KnowBe4

Deliver Real-Time Coaching in Response to Risky User Behavior

Improve Overall Security Culture and Reduce Human Risk

With the ongoing problem of social engineering attacks, bad actors try to exploit your users by looking for any way to breach your organization's cybersecurity defense layers. According to the 2025 Verizon Data Breach Investigations Report, the human factor is involved in 60% of breaches. And, your overwhelmed, stressed-out security teams need relief from the alert noise caused by the repetitive risky behaviors of your employees.

What if you could take user event data detected by your existing security stack to deliver real-time coaching to your users in response to their security mistakes, while also reducing the volume of alert noise for your Security Operations Center (SOC) team caused by those repetitive risky behaviors? Now you can with SecurityCoach™.

What is SecurityCoach?

SecurityCoach is the first real-time security coaching product created to help IT and Security Operations teams further protect your organization's largest attack surface—your employees.

SecurityCoach helps strengthen your security culture by enabling real-time security coaching of your users in response to their risky security behavior. Leveraging your existing security stack, you can configure real-time coaching campaigns to immediately deliver contextual SecurityTips that reinforce your security awareness training and policies to your users. This improves knowledge retention and helps users understand the risks associated with their behaviors.

SecurityCoach integrates with KnowBe4's security awareness training and your existing security stack to deliver real-time coaching in response to risky end-user security behavior.

SecurityCoach

Key Benefits

- Reinforce user comprehension and retention of security training and established security policies with real-time coaching on real-world behavior
- Leverage your existing security stack to deliver real-time coaching to your risky users and gain additional value from your existing investments
- Build custom campaigns for high-risk users or roles that are considered a valuable target for cybercriminals or that keep repeating risky behaviors
- Measure and report on improved real-world security behavior across your organization, providing justification for continued investment
- Reduce the burden on your SOC and improve efficacy by decreasing alert noise caused by repetitive risky security behaviors

KnowBe4

Why Choose SecurityCoach?

Your organization is facing an ever-increasing volume of social engineering attacks targeting your users. Your best defense is to develop a strong security culture across your organization that engages your users and reinforces the importance of following your organization's security policies, strengthening your human firewall.

SecurityCoach creates significant time savings for your overburdened SOC team by reducing the volume of alert noise caused by repetitive risky behaviors, allowing the SOC to focus on high-priority threats.

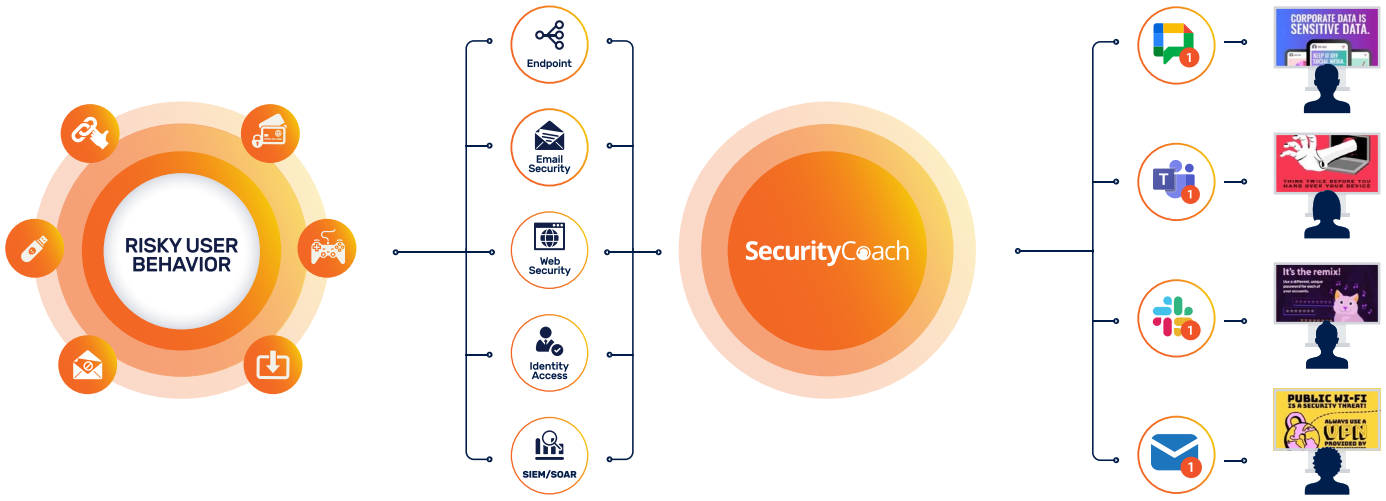
How Does SecurityCoach Work?

SecurityCoach uses standard APIs to quickly and easily integrate with your existing security products from vendors like Microsoft, CrowdStrike, Cisco and many others. Your security stack generates alerts that are then analyzed by SecurityCoach to identify events related to any risky security behavior from your users.

For example, if a user opens an infected email attachment which might spread ransomware in your network, or tries to visit a website with restricted content on their work computer, your security products detect this and create an event alert. SecurityCoach identifies that event and then, via Microsoft Teams, Slack, Google Chat or email, sends a real-time SecurityTip to that user acknowledging that "Hey, this is a security risk and here's why." You can set up coaching campaigns to target risky users based on those events from your network, identity, web security and other vendors within your security stack.

These campaigns enable you to coach your users at the moment the risky behavior occurs, providing real-time feedback and reinforcing the security awareness training campaigns you run today. Using your own security policies as a foundation and assisted by SecurityCoach automation settings, you can easily configure real-time coaching campaigns.

SecurityCoach reinforces the need to follow your organization's security policies, improving user behavior and strengthening your overall security culture.



SecurityCoach Workflow

1. The security stack vendors you integrate with in the KnowBe4 console will monitor for risky activity on your users' devices.
2. Then, alert data is shared with SecurityCoach. SecurityCoach will analyze your detected events and determine which threats provide the best opportunities to coach your users in real time.
3. When risky user behavior is detected, SecurityCoach automatically sends a real-time SecurityTip notification to that user via Microsoft Teams, Slack, Google Chat or email.

KnowBe4

Key Features

Real-Time Coaching

Real-time coaching campaigns allow you to coach your users about risky behavior in real time. When risky activity is detected, your users will receive a coaching notification with a SecurityTip about the activity and how to avoid it in the future.

SecurityTip Notifications

At the moment risky behavior is detected, SecurityCoach sends a real-time SecurityTip directly to that user via Microsoft Teams, Slack, Google Chat or email. These immediate notifications are a powerful enhancement to your security awareness program.

API-Based Integrations

Utilize vendor APIs to quickly and easily integrate with your existing security stack vendors such as Microsoft, Cisco, Netskope, Zscaler and more. Our ecosystem of **technology partnerships** is rapidly expanding to support our customers and strengthen the human firewall.

Built-In Detection Rules

Detection rules specify what risky activity you want to track using the data provided by your integrated security vendors. SecurityCoach recommends detection rules based on the most common security topics in order of priority with Very High and High Risk rules presented first.

Dashboard & Detailed Reporting

The built-in dashboard provides an overall summary of coaching campaigns, detection rules and detected security events. The detailed reports provide insights into your organization's security risks and help track trends in your users' risky activity over time.

SecurityCoach also contributes to your Risk Score calculation so SmartRisk Agent™ can provide actionable data and metrics.

Easy User Mapping

User data from your identity provider or directory is combined with your security event logs to create user mapping rules. With a variety of built-in user mapping rules and the ability to create custom rules, you can easily configure these rules to automatically map users.

Campaign Recommendations

SecurityCoach recommends real-time coaching campaigns best suited for your detection rules. You can select SecurityTips from different categories of risky behavior.

Rule-Based Automation

Based on the rules in your existing security software stack and defined high-risk users or roles, you can configure your real-time coaching campaign to determine the frequency and type of SecurityTip risky users will receive.

Robust SecurityTip Catalog

You can create campaigns using our extensive catalog containing hundreds of SecurityTips, including GIFs and videos, covering 60+ different topics. Enjoy exclusive Inside Man SecurityTip content featuring AJ as he coaches your users in real-time.

Social Engineering Indicators

The SecurityCoach integration with your KnowBe4 Security Awareness Training phishing campaigns gives you the ability to send SecurityTips detailing the Social Engineering Indicators (SEI), or red flags, that your users missed from the exact phishing test they failed.

Powerful Security Integrations

SecurityCoach uses standard APIs to quickly and easily integrate with your existing security products from vendors like CrowdStrike, Microsoft, Cisco, Netskope, Zscaler and more. Our ecosystem of **technology partnerships** is rapidly expanding to support our customers and strengthen your security culture.

To allow SecurityCoach access to your security platforms, you'll set up an integration in your KnowBe4 console. These integrations allow SecurityCoach to track when certain actions are detected. Setting up an integration is a quick and easy process, and we provide integration guides for each vendor on our knowledge base. Once integrated, events and other data from your security platforms will be displayed on your SecurityCoach dashboard.

Endpoint Security

Bitdefender, Carbon Black., CROWDSTRIKE, CYLANCE, Microsoft, Malwarebytes, SentinelOne, SONICWALL, SOPHOS

Identity Access Management

Google, okta

Communications

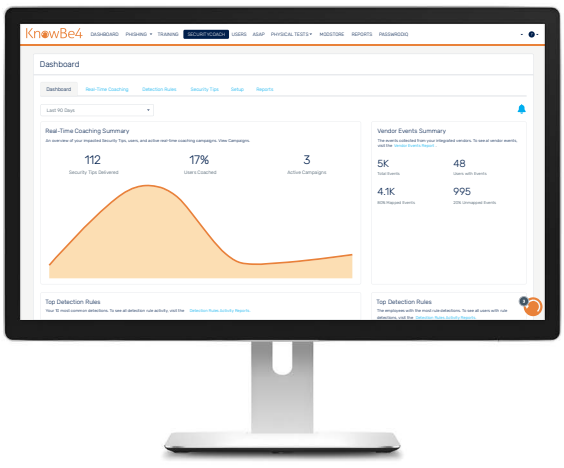
slack, Microsoft Teams, Google Chat

Email Web Security

cisco, CLOUDFLARE, FORTINET, Google, Microsoft, mimecast, netskope, proofpoint, splunk>, zscaler

With a **SecurityCoach Free Preview**, you can integrate your security products to see the volume of risky user behavior.

www.KnowBe4.com/securitycoach-preview



KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com