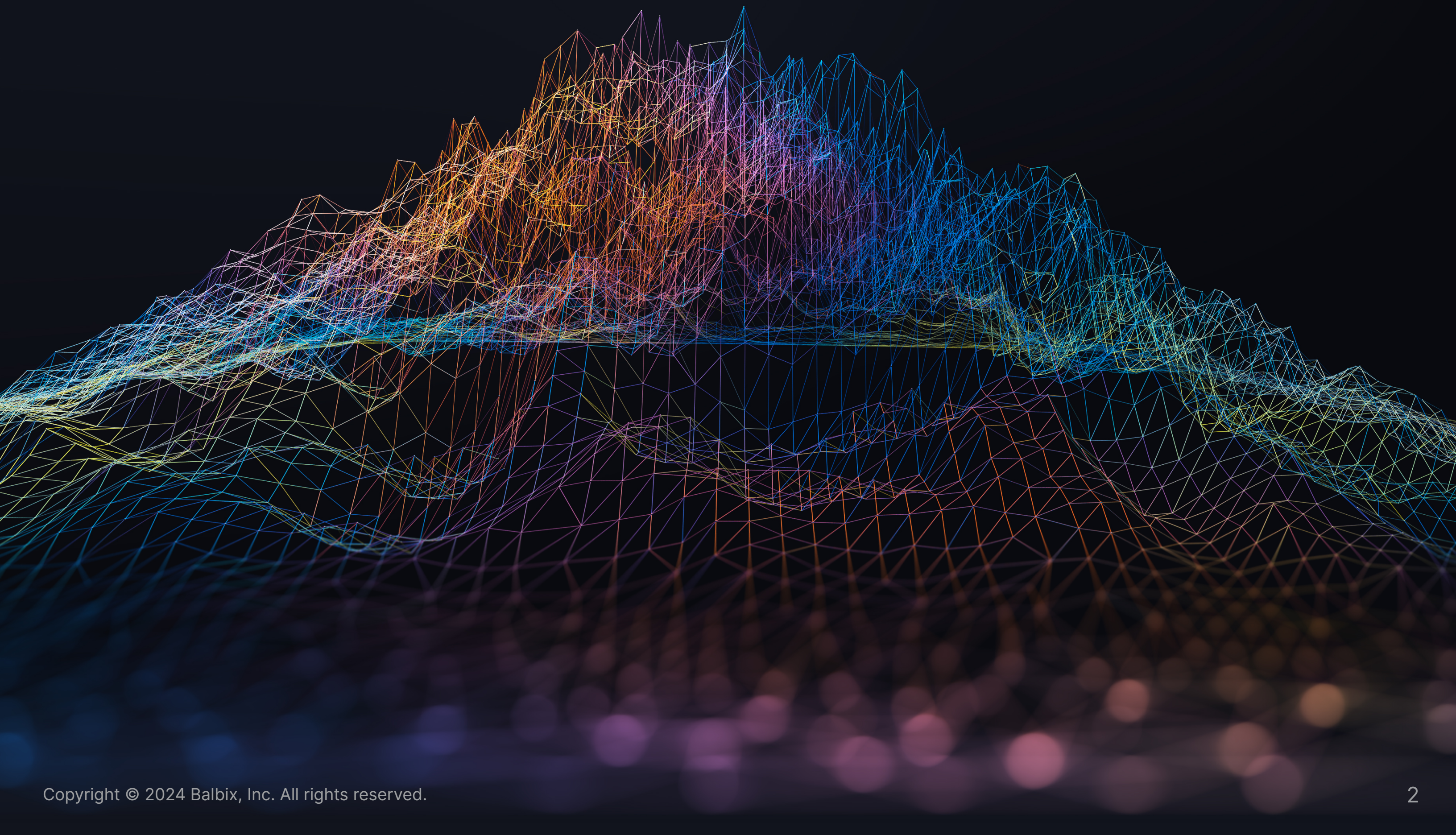


Balbix®

eBook

Earlier this year, Gartner identified Continuous Threat Exposure Management (CTEM) as one of the top 10 technology trends. CTEM transforms traditional vulnerability management by broadening the scope beyond common vulnerabilities and exposures (CVE) to all sources of threat exposures (i.e., misconfigurations, open ports, weak encryption, etc.) and a risk-based prioritization strategy. The key question most Chief Information Security Officers (CISOs) and their teams ask is how CTEM differs from traditional VM.

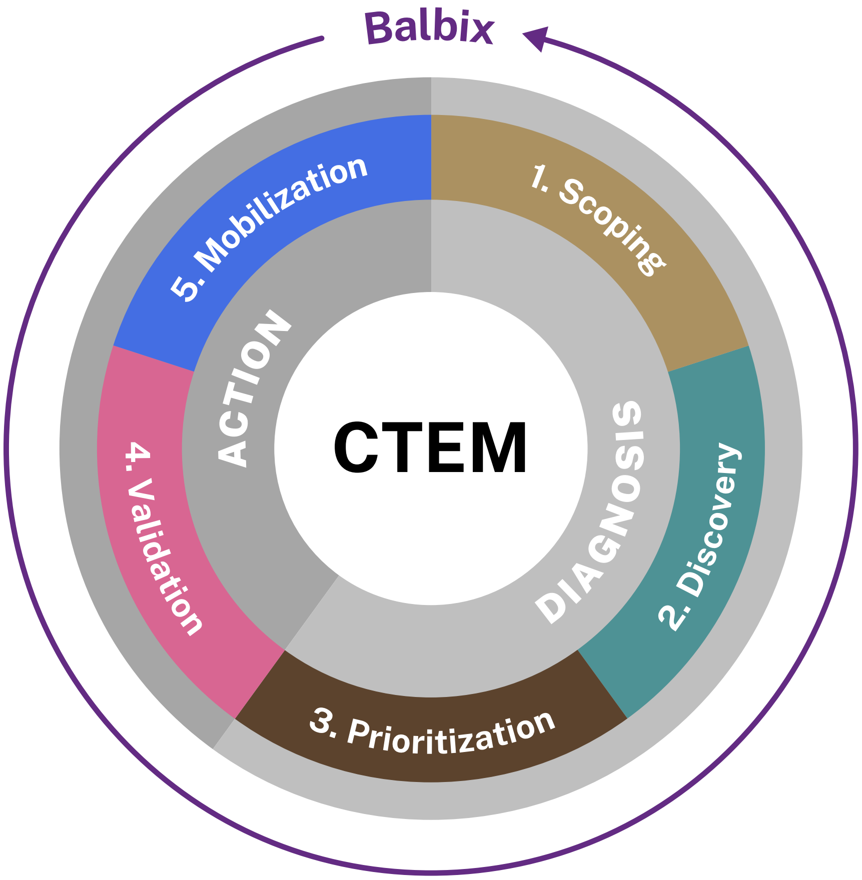
> *"The volume of discovered assets and vulnerabilities is not success in and of itself; it's far more valuable to accurately scope based on business risk and potential impact."*
>
> **—Gartner**



# What is Continuous Threat Exposure Management (CTEM)?

CTEM represents a revolutionary approach to cybersecurity, focusing on proactive measures and constant vigilance to fortify digital defenses. Unlike traditional vulnerability management strategies that depend on periodic assessments, CTEM specifies comprehensive, ongoing monitoring of the IT, cloud and IoT environments. This methodology enables real-time detection of new vulnerabilities and a dynamic response to the ever-changing cyber landscape. Learn more about the five steps in CTEM.

## CTEMs **Five Steps** to Cyber Resilience



1. **Scope**
   your organization's "attack surface"

2. **Develop**
   a discovery process for assets and their vulnerabilities & misconfigurations

3. **Prioritize**
   the threats most likely to be exploited

4. **Validate**
   if the current response plan is sufficient to protect the business.

5. **Mobilize**
   people and processes. The objective of the "mobilization" effort is to ensure teams operationalize the CTEM findings by reducing any obstacles.

# CTEM vs. Traditional Vulnerability Management

CTEM differs from traditional vulnerability management in that it emphasizes real-time threat detection and prioritization based on business impact rather than periodic scans. It also integrates seamlessly with other security tools, offering ongoing adjustments and quicker responses to evolving cyber threats. The following compares the limited capabilities of traditional VM with CTEM features:

| Features | ☒ Traditional VM | ☑ CTEM |
|---|---|---|
| **Asset Visibility** | • Limited visibility into assets. Often overlooks mobile, IoT, and cloud | • Comprehensive coverage, including mobile, IoT, and cloud |
| **Vulnerability Management** | • Periodic scans lead to potential delays in identifying new vulnerabilities | • Real-time vulnerability detection<br>• Continuous scanning and analysis |
| **Threat Intelligence** | • Doesn't use threat intelligence to prioritize vulnerabilities | • Uses threat intelligence to understand if there are cases of vulnerability exploitation in the wild |
| **Mitigating Controls** | • Doesn't use mitigating controls to prioritize vulnerabilities | • Integrates existing and/or compensating controls into prioritization |
| **Business Impact** | • Challenges tying vulnerabilities to business impact | • Links vulnerabilities to business impact and financial risk.<br>• Prioritize risks based on business impact, not just severity and probability |
| **Integration With Other Tools** | • Limited integration with tools | • Broad integrations with various IT and security tools to enable holistic security. (i.e. configuration compliance, CMDB & asset mgmt., EDR & endpoint mgmt, vulnerability management, patch management, cloud security,IoT/OT network, BAS, EASM, ticketing, AppSec etc. |
| **Automation** | • No or limited automation in eporting | • Automates detection, prioritization and remediation processes |
| **Reporting & Visualization** | • Limited visualization options. | • Advanced reporting and visualization tools to aid in understanding threats and communicating risks. Report metrics should include MTTD, MOVA, MTTP and breach impact in $$ |

# Are you ready for CTEM?

Transitioning to CTEM is a strategic move that involves reassessing how you currently identify, prioritize and mitigate vulnerabilities. Here are a few questions to ask yourself and answer if you are ready to adopt CTEM:

### 1. Vulnerability Prioritization Strategy

□ Do zero-day vulnerabilities usually take up a large bandwidth of time and resources rather than vulnerabilities that impact your environment?

□ Do you use CVSS or EPSS to prioritize vulnerabilities?

### 2. Workflow Efficiency

□ Do IT teams ask or desire more context on vulnerability remediation?

□ Do you manually search and identify which patches to apply for a particular vulnerability?

### 3. Reporting & Metrics

□ Does your current vulnerability management focus on the number of vulnerabilities resolved?

□ Does your CISO and the board ask for metrics or ROI of VM programs on risk reduction?

### 4. Integration & Automation

□ Do you want a unified view of vulnerabilities across IT, cloud, and IoT environments?

□ Are you unable to correlate and normalize data across multiple tools?

### 5. Strategic Alignment

□ Is vulnerability management considered a core component of risk reduction in your organization?

□ Are threats and/or incorporating business impact for vulnerability prioritization on the roadmap?

### 6. Stakeholder Communication

□ Can your security team articulate the impact of the vulnerability management program to non-technical stakeholders?

□ Do you want to quantify cyber risk in financial terms to prioritize actions effectively?

### 7. Continuous Improvement

□ Do you want to benchmark your program against your peers?

□ Do senior leaders desire a culture of continuous improvement and learning within your security team?

If you answered yes to half or more of the questions above, you are ready to consider CTEM.
Sign up to learn more here.

# How Balbix Can Help Migrate to CTEM

Balbix can provide a CTEM solution that addresses the following pillars:

CTEM Challenge:

## Scoping

### How Balbix helps:

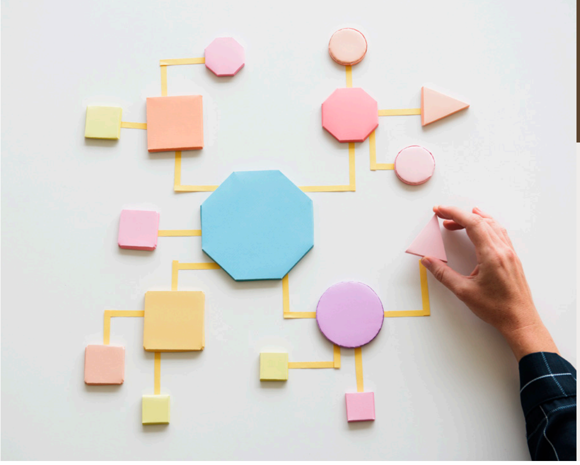
- Gain visibility into your attack surface.
- Identify, consolidate, normalize and deduplicate data gathered from IT, security, business, and home-grown tools.
- Establish cyber risk metrics and vulnerability sources.

CTEM Challenge:

## Discovery

### How Balbix helps:

- Deliver a comprehensive asset inventory – identify all assets, vulnerabilities, and mitigating controls.
- Normalize all asset data
- Define organizationally acceptable vulnerability/risk levels/ thresholds.



CTEM Challenge:

## Prioritization

### How Balbix helps:

- Prioritize based on severity, threats, mitigating controls, asset exposure, and business impact.
- Track risk metrics such as Mean Time to Patch (MTTP), Mean Time to Remediate (MTTR) and Mean Open Vulnerability Age (MOVA) across groups, geos, BUs

# How Balbix Can Help Migrate to CTEM

Balbix can provide a CTEM solution that addresses the following pillars:

**CTEM Challenge:**

## Validation

### How Balbix helps:

- Check the effectiveness of security controls using MITRE Engenuity
- Provide reports on coverage gaps for security controls.

**CTEM Challenge:**

## Mobilization

### How Balbix helps:

- Conduct fix identification
- Execute remediation/patch projects
- Implement ticketing integrations
- Establish a risk acceptance workflow
- Generate risk/exposure reports

# Greenhill

## Challenges

Greenhill was facing several critical challenges that necessitated a shift to CTEM, leading them to work with Balbix:

1. **Data Fragmentation Across Tools:** Greenhill's data from various security tools was scattered in different formats, making it challenging to unify and prioritize action items effectively. This fragmentation hindered the ability to have a cohesive view of vulnerabilities and risk, making it difficult to remediate critical vulnerabilities.

2. **Inefficient Velocity in Vulnerability Management:** The reliance on periodic assessments like annual pen-testing and quarterly vulnerability scans was inadequate. With the rapid evolution of cyber threats, new vulnerabilities could emerge and go undetected.

3. **Need for Effective Measurement of Program Maturity:** Greenhill's CIO, John Shaffer, aimed to streamline the vulnerability management process and measure the effectiveness and maturity of their cybersecurity program over time. The existing setup did not allow for easy tracking of improvements or identifying areas needing attention.

These challenges showcased the need for a more dynamic, continuous, and integrated approach provided by CTEM, allowing for real-time visibility and more proactive management of cybersecurity risks

## Solution

Greenhill's transition to a CTEM model using the Balbix platform marked a significant evolution in its cybersecurity approach. By shifting from periodic vulnerability scans to continuous monitoring and real-time risk analytics, Greenhill achieved a 55% reduction in patch time and elevated their security posture to the top 10 percentile in industry standards. Integrating Balbix with existing security tools like CrowdStrike and Illumio enabled automated processes and a unified security system that streamlined operations and quantified the ROI of their cybersecurity investments, enhancing decision-making and reporting to the board. This holistic approach allowed Greenhill to significantly reduce its cyber risk and better manage its security landscape.

> *" Balbix shows the ROI of my entire cybersecurity program. We have invested a lot of money and effort in our security initiatives. With Balbix, for the first time, I am able to see the overall effect of the cybersecurity program."*

**John Shaffer, CIO, Greenhill & Co.**

# Conclusion

Continuous Threat Exposure Management (CTEM) represents a dynamic and proactive approach to risk management. Adopting CTEM  is essential for security leaders to maintain a resilient cybersecurity posture, effectively neutralizing threats before they cause harm. By leveraging tools such as Balbix, organizations can protect their critical assets against emerging cyber threats, ensuring robust defense.

Request a demo to learn more about how Balbix can help you improve your security.

Balbix®