



Forcepoint

Risk-Adaptive Data Protection:

The behavior-based approach

Balancing Security While Enabling Your People: Your Job Just Got Harder

With the proliferation of data, cloud apps and mobility, people are now truly your corporate security perimeter. The network edge is now your employee’s kitchen, living room or home office. COVID-19 has forced organizations to accelerate the evolution of the work environment by five to 10 years: your colleagues are likely permanently remote and "WFA" (work from anywhere) and connecting to cloud services with an IP address they didn’t obtain from IT.

No longer bound by physical or network infrastructures, your people want to move at the speed of innovation, and security that inhibits productivity becomes an excuse to break the rules. Shadow IT creates blind spots where your people sidestep policies, which only increase the risk of data theft, accidental leakage, and corporate exposure.

Every entity on the network, from privileged accounts and contractors to employees and even bad actors, are potential threats to IP and other users. In a mobile and SaaS world, how do you handle the insider threat with the new reality of where "inside" is? On top of this, regulations such as GDPR and CCPA compel you to respond quickly to breaches and proactively mitigate risk or, otherwise, face stiff fines and other penalties.

The old security approach tried to keep attackers out by building higher walls. Now your people are beyond the walls. We need a new security model that safely enables employees as much as it protects IP and critical data.

Statistics sourced from: Gartner, Public Cloud Services, Worldwide, 2018-2024, Verizon 2020 Data Breach Investigations Report, Ponemon - 2020 Cost of Insider Threats Global Report, EY & iapp - Privacy Leader's Views: The Impact of COVID-19 on Privacy Priorities, Practices and Programs.



\$513 Billion
Cloud market size worldwide in 2024



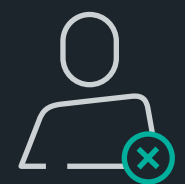
80%+
Of hacked breaches involve brute force or lost or stolen credentials



43%
Web apps involved in breaches



47%
Growth of Insider Threats since 2018



62%
Incidents due to negligent insiders

Why Security Teams Plan to Fail

Why must we accept that breaches are inevitable? While traditional data protection does provide visibility into an organization's data activity, it lacks the context behind user interactions. The result: the system struggles to distinguish between legitimate and risky data usage, triggering excessive alerts that overwhelm IT Security.

So you're left with two choices—neither are very palatable.

- A** Err on the side of caution and apply restrictive policies to mitigate risk, which dampens productivity and encourages employees to try bypassing security, or
- B** Allow minimal policy enforcement to enable productivity, enable passive monitoring data security and act as a forensic tool if, and when, a breach occurs.

For many, option B is the lesser of two evils. It's easier and less damaging to the business to clean up after the event than to try to stop it. Adding a distributed workforce on top of this scenario ratchets up the security challenges.



The Breakthrough: Putting Behavior at the Center of Data Security

The answer is to both protect and free the enterprise by being able to identify, quantify and proactively respond to data risk. The solution is behavior-based data security that focuses on your people and how they interact with your data. By understanding that people are the new perimeter we can secure your data wherever they access it: at headquarters, remote branches, home and office, or in the cloud—anywhere.

Upgrade to Risk-based Data Protection

Enterprises govern most strategic decisions by understanding their risk, being able to quantify risk, balancing their tolerance for it and defining their processes for mitigating against risk. To achieve this, IT and security teams need the tools and capabilities to understand where, how and by whom data is used so they gain the comprehensive context required to prioritize and react to risk.

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

In this way, you can essentially trust an intelligent solution so that you can trust and enable your employees.



Risk-Adaptive Data Protection: A personalized automated approach to Data Loss Prevention (DLP)

What is behavior-based data security?

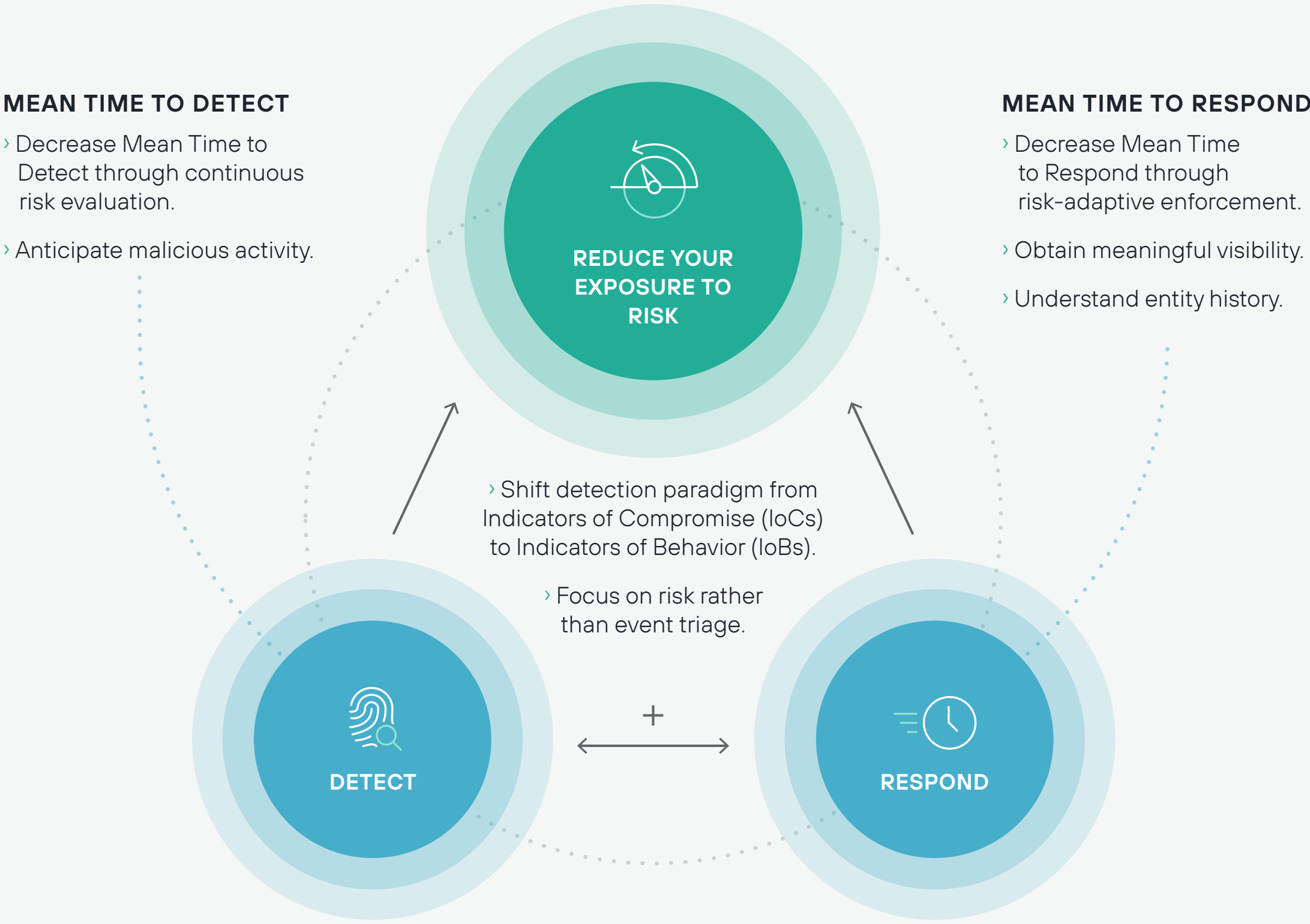
Behavior-based data security integrates behavior analytics with data loss prevention (DLP) to provide proactive dynamic policies and enforcement. Understanding behavior allows you to decide when to trust a user’s access to and interaction with data—or when to block it.

Beyond identity and access, how do you know if the users on your network are really who they say they are? Should the trust you place in them be a constant value? When a user accesses data or a system for the first time, are you certain it is really the user or machine you think it is, or have those credentials been compromised?

By analyzing the behavior of machines and humans, you can move from a binary block-or-allow security strategy to implementing more nuanced policies that factor in user and entity risk. Policy actions can be customized by the level of risk a user brings to the policy (low, medium, high or critical risk). Forcepoint

DLP offers over 1500 out-of-the-box policies that can be individually personalized in this way, automating DLP policy action to a highly precise enforcement. Behavior-based, adaptive data protection continuously calculates risk, allowing you to constantly evaluate whether the user or device is acting as expected or is actually compromised. Furthermore, by leveraging your existing security and non-security investments to inform behavioral analytic models you can take proactive action instead of a reactive, audit-only stance.

When the behavioral risk score reaches a critical threshold—and the model predicts that a data breach is imminent—risk-adaptive security automatically applies a range of actions that are proportional to the risk and sensitivity of the data. Now security can offer a solution that not only safely enables your people but reads the signs and stops a breach before it happens.

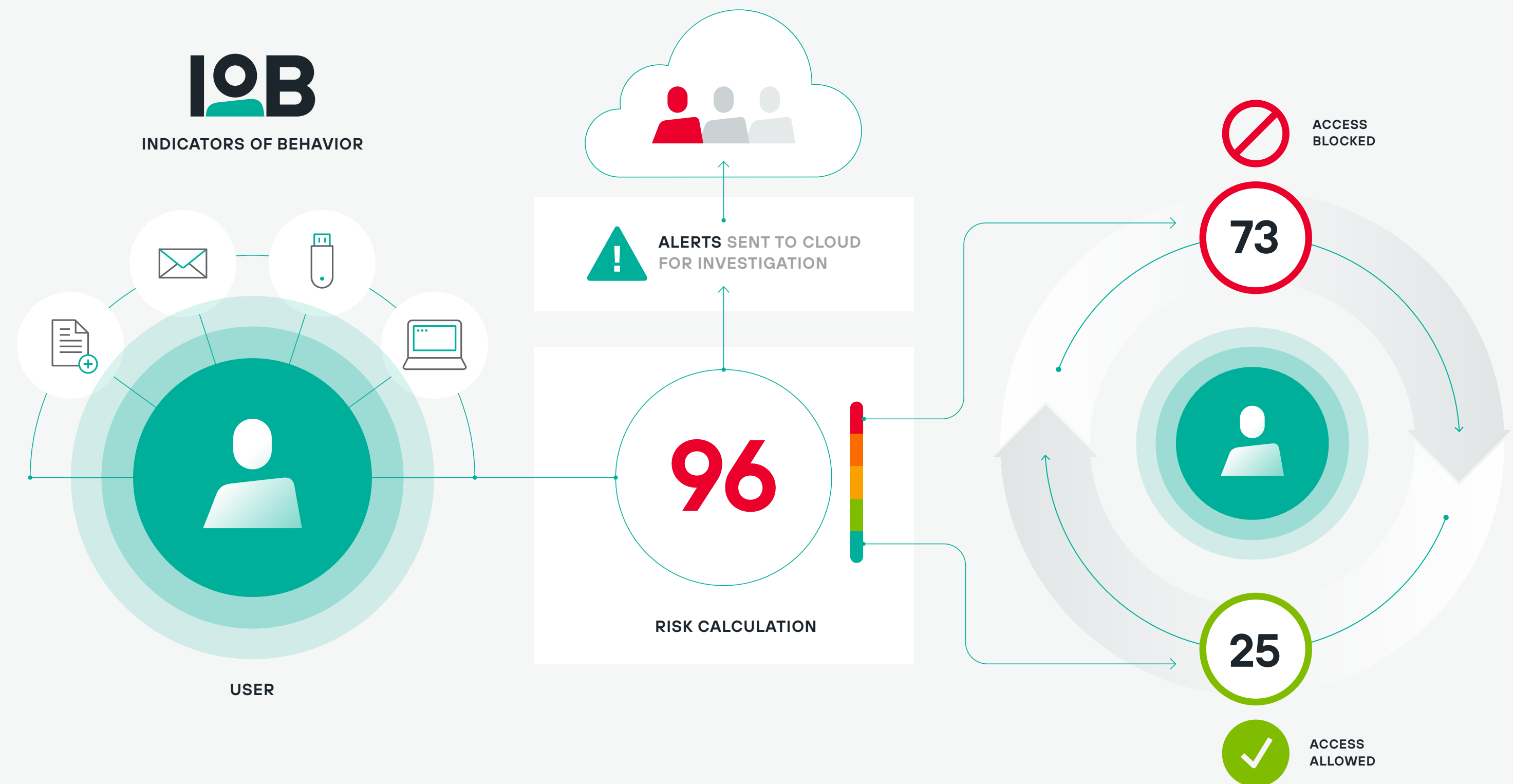


Risk-Adaptive Data Protection: Using Indicators of Behavior

The behavior-based approach to risk-adaptive data protection requires a shift toward Indicators of Behavior (IOBs). IOBs is a context-rich monitoring approach that analyzes user activities across multiple channels to understand the intent behind a flagged incident. IOBs are key to a proactive, zero trust DLP approach instead of relying solely on reactive IOCs (Indicators of Compromise).

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

- Includes enterprise-wide visibility (network, endpoints, and cloud)
- Detects when people are exhibiting risky 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 or suspicious based on behavior in context, reducing false positives
- Leverages intelligent data security to revisit decisions as you and your machines learn



Behavior-based Approach in the Real World: How the Risk Score is Calculated

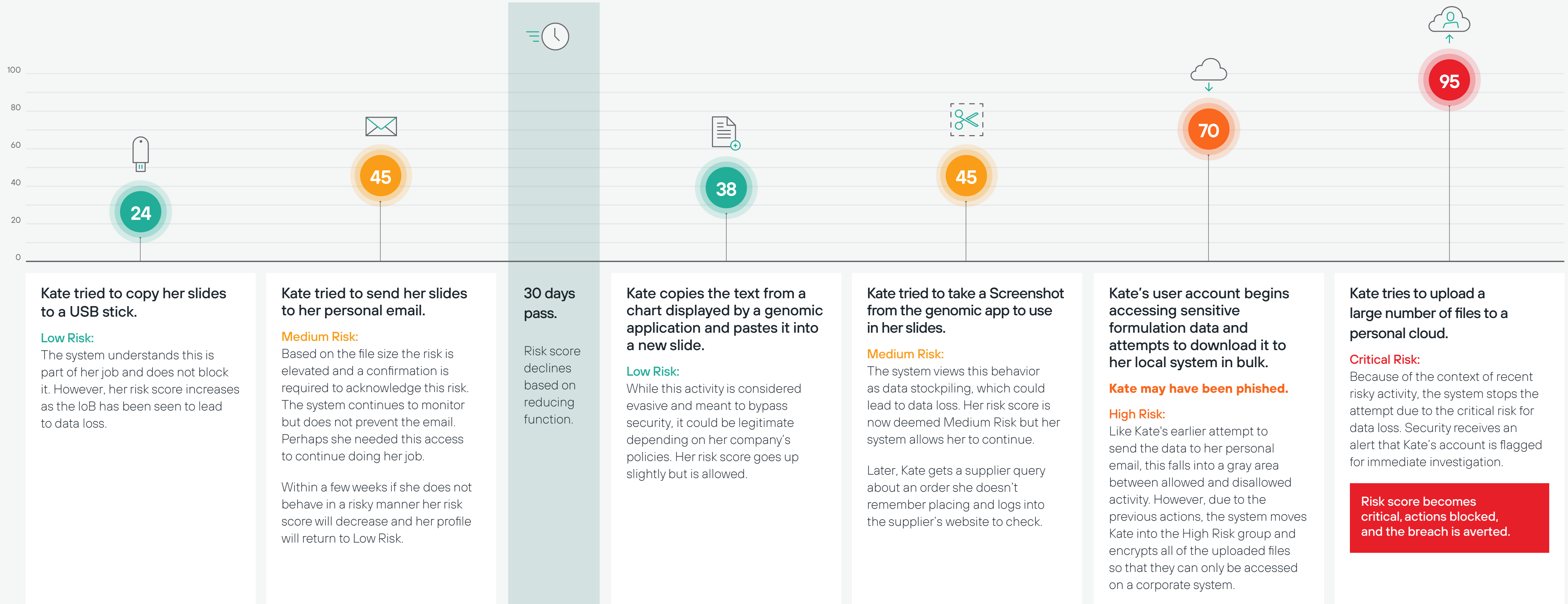
The answer is to both protect and free the enterprise by being able to identify, quantify, and proactively respond to data risk.

Let's explain how this works with a scenario through a behavior-based lens:

- Kate is a research chemist who will give a presentation to senior leadership.
- Kate is a good employee. We want to enable her to do her job.

Here's how the system works to keep both her and the data safe as her actions unintentionally put both at risk...





The Upshot For CISOs

As you can see, each experience with Risk-Adaptive DLP is different for every user depending on the risk level associated with various activities. Security can enable productivity while continuously observing or auditing digital signs for risk to stop a potential breach.

Moving to a risk-based, dynamic security posture elevates the role of IT security within the enterprise. Addressing security through the lens of behavioral risk is a strategy and common language your partners in the business can understand. Focusing on behavior allows you to shed security's reputation as the department of "No" to become the department of "Yes." It becomes easier to trust security's decision-making and quantify IT security's contribution as innovators.



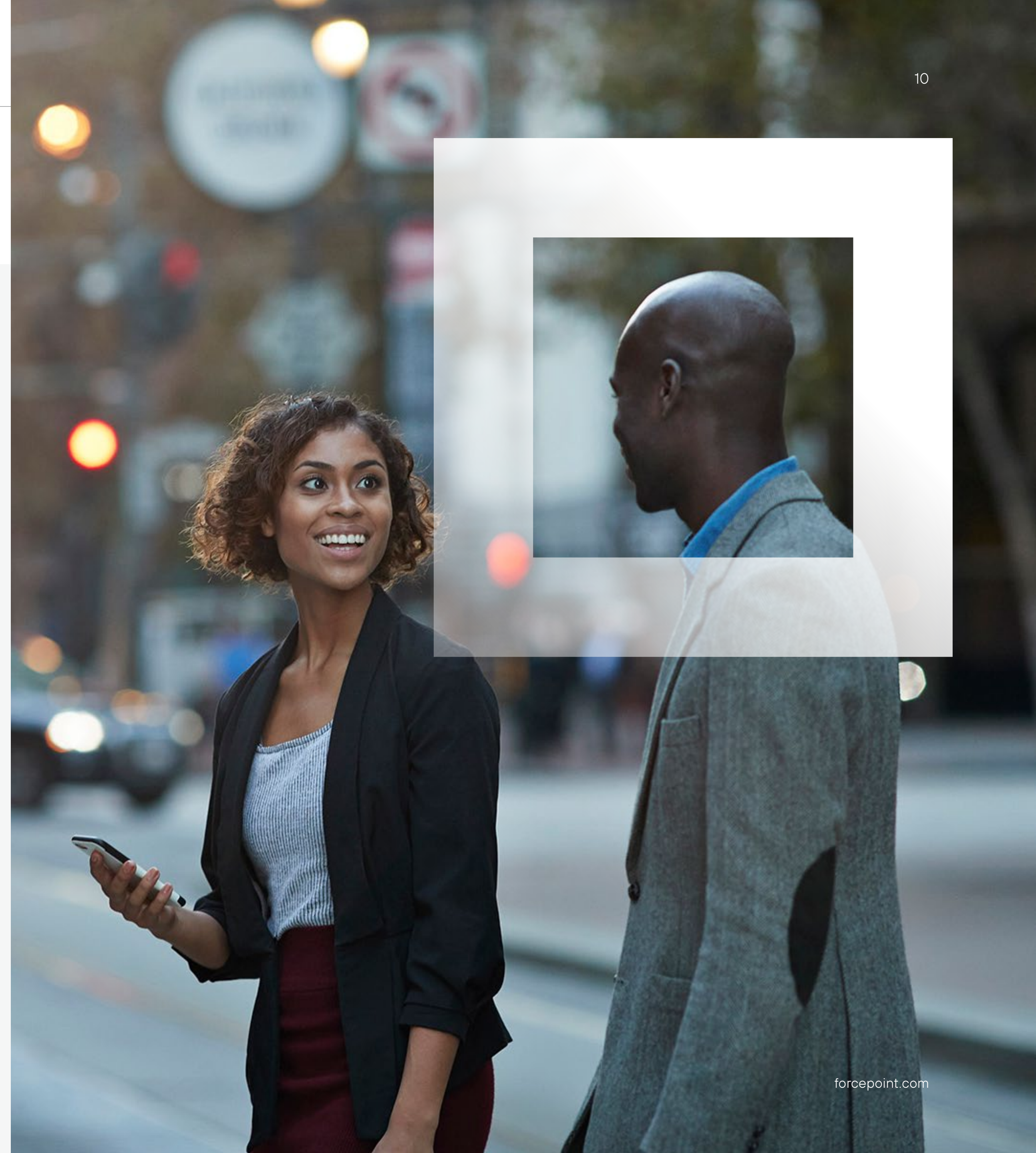
The Final Word on Risk-Adaptive

—

“We can start to be much more targeted in our security, rather than almost putting a wall up and saying, ‘We’re not going to let anybody do anything.’ I just think it’s going to allow us to enable our teams to work better to do their own role in their own job.”

MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNISIS

- **For more information, visit: forcepoint.com/RAP**
- **Discover more Forcepoint customer stories.**
- **Schedule a Demo.**





forcepoint.com/contact

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](#).

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. Risk-Adaptive Data Protection eBook 20APR2022