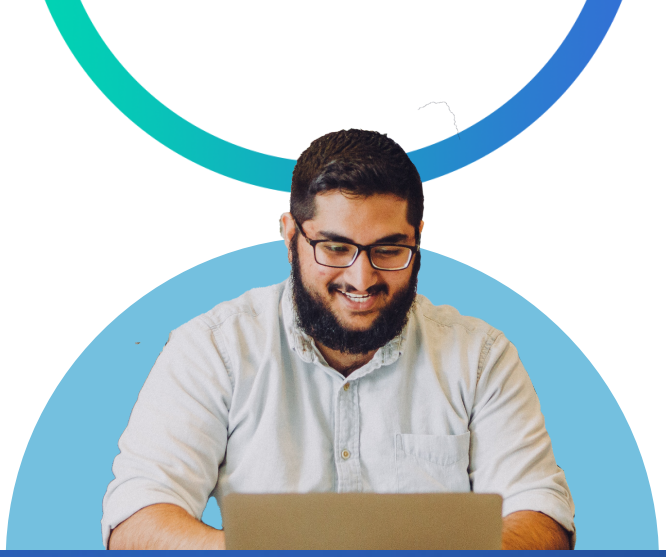
livingsecurity

Transform Human Risk into a Strong Security Culture and Proactive Defense With Human Risk Management



Today, 85% of cybersecurity breaches involve a human element.

However, because the human element is incredibly unpredictable and difficult to manage, of the 0.3-0.8% of company revenue spent on cybersecurity the majority goes to technology.

Top Challenges CISOs and Security Leaders tell us they face and don't have clear answers

1. How do we measure and quantify the human factor of cybersecurity risk?
2. What human behaviors are our biggest cybersecurity risks and how are we addressing them?
3. How do we show ROI and evolve our program to effectively address emerging human risks?

INTRODUCING UNIFY INSIGHTS

Unify Insights is the first module of the Unify Human Risk Management Platform that leverages your existing employee behavioral data to deliver insights to security leaders so they can make informed, data driven decisions on how to prioritize resources and proactively decrease employee risk across an organization. This type of quantifiable human risk management delivers board, executive, manager, and even end-user levels of reporting that drives transformation of security maturity and arms you with the tools and knowledge necessary to actively defend your organization.

EMPOWER YOUR PEOPLE AS A PROACTIVE DEFENSE

Your employees are the key to identifying potential threats and incidents that bypass technology controls. At Living Security, we believe your employees can be your greatest asset, taking vigilant actions rather than being susceptible to threats, decreasing your overall risk. Altering behavior and empowering employees to be the most effective defense against cyber threats requires a data-centric, analysis driven approach. By analyzing data from technologies that your organization already owns and layering that with an understanding of processes that are in place, security leaders will finally be able to understand why employees engage in certain behaviors, effectively drive lasting change in those behaviors, and accurately report on the organization's risk-reduction and progress towards a more security-minded culture.

KEY ELEMENTS OF THE HUMAN RISK MANAGEMENT SOLUTION

Unify Insights, combined with Living Security's industry leading Training, Teams, and Phishing provides all of the capabilities needed to fully implement Human Risk Management within your organization. These components allow the enterprise to manage the human risk and provide the content and engagement activities to provide focused and relevant training to specific groups of employees.

QUANTIFY RISK WITH ACTIONABLE INSIGHTS:
Aggregate the data from your various siloed security systems and actual human events to get clear and comprehensive insights to quantify your cybersecurity human risks including the who, what, and where at any given moment.

Get answers:

- What does our cybersecurity human risk picture look like?
- How does our current risk align with our tolerance level?
- Where is our risk high that we need to prioritize actions?

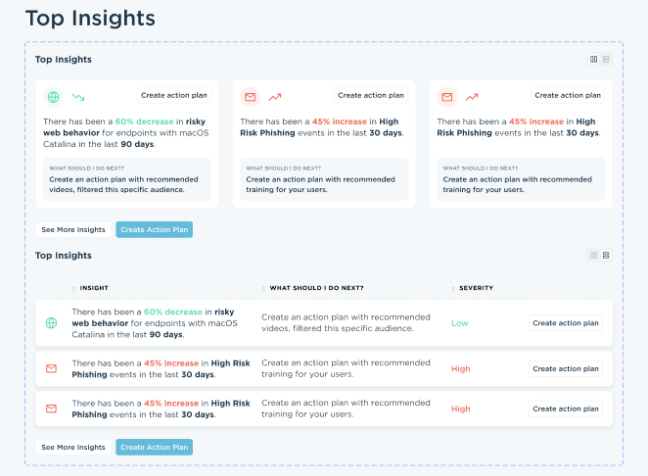
Unify in Action: Engage the Business in a Risk Focused Conversation

Overview: Uplevel the security conversation by putting it in business terms your Directors, VPs and Senior Executives understand by leveraging Unify's grouping and segment scorecards. Understanding who is most at risk and what behaviors are contributing allows security to partner with the business to create change.

By ranking groups, we can create a natural desire to improve and that alignment will start a culture change when it comes to security across the business.

DETECT BEHAVIORAL GAPS & TARGET RESPONSES: Activities (risky or vigilant) are aggregated by department, location, and group allowing you to identify themes that lead you to the root cause of behaviors so you can prioritize the most effective responses.

Automate targeted training interventions or positive reinforcement with real time communications to engage employees so they more clearly understand the impact of their behaviors and make lasting changes.



Get answers:

- Which behaviors are most impactful to organizational risk, require further investigation, or would benefit from an adjustment of controls or targeted training?
- What positive behaviors should we reward and reinforce?
- Which risky behavior remediation actions are proving to be most effective?
- What changes have we made to drive improvements?
- How much have we improved and where should we focus next?

Unify in Action: Routinely Test Users Most Likely to be Successfully Phished

Overview: Ensure you are actively tracking your risk for employees who based on their role, tenure at the organization, and other factors are at a higher risk for phishing attempts. With Unify, you can recognize this group, track their behaviors and send them tailored training that is automatically adjusted as their behaviors and skills become more mature.

Data Sources:

- Active Directory
- HR System
- LMS Training Data
- Email Security
- Phishing Simulation
- OSINT

Details:

- Use characteristics about the user to identify which users are appealing to attackers (Active Directory & HR System)
- Identify the user's current proficiency in phishing (LMS Training Data & Phishing Simulation)
- Understand what phishing types and tactics users struggle with (Phishing Simulation)
- Understand which users can be identified by an attacker or have information that is exposed externally (OSINT)
- Analyze the volume of spam and phishing attacks received by the user (Email Security)
- Correlate spam/phishing volume received to user's overall url and attachment click rates)
- Automate Phishing simulation frequency for the user. (Phishing Simulation)

Unify in Action: Prioritize Patching Based on User Risk

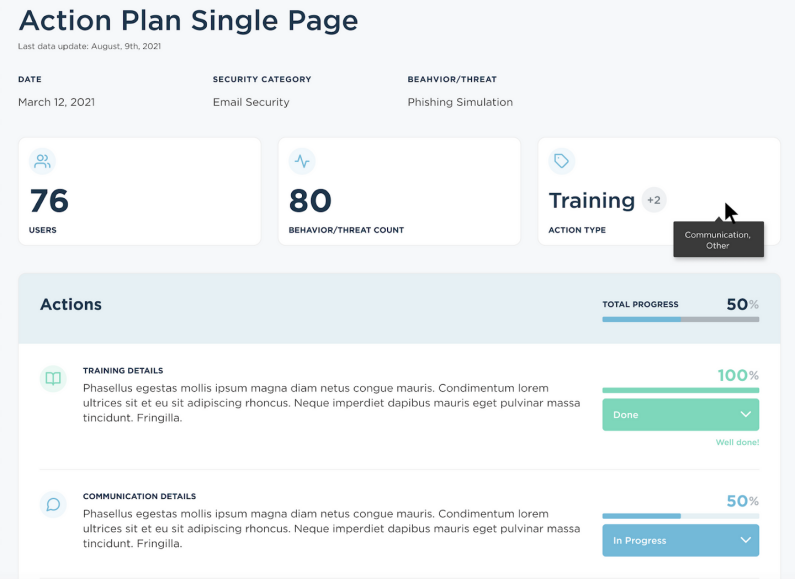
Overview: Patching is an ongoing battle with more products and new exploits, prioritizing these efforts is necessary. Rather than evaluating which patches to execute first based on general severity of exposure, with Unify you can bring your security team, patching team and security awareness teams together to ensure the right vulnerabilities are identified and protected first. Identify your riskiest users and critical vulnerabilities in your systems to understand your biggest exposure from both a technical and human risk perspective.

Details:

- Identify user's overall behavior risk scores, primarily in Email and Web
- Identify CVEs that would most likely be exploited due to user's behavior
- Prioritize patching based on CVE severity and user risk level

Data Sources:

- Vulnerability Scanners
- Patch Management
- Email Security
- Phishing Simulation
- Web Filtering / Proxy



MEASURABLE RESULTS: Use the results from the program actions you've implemented to evolve your security program, making more informed decisions on resource prioritization, spend and proving your impact on organizational cybersecurity risk for executive and board level conversations and reporting.

Get answers:

- How has behavior changed with the implementation of our latest program or technology?
- Are we reducing our cybersecurity incidents?
- What is the ROI of our security efforts?

Unify in Action: Demonstrate Changes with Data

Phishing remains to be one of the most frequently used social engineering methods among attackers. With Unify you can address phishing more tactically.

Using user characteristics from your data sources like active directory, HR platforms, open-source intelligence and correlating that with risky email behaviors, phishing reporting frequency, and training scores, Unify can show the percent increase in appealing phishing targets with risky email behaviors.

Leveraging Unify's action plan functionality, you can respond quickly by automatically blocking these users from specific domains, assigning short training modules relevant to each user's risky email behaviors, and trigger a targeted phishing simulation containing tactics that the user has struggled with in the past.

The action plan metrics then allow you to monitor if the user's behaviors have changed. To take things a step further, use Unify's actions plans to applaud users on their effort through an internal chat message or email including the improvement metrics and how their vigilant actions benefit the organization.

READY TO UPGRADE HOW YOU'RE MANAGING YOUR CYBERSECURITY RISK?

Drive your cybersecurity program forward with visibility into your organization's human risk with data and insights to find and respond to attacks and enhance your controls. Get started measuring and improving your employees' security behaviors today.

Contact info@livingsecurity.com or visit www.LivingSecurity.com for more information