Risk-Adaptive Data Protection

How focusing on risky behavior enables innovation and protects data everywhere

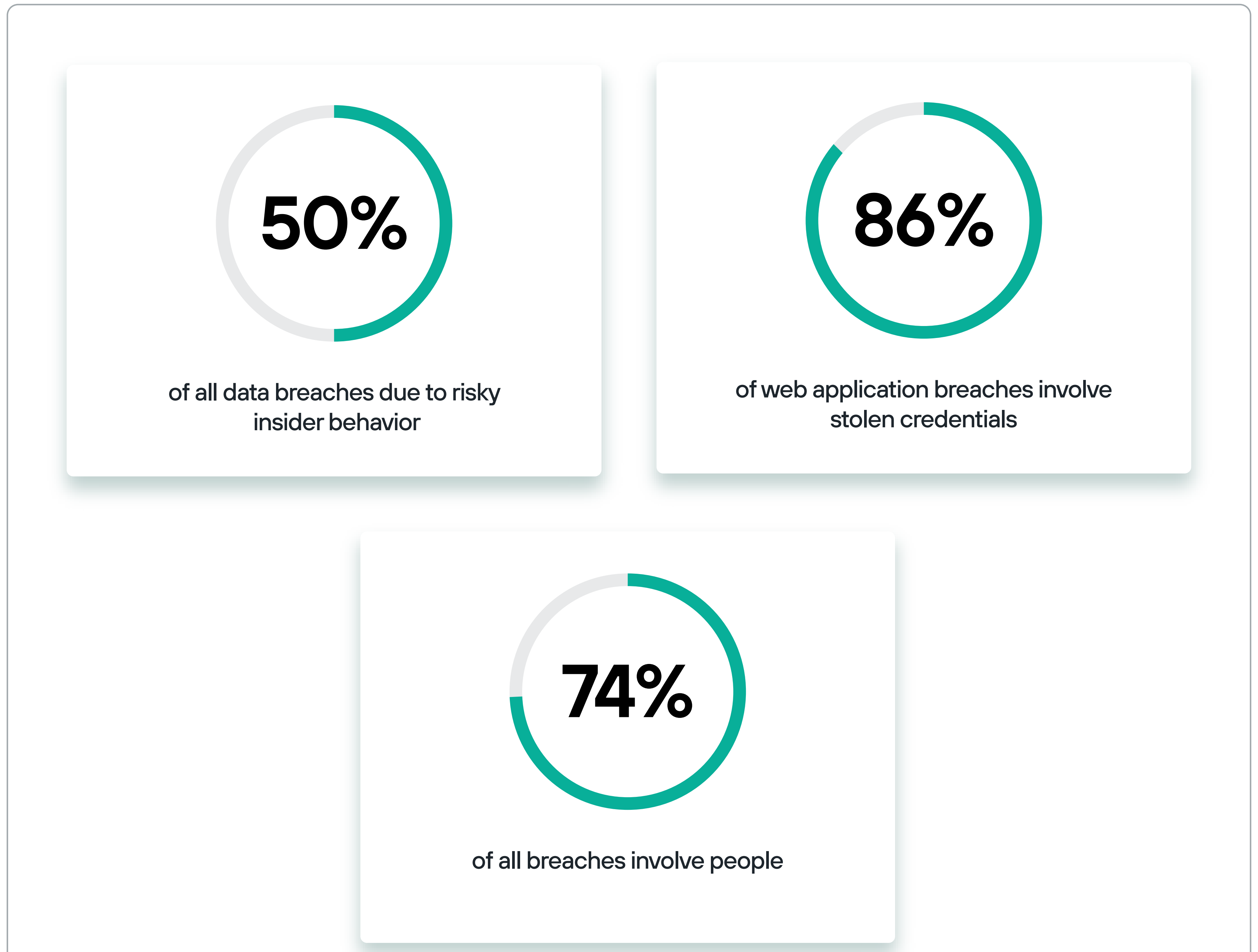
Understanding Risk in the Era of Data Proliferation

Your company's data isn't merely valuable, it's the catalyst for growth and innovation.

As data becomes increasingly ingrained in every aspect of your organization, its critical nature also amplifies the corporate risk. Data can leave through many doors, ranging from uploads to websites and cloud applications to the use of personal devices like USB drives and Bluetooth devices, presenting formidable challenges for security teams.

Understanding the exact whereabouts of all data, who has access to it, and the sensitivity of the information within each file is an immense undertaking for security teams. While implementing blanket protection policies may appear to offer a solution, complexities emerge when specific access needs clash with security requirements. This is especially true across diverse device types and user roles, particularly in scenarios involving contractors and partners who may not be readily visible to security teams.

At its core, cybersecurity is synonymous with data security. We need a new security model that upholds Zero Trust principles, continuously monitors risk, and dynamically adapts enforcement measures based on risk levels to prevent data breaches.



50% of all data breaches due to risky insider behavior

86% of web application breaches involve stolen credentials

74% of all breaches involve people

Verizon Data Breach Investigations Report 2023

Preventing Breaches without Stifling Business

Why resign ourselves to the inevitability of breaches? While traditional data protection offers some visibility into an organization's data activity, it lacks the necessary context behind user interactions. Consequently, the system struggles to differentiate between legitimate and risky data usage, triggering excessive alerts that overwhelm IT Security.

You're left with two unappealing choices.

- Option A:
  Apply restrictive policies that block productivity, increase IT investigation workloads, and prompt employees to try circumventing security, or

- Option B:
  Run in audit mode for minimal policy enforcement to facilitate productivity, enable passive monitoring of data security, and serve as a forensic tool in the event of a data breach. It is important to note people who actively block threats report less data breaches.

> Option B, often perceived as the lesser of two evils, involves passive, reactive security measures. Many believe it's easier to clean up after security incidents than to prevent them entirely. However, the superior strategy is to automate highly active highly accurate enforcement based on understanding risk.

The Breakthrough:

Placing Behavior at the Center of Data Security

The solution is behavior-based data security, which prioritizes understanding and quantifying risk to enable proactive responses. Focusing on risky user activity empowers you to more effectively secure data wherever it's accessed--at headquarters, remote locations, or in the cloud. This behavior-led approach can both protect sensitive information and fuel innovation.

Upgrade to Risk-based Data Protection

Companies make strategic decisions by understanding their risks, quantifying them, balancing their tolerance levels, and defining their processes for risk mitigation. To achieve this, IT and security teams need the tools and capabilities to discern where, how, and by whom data is used. This comprehensive understanding provides the context needed to prioritize and respond effectively to risks.

Security teams require best-in-class capabilities to:

- → Understand the baseline for normal data usage, access, and location to provide context for measuring anomalous or risky data usage
- → Connect seemingly disparate data interactions to build a risk profile to quantify, rank, and prioritize mitigation
- → Apply adaptive policies that focus security where and when risk increases, allowing more data freedom where risk is low
- → React automatically to high-level alerts and block interaction when risk becomes critical and a breach perceived to be imminent

This dramatically reduces false positives and false negatives that cause friction, and by doing so you can boost individual productivity.

Put another way, intelligent behavior-based data security that automates policy enforcement allows you to trust and enable your employees.

Risk-Adaptive Data Protection:

Automated Zero Trust Data Security

What is behavior-based data security?

Behavior-based data security integrates behavior analytics with data loss prevention (DLP) to provide proactive dynamic policies and enforcement. Understanding behavior allows you to decide when to trust a user's access to and interaction with data–or when to block it.

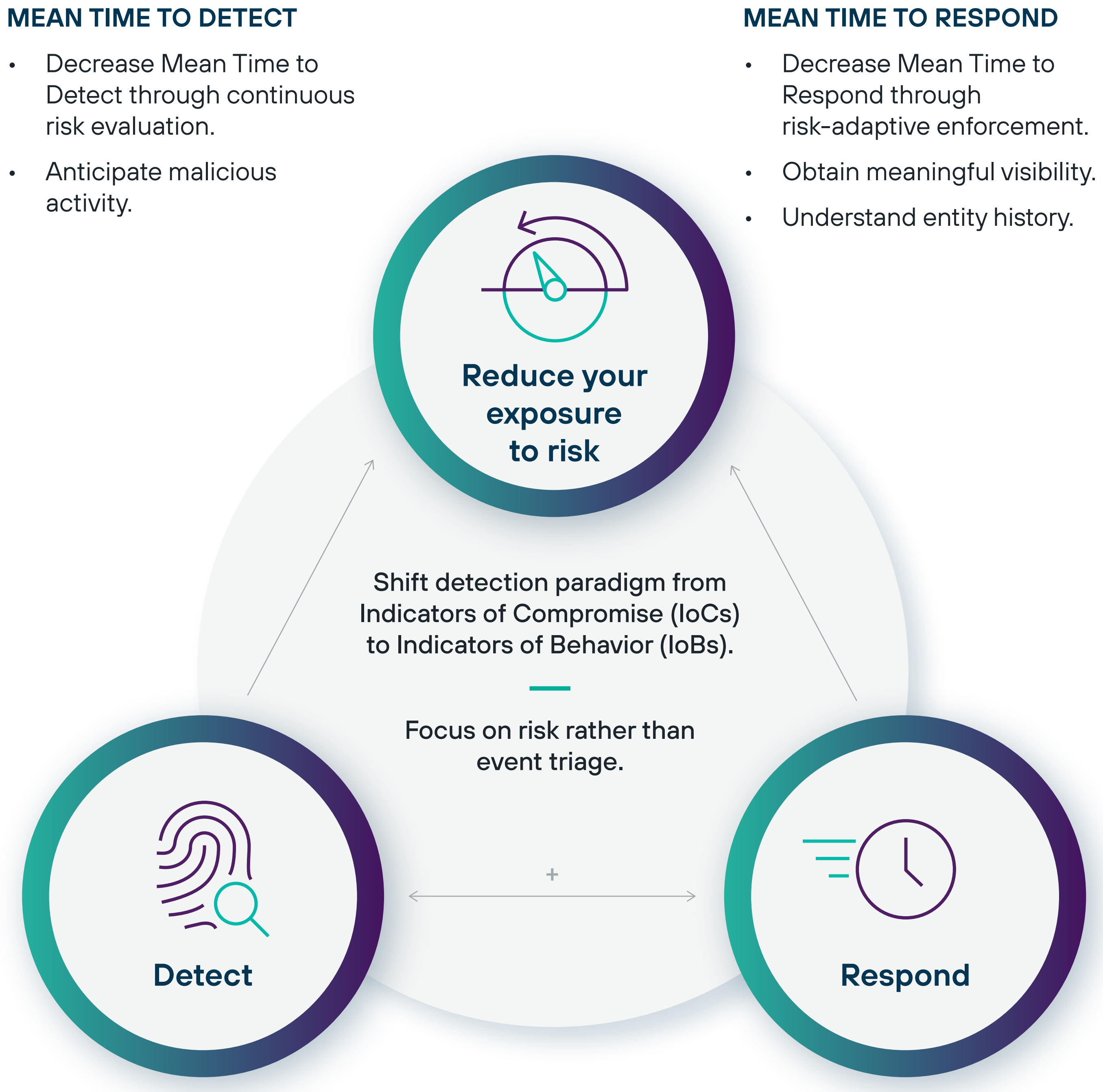
How can you verify the authenticity of users on your network beyond identity and access? Does the trust placed in them remain constant? When users access data or systems, can you determine if they are merely performing their duties, unintentionally bending rules, or acting maliciously?

By analyzing the behavior of machines and humans, you can shift from a simplistic, binary block-or-allow security strategy to more nuanced policies that factor in user and entity risk levels. Policy actions can be tailored to the risk level of risk a user poses, be it no-risk, low, medium, high or critical risk.

Forcepoint DLP offers over 1,700 pre-configured policies, classifiers, and templates that can be individually personalized, automating DLP policy action to a highly precise enforcement. Adaptive data protection that is behavior-based continually evaluates and calculates risk, allowing you to constantly assess whether the user or device is acting as expected or has been compromised.

Furthermore, by leveraging your existing security and non-security investments to inform behavioral analytic models, you can take proactive action instead of reactive, audit-only measures.

When the behavioral risk score reaches a critical threshold–and the model predicts an imminent data breach–risk-adaptive security automatically initiates a range of actions that are commensurate to the risk level and sensitivity of the data. This capability allows security to not only safely enable your people but also to detect warning signs and thwart breaches before they occur.



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.

Shift detection paradigm from Indicators of Compromise (IoCs) to Indicators of Behavior (IoBs).

Focus on risk rather than event triage.

Using Indicators of Behavior to Build a Dynamic Risk Score

The behavior-based approach to risk-adaptive data protection requires a shift toward Indicators of Behavior (IoBs). IoBs offers context-rich monitoring, analyzing user activities across multiple channels to understand the intent behind flagged incidents. Tailoring IoBs to user roles ensures risk scores aren't affected by activities deemed normal, such as a financial analyst editing PCI data. Context-rich IOBs are crucial for a proactive, zero-trust DLP approach, moving beyond reliance on reactive IoCs (Indicators of Compromise).

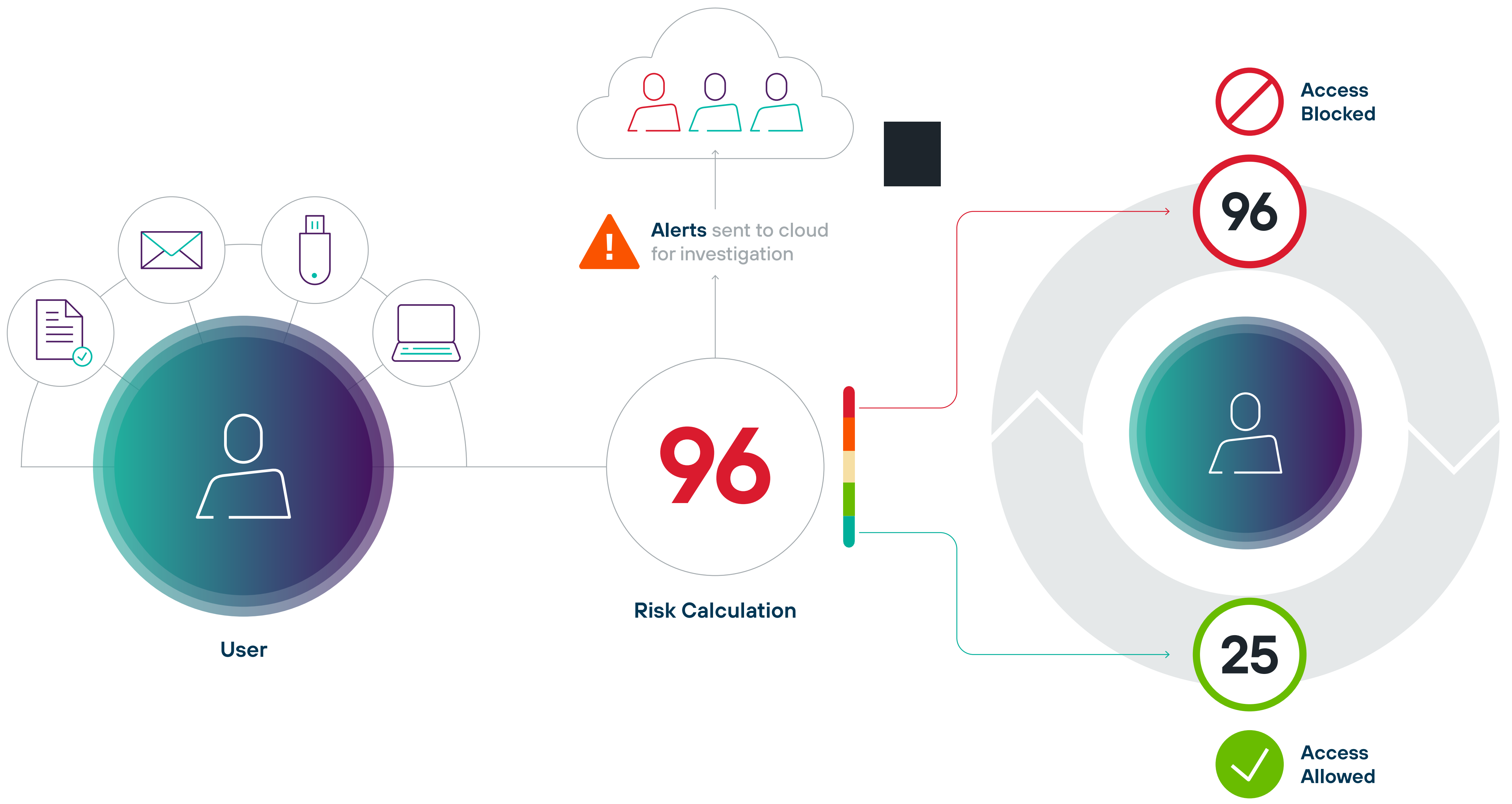
Behavior-based data security adapts to changing levels of risk:

→ Visibility from the endpoint for the IoBs, and enforcement through the policies based on risk available across all main channels.

→ Detects when people are exhibiting risky or anomalous behavior: their risk score changes depending how they behave at any time, allowing security to tighten targeted policies and block actions if required

→ Decides what is innocent, atypical, or suspicious based on behavior in context, reducing false positives

→ Leverages intelligent data security to revisit decisions as you and your machines learn



Adapting Risk Scores in Real-time: Intelligent Breach Prevention

Risk-Adaptive Protection reduces false positives and negatives, offers crucial context for data movement, automates policy enforcement, and strengthens Zero Trust security

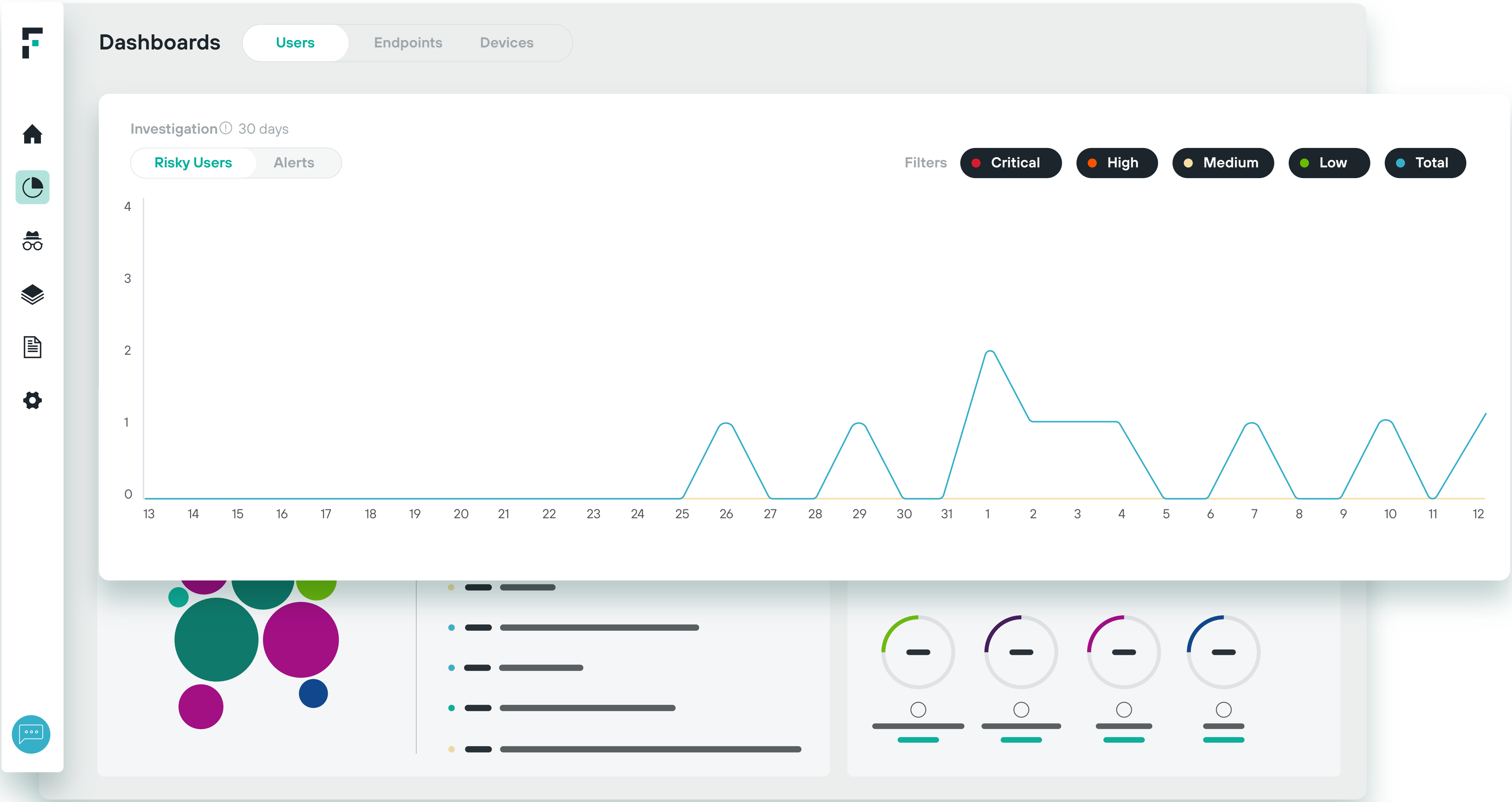
Behavior-based data security adapts to changing levels of risk:

→ Kate is a research chemist who is preparing for a presentation to senior leadership at the end of the quarter.

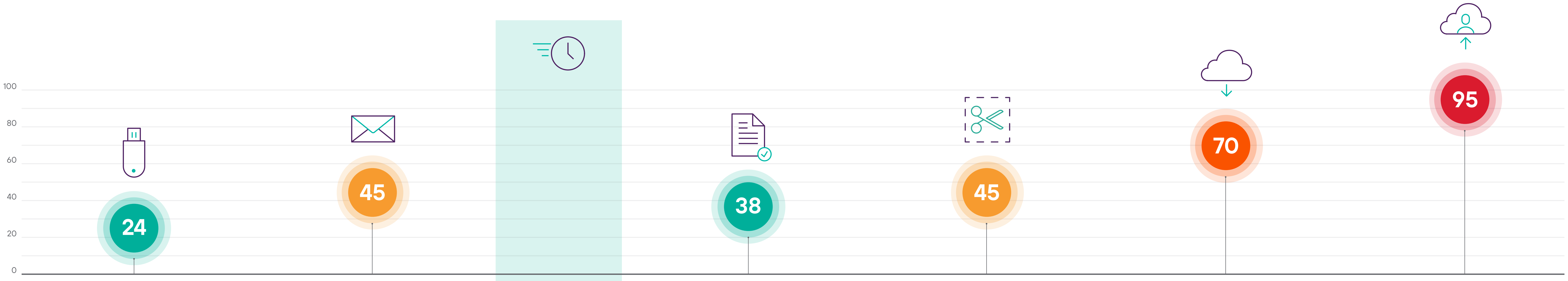
→ Her presentation will require her to include confidential company information.

→ Kate is a good employee. We want to enable her to do her job.

Follow Kate as the Risk-Adaptive Protection system enables access to the data she needs, while remaining vigilant for inadvertent risky behaviors that could lead to a serious data breach....



Continuously monitoring, detecting, and analyzing behavior to stop malicious or unintentional data breaches



Kate tried to copy her slides to a USB stick.

Low Risk:
The system understands this is part of her job and does not block it. However, her risk score increases as the IoB has been seen to lead to data loss.

Kate tried to send her slides to her personal email.

Medium Risk:
Based on the file size the risk is elevated and a confirmation is required to acknowledge this risk. The system continues to monitor but does not prevent the email.

Perhaps she needed this access to continue doing her job.

Within a few weeks if she does not behave in a risky manner her risk score will decrease and her profile will return to Low Risk.

30 days pass.

Risk score declines because no anomalous, risky behavior has occurred...

Kate copies the text from a chart displayed by a genomic application and pastes it into a new slide.

Low Risk:
While this activity is considered evasive and meant to bypass security, it could be legitimate depending on her company's policies. Her risk score goes up slightly but is allowed.

Kate tried to take a screenshot form the genomic app and upload the image to a cloud location to use later.

Medium Risk:
The system views this behavior as data stockpiling, which could lead to data loss. Her risk score is now deemed Medium Risk but her system allows her to continue.

Later, Kate gets a supplier query about an order she doesn't remember placing and logs into the supplier's website to check.

Kate's user account begins accessing sensitive formulation data and attempts to download it to her local system in bulk.

Kate may have been phished.

High Risk:
Like Kate's earlier attempt to send the data to her personal email, this falls into a gray area between allowed and disallowed activity. However, due to the previous actions, the system moves Kate into the High Risk group and encrypts all of the uploaded files so that they can only be accessed on a corporate system.

Kate tries to upload a large number of files to a personal cloud.

Critical Risk:
Due to Kate's risky behavior, the system blocks her attempt because her current status is "critical risk." . The context indicates that her action poses a high-risk and requires blocking..

As the risk score becomes critical, the system blocks actions, averting the breach.

Separating Risk Signals from the Noise

As Kate engages in various activities, the Risk-Adaptive Protection system facilitates secure data access while implementing controls commensurate with the risk level. The system continuously monitors and analyzes user interactions to provide much-needed context to data movements, which reduces both false positives and false negatives, and proactively stop breaches before they can occur. By understanding the digital indicators of risky user behavior and automating enforcement, Risk-Adaptive Protection bolsters Zero Trust security.

Moreover, transitioning to a risk-based, dynamic security approach enhances the significance of IT security teams. Viewing security through the prism of behavioral risk provides a strategy and common language that business partners can comprehend. By prioritizing behavior, security transforms from being perceived as the department of "No" to the department of "Yes," fostering trust in security decision-making and facilitating the quantification of IT security's role as innovators.

> "We tend to be risk-averse as a company, so Risk-Adaptive Protection policies can help us verify that one of our developers, for example, isn't sending data that they shouldn't be sending."
>
> **MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNISIS**

> "We plan to determine more RAP policies by looking at additional risky user behaviors. Monitoring anomalous behaviors that help us identify high-risk users is an incredibly exciting feature and is a huge reason we use RAP with Forcepoint DLP."
>
> **MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNISIS**

Embracing Risk-Adaptive Protection Empowers Data Security Everywhere

Risk-Adaptive Protection stands as a cornerstone in Forcepoint's unique approach to simplifying security—we call it the **5 Steps to Data Security Everywhere**. This blueprint helps organizations develop a methodical and comprehensive approach to safely use data anywhere. Security teams can iteratively refine their enforcement policies and apply the same set of policies everywhere, resulting in a single set of uniform policies for securing data across all the digital paths in which organizations conduct business.

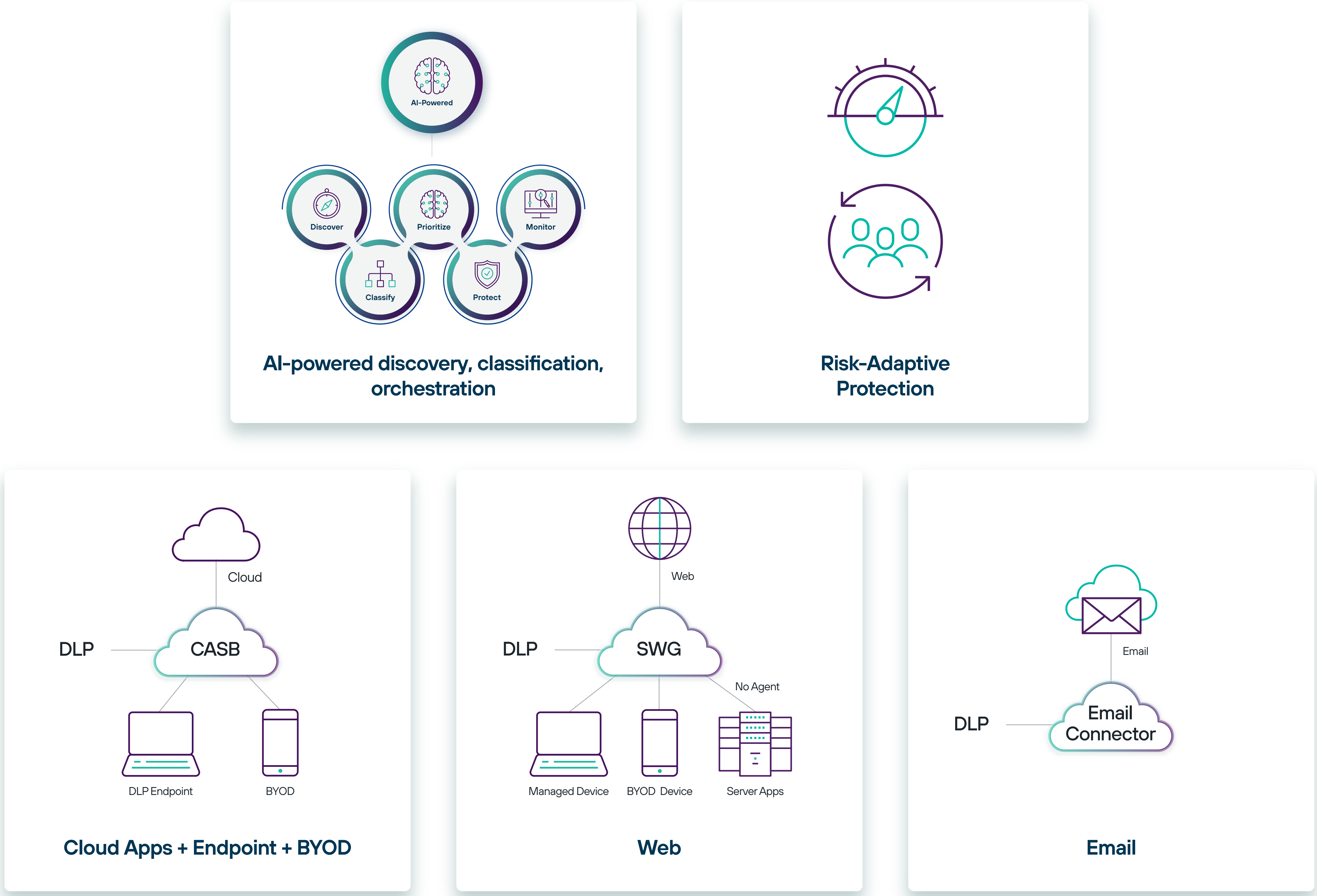
Customers have the flexibility to start on their journey from any point, enhancing their security measures with AI-driven intelligence, behavioral risk analysis, and controls tailored to apps, endpoints, BYOD, websites, and email as needed. With Forcepoint, customers can effortlessly adopt and maintain a single policy to control all data, thereby achieving success in their business and workforce strategies while ensuring Data Security Everywhere.

→ **For more information, visit: CDW.com/forcepoint**

→ **Discover more Forcepoint customer stories.**

→ **Schedule a Demo.**

5 Steps to Data Security Everywhere



AI-powered discovery, classification, orchestration

Risk-Adaptive Protection

Cloud Apps + Endpoint + BYOD

Web

Email

Forcepoint

CDW.com/forcepoint

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 www.forcepoint.com, Twitter and LinkedIn.

[FP-Ebook-Risk-Adaptive Data Protection-CDW-EN] 18Apr2024