Why You Should Update to Risk-Adaptive Data Protection

What is Risk-Adaptive Protection?

Risk-Adaptive Protection (RAP) is a security solution that alerts organizations of risky behavior, this means adjusting how they enforce data security policies based on insider risky behaviors.

A company's data is its greatest asset! Data leakage happens through several avenues, some breaches are so powerful they can overwhelm some of the protections in place. Learn how data breaches happen and how Risk Adaptive Protection prevents catastrophe.

Why Risk-Adaptive Protection?

Human behavior causes data breaches, Risk-Adaptive Protection uses behavior-based security to reduce the risk. Be sure you're aware of insider threats so you can protect your organization.

86%

OF WEB APPLICATION BREACHES **INVOLVE STOLEN CREDENTIALS**

Stolen credentials lead to nefarious behavior, ensure your data's security with Risk-Adaptive Protection.

50%

OF ALL DATA BREACHES ARE DUE TO RISKY INSIDER BEHAVIOR

Whether accidental or intentional, data breaches occur.

74%

OF ALL DATA BREACHES **INVOLVE PEOPLE**

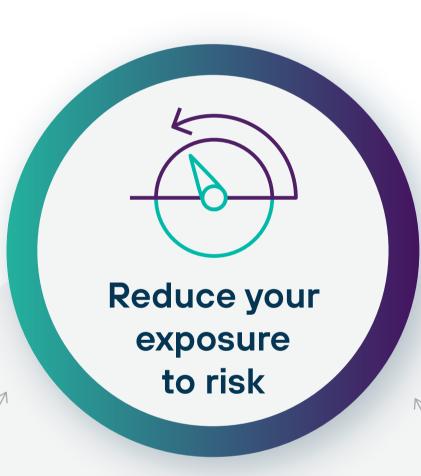
Security isn't as simple as securing devices, behavior-based security is crucial.

Citation: Verizon Data Breach Investigations Report, 2023

Benefits of Switching to Risk-Adaptive Protection

MEAN TIME TO DETECT

- Decrease Mean Time to Detect through continuous risk evaluation.
- Anticipate malicious activity.



MEAN TIME TO RESPOND

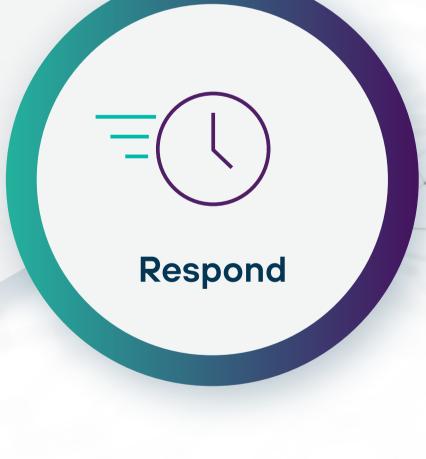
- Decrease Mean Time to Respond through risk-adaptive enforcement.
- Obtain meaningful visibility.
- Understand entity history.

Indicators of Compromise (IoCs) to Indicators of Behavior (IoBs). Focus on risk rather than

Shift detection paradigm from



event triage.



DETECTION Decrease detection time through continuous risk evaluation.

FASTER

Anticipate malicious activity.

RESPONSE Decrease response time through risk-adaptive enforcement.

FASTER

Obtain meaningful visibility.

Understand entity history.

RISK-ADAPTIVE PROTECTION Use 130+ indicators of behavior to systematically define user intent.

AUTOMATE DATA SECURITY WITH

Apply a risk score of 0-100 to identify

incidents that need further analysis.

Enforce various actions based on risk score, from audit to blocking.

TALK TO AN EXPERT

About Forcepoint Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero

Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on <u>www.forcepoint.com</u>, <u>Twitter</u> and Linkedln.

All other trademarks used in this document are the property of their respective owners.