SOLUTION BRIEF

Bitdefender

HUMAN RISK ANALYTICS

Human Risk Analytics and the Road to Zero-Trust Computing

www.bitdefender.com

Why do organizations keep getting breached by the same old tricks?

Why do companies continue to experience devastating cyber-breaches despite spending hundreds of millions on security tools and services? And why do the same attack vectors—email, web, and USB—continue to dominate in attack patterns? Because they work. They target human frailties, which no software solution can solve. Our employees continue to be our weakest link—ruled by laziness, habit, routine, and complacency—behaviors that cumulatively create outsized organizational risk.

Remote workers each access approximately 31 malware sites per month, plus 10 phishing domains. That equates to one malware site every day, and one phishing domain every 3 days

Human beings make mistakes. To small and large extent, most of us make them every day. Mistakes include errors in judgment, working to fast, multitasking, and working on small screens where you can't "hover" the mouse to see the complete sender's email address or "real" destination masked behind the shortened URL. Each of these activities contributes to user-centric errors that increase risk in the aggregate. Most mistakes are inconsequential, but some can lead to devastating adverse business consequences.

The problem is not getting better … it's getting worse

Despite user training, the same phishing attacks seem to work year after year. Employees typically access 59 risky URLs per week, or 8.5 per day, according to new data. That's more than once per hour in an eight-hour workday. Depending on their knowledge of the threat landscape, corporate employees can be as dangerous as an external cyberattack on the company – especially if those employees are working remotely. Users also continue to login to unencrypted websites, passing their credentials in plaintext over the open Internet for anyone to see. They also reuse passwords far too liberally and rely on old passwords that rarely get changed.

According to a Bitdefender survey of 6,724 IT professionals across the globe, 86% of businesses agree that cyberattacks have been on the rise during the COVID-19 pandemic. More than one in three (34%) say they fear employees are feeling more relaxed about security issues because of their surroundings, while others say that employees are not following protocol, especially in identifying and flagging suspicious activity. IoT as an attack vector is also up by 38%, underscoring the dangers posed by our convenient smart devices sitting on the same network as the corporate laptop and unprotected by a corporate security stack.

What can we do to minimize the human risk?

Chalk it up to human nature. What can be done? Smart thinkers at Bitdefender pondered this problem and came up with a novel solution that addresses human shortcomings by assessing and measuring specific risky activities and behaviors that create significant business exposure.

So, what do we measure to assess human risk? Specifically, we look at the following risk factors:

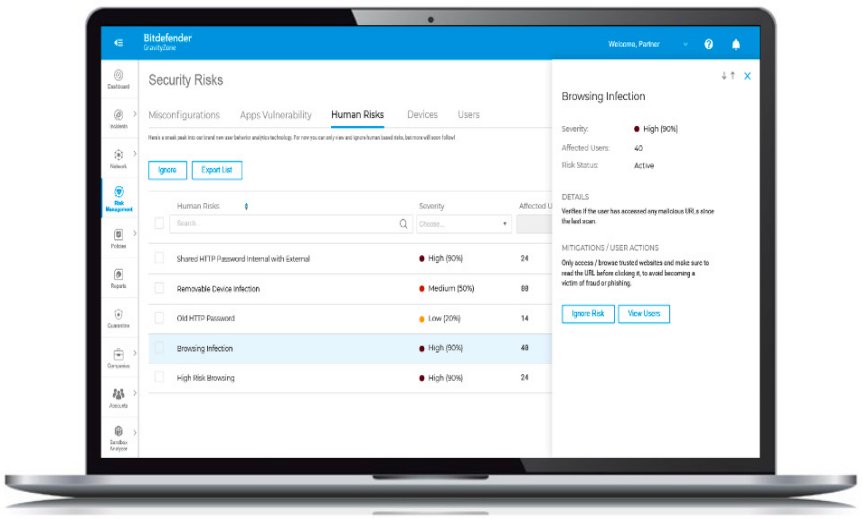
- Where they browse
- What files they open
- What file locations they access
- How and where they login
- Password hygiene and reuse

BROWSING	FILE SOURCES	FILE LOCATIONS	WEBSITE LOGINS	PASSWORDS
Risky websites Phishing links	Downloads Attachments	USB drives Network shares	Internal / External HTTP / HTTPS	Old Shared

How human risk analytics improves security and reduces risk

Users add risk every time they open an email, click a link, or download a file. Every interaction with the outside world inherently involves taking on some element of added risk. Detection will never be 100% effective—that's why we have EDR, Network Traffic Analytics, and SIEM tools to collect and analyze logs. Visibility is essential, as you can't gauge exposure or assess risks if you can't see the underlying risky behaviors that create the opportunity for breaches to take place.

Most users mean well and are reasonably conscientious online. Insider threats are probably not your biggest problem. Your users likely are not deliberately acting stupid, careless, or reckless—they just don't know any better, despite years of security awareness training. It all comes down to human nature—how to manage it to drive successful business outcomes. Our objective is to correct the errant behavior, not to punish the individuals involved, as they don't realize they are acting risky or doing anything wrong. Hold your people accountable through visibility and specificity so they see that their everyday online behaviors are putting the business at risk.



Human risks include where they browse, what files they open, which sources, and how they login

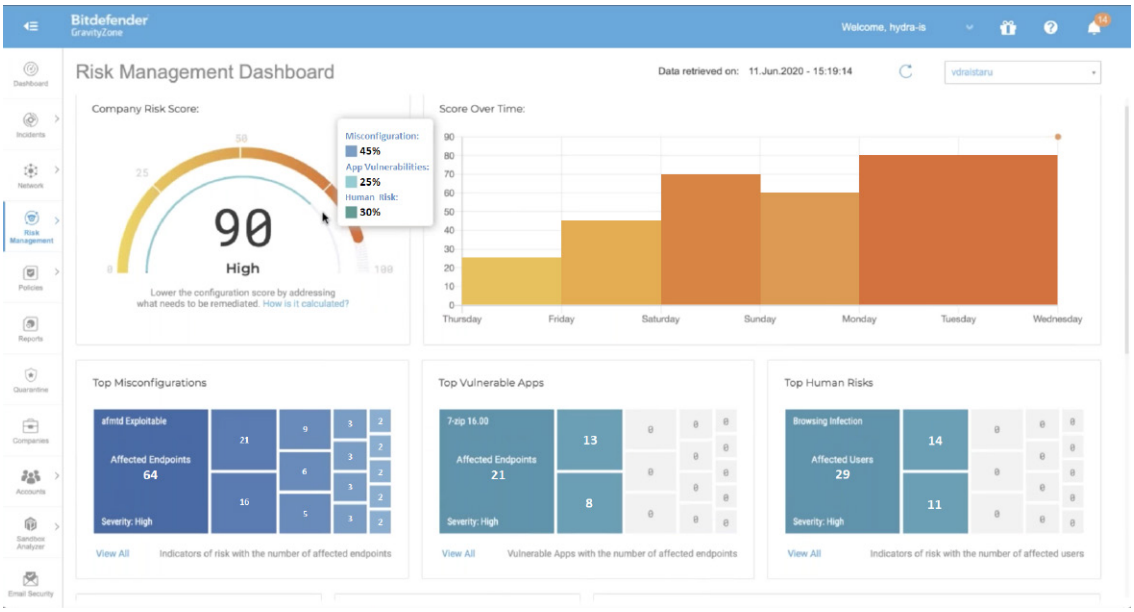
Analyzing human risks improves overall detection and response

Human Risk Analytics provides critical input to a long-running blind spot, your users. It gives a detailed looking into what they do and where and how they do it, while preserving user autonomy to perform their jobs and retaining a measure of privacy for their actions. HRA provides one more set of key risk factors to be evaluated in an integrated and holistic manner. In this way, human risk is just as important as application risk or device risk.

Organizations can look at risk management as an equation with the following variable factors:

Total Risk = Misconfigurations + Software Vulnerabilities + Human Risks

Continuous assessment and measurement are needed for each of these factors. This requires sustained attention and effort to stay on top of the security risk elements, very much in the way that EDR requires skilled analysts to stay on top of the incoming alerts. Much can be done to reduce misconfigurations and software vulnerabilities through automated configuration and patching, however there is no patch to "fix" human frailties or alter their ingrained habits. Organizations can, however, shine a light on these behaviors, identify the most egregious violators, and then take corrective actions to improve user behaviors over time.



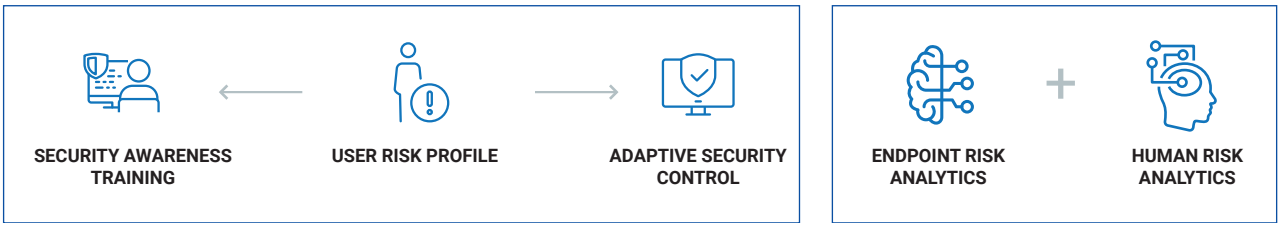
Human risks often comprise a significant portion of your overall exposure

Aligning protection capabilities to a strategic defensive framework

No single vendor can provide a complete security solution. With dozens of recognized security categories, multi-vendor implementations are required to cover each of the areas of risk and minimize exposure. It is critical that security solution providers align their features and capabilities to a strategic defensive framework to facilitate

common understanding, promote interoperability, reduce overlaps, and eliminate coverage gaps. The growth of vendor capabilities must be strategic and part of a larger purpose, randomly designed or haphazardly released without supporting and furthering a larger purpose. Aligning product releases to a well-defined security model ensures that new features meet this important threshold.

One powerful strategic security model is **zero-trust computing (ZTC)**. Human Risk Analytics furthers ZTC by identifying risky users based on their behaviors, providing critical information to business and security teams that they can utilize to better secure their systems and networks.



Human risks should be baselined, evaluated and managed on an equal footing with endpoint risks

A prominent ZTC model is **Forrester's Zero-Trust eXtended Framework (ZTX)**. Its highlights:

- **Zero-Trust Data** – Secure, manage, and classify data, encrypt data in transit and at rest
- **Zero-Trust Networks** – Segment, isolate, and control the network
- **Zero-Trust People** – Limit and enforce user access, authenticate and monitor access
- **Zero-Trust Workloads** – Secure the entire application stack from app layer through HV/VM
- **Zero-Trust Devices** – Isolate, secure, and control every device on the network at all times
- **Visibility & Analytics** – Network awareness to accurately observe threats & orient defenses
- **Automation & Orchestration** – Increase analyst capacity, shorten incident response times

Human Risk Analytics supports the **Zero-Trust People** tier of the Forrester ZTX Framework. User trust should be *earned* and *retained*, rather than *assumed* in perpetuity based simply on a user's job function, location, or device. Users that behave safely and responsibly may be granted more access privileges than users who behave carelessly or recklessly. Organizations that are properly informed of these risky behaviors can apply corrective actions to their users, using either a carrot (greater access) or a stick (reduced access) as motivation to reinforce desired behavioral patterns.

The case for including HRA in evolving ZTC models

Zero-trust computing models are incomplete without Human Risk Analytics. Access rights are important, but how people use those rights is just as critical. Based on their behavior, access rights can and should be reviewed and adjusted accordingly to minimize organizational risk while maximizing the ability for the user to do their job. As part of Zero-Trust People, ZTC models would extend beyond simply granting initial access to company content—intellectual property, proprietary information, and personally-identifiable information)—and would also now extend to external/ untrusted content that you or your company do not control, all on a reviewable (non-assumed, non-permanent) basis.

These same continuing "review and evaluate" principles could apply in every context where users access content based on their demonstrated behaviors and responsible use of business computing resources:

- Web / Cloud – Remote logins and untrusted file downloads
- Network – Shared file access, data in motion
- Datacenter – Proprietary data access
- Email – Attachment downloads
- Mobile – Remote access on devices with less protection
- Portable Storage – Unknown, risky file access

Bitdefender Integrated Solution mapped to the ZTX Framework

Bitdefender has developed an innovative integrated solution portfolio designed to support zero-trust computing in numerous aspects. Mapping specifically to Forrester ZTX elements, the Bitdefender portfolio contributes to ZTC as follows:

Zero Trust				
Data	**Networks**	**People**	**Workloads**	**Devices**
Full-Disk Encryption	Network Attack Defense	Human Risk Analytics	Application Control	Device Control
Endpoint IDS	Automated VM Inventory	Users and Groups	Cloud Workload Protection	Device Risk Analytics
Endpoint Firewall	Network Traffic Security Analytics	Granular Security Profiles	Hypervisor Introspection	Patch Management

Visibility & Analytics	Automation & Orchestration
Risk Management Dashboard	Managed Detection and Response
Network Traffic Security Analytics	API-Driven Solution Portfolio
Managed Detection and Response	SIEM/SOC Support

Vendors who claim ZTC should support human risk analytics

Zero-trust computing demands continuous assessment and adjustment of security controls pertaining to the intersection of user behaviors with their associated devices, networks, datacenters, and cloud storage locations. The key commonality is how the user makes use of the resources through their choices and behaviors. Users will always be the weakest link, with so many changes to business technology coming so quickly and demanding new ways of working and collaboration. There will always be windows of opportunity for attackers to exploit the human element through social engineering and taking advantage of poor security habits.

This is no longer just a technology problem—it's also a people problem, but technology can help by shining a light on potentially risky activities and providing organizations with the tools necessary to assess behaviors and achieve

continuous improvement. Human Risk Analytics is the next step toward zero-trust computing. Bitdefender encourages the security industry and the analyst community to support HRA by incorporating it into the ZTC models and demanding that security vendors further HRA in their own solutions.

WHY BITDEFENDER?

UNDISPUTED INNOVATION LEADER.

38% of all cybersecurity vendors worldwide integrated at least one Bitdefender technology. Present in 150 countries.

WORLD'S FIRST END-TO-END BREACH AVOIDANCE

The first security solution to unify hardening, prevention, detection and response across endpoint, network and cloud.

#1 RANKED SECURITY. AWARDED ACROSS THE BOARD.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER RECOMMENDED NSS

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its numberone-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-CZ-SolutionBrief-HRA-creat4754-en_EN
08/28/20September 7, 2020 8:04 am09/07/20