Real-Time Coaching

Integrations Brief

Real-Time Coaching turns the alerts your security stack generates into in-the-moment coaching when users engage in risky activity. Instead of waiting for training after the fact, Real-Time Coaching delivers a SecurityTip the instant risky action is detected, reinforcing secure behavior while the moment is still fresh.

Real-Time Coaching on third-party risk signals is a core capability of KnowBe4's Security Awareness Training (SAT) Advanced tier. It connects to your existing endpoint, identity, email, web, communication and SOAR/SIEM tools through standard API integrations, so the vendors you've already invested in become another source of coaching triggers. These signals feed into your Risk Score, delivering a clearer, more accurate view of risk across your environment.

Endpoint Security

These integrations connect Real-Time Coaching to your endpoint detection and response tools, turning malware, ransomware and device-policy alerts into coaching opportunities the moment risky activity is detected.

Bitdefender GravityZone

Coach users when **Bitdefender** Gravity Zone AV flags viruses, malware or other endpoint threats.

Malwarebytes

Turn **Malwarebytes** threat detection alerts into targeted SecurityTips when users encounter malware, spyware and adware.

Carbon Black.

Stay on top of malware, adware and other endpoint threats detected by **Carbon Black** and turn risks into teachable moments.

Microsoft

Turn **Defender** for Endpoint's malware and exploit detections into contextual coaching so employees learn from the threats they trigger.

CODE42

Catch risky data security threats like risky data movement, cloud sync and removable media with **Code42**'s Incydr and coach users on safe data handling.

SentinelOne

Leverage **SentinelOne**'s security data for endpoint threats, malware and more to deliver real-time coaching moments that reinforce safe device behavior.

CROWDSTRIKE

Catch **Falcon**-detected threats and risky endpoint activity and turn them into instant coaching moments.

SONICWALL

Trigger coaching on risky browsing and endpoint policy noncompliance when you integrate **SonicWall** Capture Client with KnowBe4.

CYLANCE

Coach users on risky endpoint actions the moment **Cylance**'s AI-driven driven detections flag potentially unwanted programs or policy violations.

SOPHOS

Coach users in the moment when **Sophos** detects unauthorized devices or potentially unwanted programs on your network.

Benefits and Outcomes

- Detected threat events become a coaching opportunity automatically, with no manual follow-up from IT or security teams.
- Employees build safer habits, reducing repeat incidents and strengthening your security culture.
- Measurable reduction in risk and improved comprehension and retention of your security awareness training, best practices and established security policies.
- Time saved for SOC analysts through automation and reduced alert noise.

Use Case Examples

Malware Avoidance

When your EDR tools detect malware, Real-Time Coaching maps the malware to a specific user and sends them a targeted coaching message on avoiding malware.

Catch Data Exfiltration Attempts

Removable media or cloud-sync activity flagged by your endpoint security signals a potential data-loss event. Real-Time Coaching intervenes before the behavior becomes habitual.

Identity and Access Management

These integrations tap into your identity providers' risk signals including leaked credentials, risky sign-ins and suspicious account activity, so your users are coached the moment their identity is put at risk.

Coach users on identity risk the moment it happens, using **Google** IAM audit-log signals like leaked passwords and account security events.

Turn **Entra ID**'s risky sign in and leaked-credential alerts into real-time coaching that reinforces safe authentication habits.

Leverage **Okta** identity protection alerts like suspicious logins and account risk, and coach users on credential hygiene when risks are identified.

Benefits and Outcomes

- Faster behavior change around leading causes of account compromise such as password sharing and credential reuse.
- Measurable reduction in risk and stronger security culture across your organization.
- Consistent identity risk education and improved retention of your security awareness training, best practices and established security policies.
- Time saved for SOC analysts and reduced alert noise caused by users repeating risky behaviors.

Use Case Examples

Credential Safety

When your IAM solutions flags a leaked password or suspicious logins, coach the affected user with best practices on authentication and credential safety in the moment.

Malicious Activity

When your IAM detects activity from a malicious IP address, Real-Time Coaching can intervene and guide the user on safeguarding their identity from malicious actors.

Communication

These integrations meet employees where they already work, delivering SecurityTips through the everyday communication channels people actually check – turning security coaching into a natural part of the workday instead of an email that gets ignored.

slack

Deliver real-time SecurityTips directly in **Slack**, so coaching lands in the channel employees are already active in.

Reach users in **Google Chat**, so no one misses a teachable moment wherever they communicate.

Microsoft

Send instant coaching directly into **Microsoft Teams** for immediate visibility.

Benefits and Outcomes

- Nearly 3 out of 4 users don't repeat a mistake after a single Real-Time Coaching message, and coaching messages in communication tools like Slack get responses 4x more often than email.
- Consistent security culture reinforcement across your organization regardless of which communication platform a team or department uses.
- Better long-term retention of the lesson and less coaching fatigue users can experience from email reminders.
- Time saved for SOC analysts and reduced alert noise caused by users repeating risky behaviors.

Use Case Examples

Coaching Nudges, Not a Lecture

A short, contextual SecurityTip delivered in channel right after the risky actions occurs drives better behavior change than a formal notice after the fact.

Coaching Where Attention Already Is

When risky behavior is detected, coaching is delivered in the channels employees already use so they don't miss or ignore them.

Email and Web Security

These integrations leverage email and web safety monitoring such as malicious email alerts, DLP violations and risky URL or web-category detections to send real-time SecurityTips to users the moment they put themselves, and your organization, at risk.

Coach users across both email and web risk by combining **Cisco** Secure Email's malware, phishing and DLP detections with Cisco Umbrella's web and DNS-based threat alerts.

Turn **Mimecast**'s email detection alerts into real-time coaching, closing the gap between a risky email interaction and the lesson that prevents the next one.

Coach users across the full web and email surface leveraging **Cloudflare** Area 1's email threat detection and Cloudflare Zero Trust's risky-site and malware download alerts.

Watch for policy violations, DLP alerts, and suspicious activity through **Netskope** and coach users the moment risk is detected.

Coach users the moment they attempt to reach a risky or malicious site using **FortiGate** Cloud's web URL detection alerts.

Turn **Proofpoint**'s malicious email alerts into immediate coaching that reinforces safe email habits when users make a risky click or open.

Reinforce secure email and file-sharing behavior using Gmail's audit-log signals and **Google** Drive's external-sharing alerts.

Turn **TrendAI**'s email and web threat detections into real-time coaching that builds secure behavior.

Coach users off one pipeline that combines **Microsoft 365**'s malicious-email and DLP alerts, Defender for Cloud Apps' cloud risk signals and Edge for Business's risky-site detections.

Monitor **Zscaler** web logs for risky browsing and data-sharing activity and deliver coaching the moment a violation occurs.

Benefits and Outcomes

- Fewer repeat mistakes from the same users and a measurable reduction in risk and phishing engagement over time.
- Safer browsing habits that reduce reliance on blocking rules alone and lower your risk of malware delivery.
- Significant additional value from your existing investments in email and web security tools.
- Stronger data-handling habits and fewer accidental exposure incidents across the vast email and web attack surface.

Use Case Examples

Address Phishing Risk

When your email security tools flag a malicious email a user interacted with, they receive a SecurityTip on avoiding phishing, tying training directly to their own behavior.

Correct Risky Browsing

When your web security tools detect a visit to a risky or malicious site, or a web-category policy violation, they receive immediate coaching rather than a blocked-page message with no context.

SOAR/SIEM

These integrations let Real-Time Coaching ingest detection data through your existing security data pipeline, so organizations standardized on a SIEM can extend coaching without a separate direct integration for every vendor.

splunk>

Pull supported security vendor data through **Splunk**, so Splunk-connected detection sources can trigger coaching.

Benefits and Outcomes

- Even broader detection coverage with less integration overhead for your team.
- A more sustainable, lower-maintenance path to expanding risk coaching over time.
- Measurable reduction in risk and stronger overall security culture.
- Significant additional value from your existing security investments.

Use Case Examples

One Pipeline, Many Vendors

Security teams already centralizing alerts in SOAR/SIEM tools can route that data into Real-Time Coaching without creating individual connections for each applicable vendor.

Scale Coaching

As new detection sources are onboarded into your SOAR/SIEM, they can extend coaching coverage alongside your existing security investments.

Bringing It Together

Real-Time Coaching's value compounds with every integration you add: more detection sources means more data to drive Risk Score, more threat coverage, and more precise and timely coaching delivered through the channels employees already use. Whether your goal is to reduce malware incidents, tighten identity hygiene, or to get more out of the tools you've already deployed, Real-Time Coaching turns your existing security investments into a core part of your security awareness program with no additional agents to deploy and no extra burden on your users.

Learn More About Real-Time Coaching

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