

# The Never-ending Game

THE WINNING STRATEGY:  
6 STEPS TO BUILDING A BETTER SECURITY PROGRAM

**GPVUE**  
SECURITY PROGRAM

## Tired fragmented approach causes...

**Bloated, underutilized tool sets**

Alert **fatigue and overworked** personnel

**Lack of organizational buy-in** for cybersecurity

A feedback loop of cybersecurity programs that are **caught in a never-ending game of catch-up**



Core problems of the traditional approach to cybersecurity programs are now exposed.

## “How do we fix it?”



**Take Inventory**  
Know your security environment

**Assess**  
What’s the level of maturity of each security practice in your organization?

**Identify**  
What are the gaps in your security program?

**Prioritize**  
Make better risk-based decisions for how to move forward

**Implement**  
Optimize existing technologies or purchase new tools

**Test Continuously**  
Engage your program to keep your teams and personnel in peak form, but more importantly to measure and report on the success of your improvements.



**GPVUE is a strategic, programmable cybersecurity approach that goes beyond individual solutions and services to give you a more mature security program and posture.**



## What’s Your Cybersecurity Maturity?



Knowing your security maturity level is key to deciding whether it makes sense to apply a cybersecurity program management approach. To assess your organization’s level of security maturity, take our new security assessment questionnaire, which explores the extent of your current security program, your experiences hiring cybersecurity talent, and how you would rate your security program’s functionality.

[Test Your Security Maturity](#)