A CYCOGNITO SOLUTION BRIEF

Exposure Management

Reactive to Proactive

Gartner predicts that by 2026, "non-patchable attack surfaces will grow from less than 10% to more than half of the enterprise's total exposure."[1] As fewer and fewer assets are eligible to be patched, it's clear that existing remediation practices won't be effective and exposure, along with the risk that comes with it, will have to be managed, not eliminated.

A CYCOGNITO SOLUTION BRIEF

The Problem

What is Exposure Management?

Gartner divides the Continuous Threat Exposure Management (CTEM) process into several components: Diagnosis and Action, with subdivisions into Scoping, Discovery, Prioritization, Validation and Mobilization.

Organizations begin by identifying the scope of their exposure, finding assets within that scope, prioritizing and validating issues, and then taking action to manage identified risks.

Exposure management is a practice and a process, not just a product.

Exposure management is a practice and a process, not just a product. Organizations that adopt CTEM as a framework for risk reduction can use this emerging initiative to broaden their gaze to encompass issues beyond software-based vulnerabilities, like under-managed and misconfigured assets. CTEM also refocuses teams' time and energy on the actual risk posed by each potential external exposure.

Find, Test, Prioritize, Fix

CTEM can sound simple but contains hidden challenges, particularly when it comes to performing these actions automatically and at scale.

DYNAMIC EXTERNAL ASSET INVENTORY

To truly manage exposure, teams need a comprehensive, up-to-date view of the attack surface that identifies where assets are and how they are connected.

HIGH CONFIDENCE IDENTIFICATION OF ISSUES

To remediate efficiently, teams need high confidence test data and proper context. Active testing must be frequently and automatically performed across the entire external attack surface to obtain the highest quality critical data.

INTELLIGENT PRIORITIZATION

Basing issue prioritization solely on CVSS score fails to consider the context of your unique attack surface. Incorporating business context about the affected asset and actual data from active testing enables teams to make informed decisions about risk and exposure.

SEAMLESS OPERATIONALIZING OF INFORMATION

Integrating data gathered through the discovery, testing, and prioritization phases into existing remediation processes smooths communication and accelerates action.

A CYCOGNITO SOLUTION BRIEF

Comprehensive Visibility through Exposure Management

Berlitz, a global education organization, faced challenges in their attack surface.

The organization is over 145 years old, and much of their systems were decentralized. "Until recently a lot of operational functions were decentralized and regionally operated. Anyone with a little budget could authorize a public-facing resource." said Daniel Schlegel, Global IT CIO, Berlitz Corporation. This is a common problem for distributed organizations with many subsidiaries, especially when the subsidiaries are given a lot of autonomy – they can act quickly and nimbly to respond to issues, but end up with a miasma of poorly understood, under-managed or forgotten exposures.

The first response for many in this situation is to attempt to build an external asset list. However, they quickly realize it is a never ending task that is out of date quickly. However, without context about how those assets are connected to the attack surface, what platforms they expose and what data is put at risk, the result is often just a long, unprioritized list of assets and issues.

For Berlitz, it was important to have a holistic view of their attack surface. Daniel explains, "we needed to have a broad overview across the board, literally every platform. whether there was possible exposure to PII, unpatched web servers, or identifying any other open vulnerabilities, like expired certificates."

> **"We needed to have a broad overview across the board, literally every platform. whether there was possible exposure to PII, unpatched web servers, or identifying any other open vulnerabilities, like expired certificates."**
>
> DANIEL SCHLEGEL, GLOBAL IT CIO, BERLITZ CORPORATION

With this deep understanding of their exposures and what risk each exposed asset posed to the organization, the team felt confident they could perform true exposure management.

> **"CyCognito enables us to bring all our external assets under one umbrella, to look at this more holistically and centrally manage what's going on."**
>
> DANIEL SCHLEGEL, GLOBAL IT CIO, BERLITZ CORPORATION

Berlitz quickly realized that the issue of unmanaged attack surface sprawl must be solved on two fronts – first, by automatically identifying all exposed assets and then by rigorously assessing and prioritizing their exposure. Without the first, assets with critical issues may go unnoticed and forgotten, while without the second security teams are left unable to determine which issues to remediate first.

With CyCognito, Berlitz has gained comprehensive visibility across their entire digital landscape. Schlegel says, "CyCognito enables us to bring all our external assets under one umbrella, to look at this more holistically and centrally manage what's going on."

A CYCOGNITO SOLUTION BRIEF

Use Cases

Understand Risk Caused by External Exposures

An Exposure Management program helps your organization evaluate the impact of potential security incidents and prioritize fixes accordingly.

Intelligent risk assessment allows your team to prioritize fixes and evaluate the threat posed by unpatched or unpatchable vulnerabilities.

Proactive, Not Reactive

The volume of new CVEs every month can keep security teams on the back foot. Exposure Management is a proactive approach that continuously evaluates the risk in your external attack surface.

Proactively identify threats to your organization with continuous automated assessment and prioritization of issues across the entire external attack surface.

Automate Complete Discovery, Testing, and Prioritization

Exposure Management requires comprehensive coverage of the attack surface – only continuous monitoring of 100% of exposed assets delivers complete insight.

CyCognito continuously maps your attack surface and discovers new assets, automatically adding business context and attribution and actively testing for critical security issues.

1. Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

We are CyCognito, a revolutionary approach to exposure and risk management driven to create positive business impact. We help organizations identify, understand and master their risk in profound new ways. **Rule Your Risk.**

For more information on CyCognito's External Attack Surface Management solution, go to **cycognito.com/how-it-works** or schedule a demo at **cycognito.com/demo-video**.

CYCOGNITO