FORCEPOINT

RETHINKING DATA SECURITY WITH A RISK-ADAPTIVE APPROACH

CONTENTS

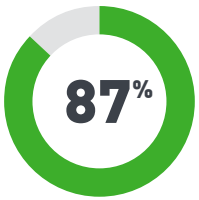
Keeping Up with the Increasing Security Risk of the Mobile-Cloud Era

The two megatrends of cloud-based applications and mobile devices have been a boon for company productivity, agility, and innovation. The mobile-cloud combo empowers employees to work and be productive literally anywhere.

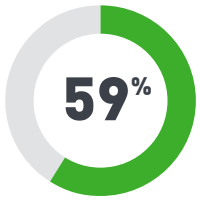
However, the mobile-cloud era has created a conundrum for cybersecurity teams. Here are some of the challenges:

1.87 BILLION

MOBILE WORKERS AROUND THE GLOBE BY 2022, REPRESENTING 42.5% OF THE GLOBAL WORKFORCE



COMPANIES THAT RELY ON EMPLOYEES HAVING ACCESS TO MOBILE BUSINESS APPS FROM THEIR PERSONAL SMARTPHONES



ORGANIZATIONS THAT HAVE A FORMAL BYOD POLICY

IT SPENDING FOR SHADOW IT IN LARGE ENTERPRISES

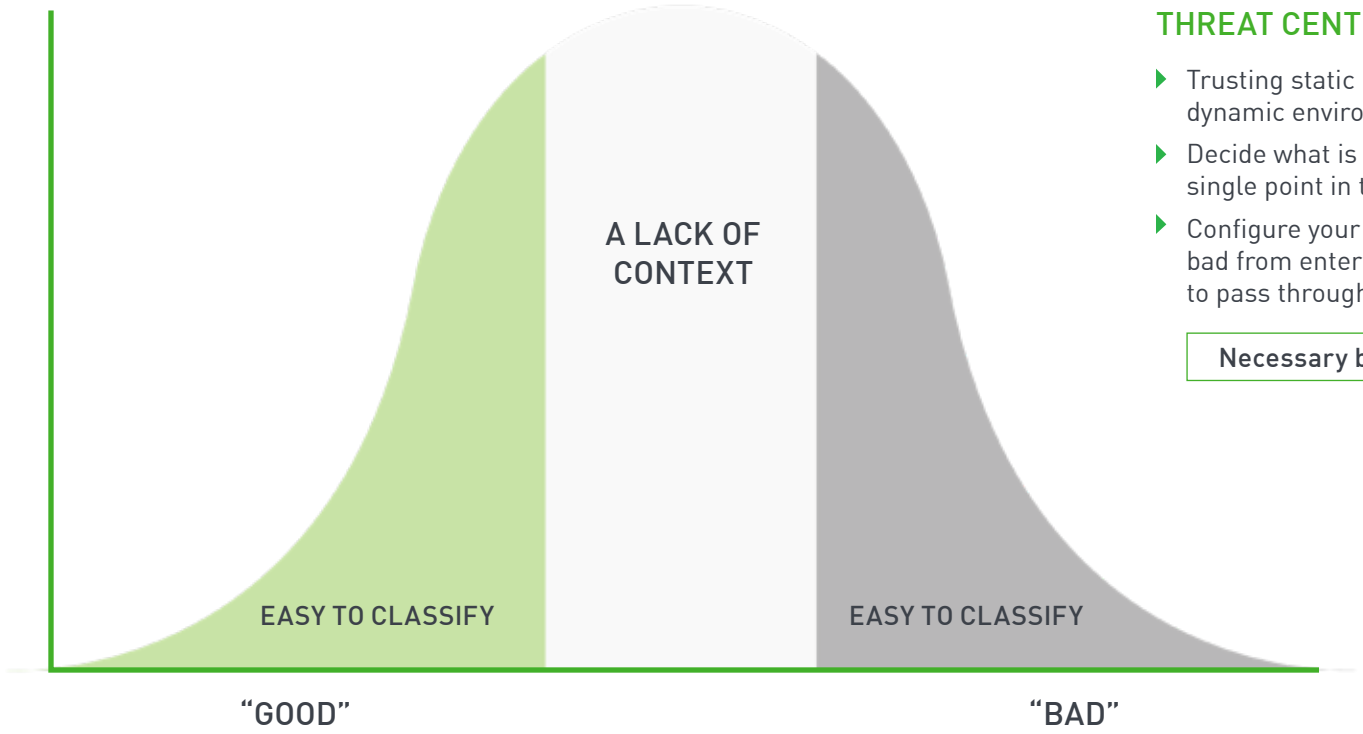
Sources: Strategy Analytics, Syntonic, Everest Group

The Problem with Today's Data Security Approach

If we look at how cybersecurity has traditionally been approached up to this point, it's centered on threat-centric responses. You built a wall around your perimeter, controlled access in and out of that wall, and when something bad happened, you responded. That was effectively your defense, and it was relatively easy to implement.

Today, the traditional perimeter has dissolved, primarily because of two changes within the enterprise: the rise of the mobile employee and the widescale adoption of cloud services. By the same token, cyber activity once easy to define as "good" or "bad" has become nebulous. This poses a crushing problem to threat-centric security, whose static policies are forced to make decisions about cyber activity with no insight into its broader context.

The result is a disproportionate number of flagged activities, overwhelming security teams who have no way to understand the ones most worthy of investigation.



THREAT CENTRIC

- Trusting static policies in a dynamic environment
- Decide what is good or bad at a single point in time
- Configure your defenses to stop the bad from entering and allow the good to pass through

Necessary but insufficient

Fixed Policies Based on Pre-Defined Rules

Let's look at an example. Kate, is a Research Chemist who will be giving a presentation to senior leadership. She wants to copy her slides to a USB stick.

Kate, PhD
Research Chemist

Traditional DLP

POLICY

Block files from being copied to USB drives, alert gets sent to IT

USER IMPACTS

- Kate is frustrated because simple tasks are blocked
- Kate will find another way to solve her problem
- The data protection system becomes ineffective

ADMINISTRATOR IMPACTS

- The admin needs to track down the alert
- Thousands of alerts come in overwhelming the security admin team
- The security team turns off the DLP policy because there are too many false positives

Today's Data Protection Options are Limiting

Today, IT security protects data in different ways, using a variety of different tools. These tools are designed to do the same thing—protect data—but none of them are really all that effective.

That's because they use static, threat-centric policies to block or allow access to data. And that was OK when everyone worked within a perimeter.

There are issues with siloed tools as well.

Traditional UEBA
Forensic Analysis

Learning why something happened yesterday does not stop the problem

Traditional Insider Threat
Constant Monitoring

Balancing workforce privacy and IP protection is critical

Traditional DLP
Block it or Allow it

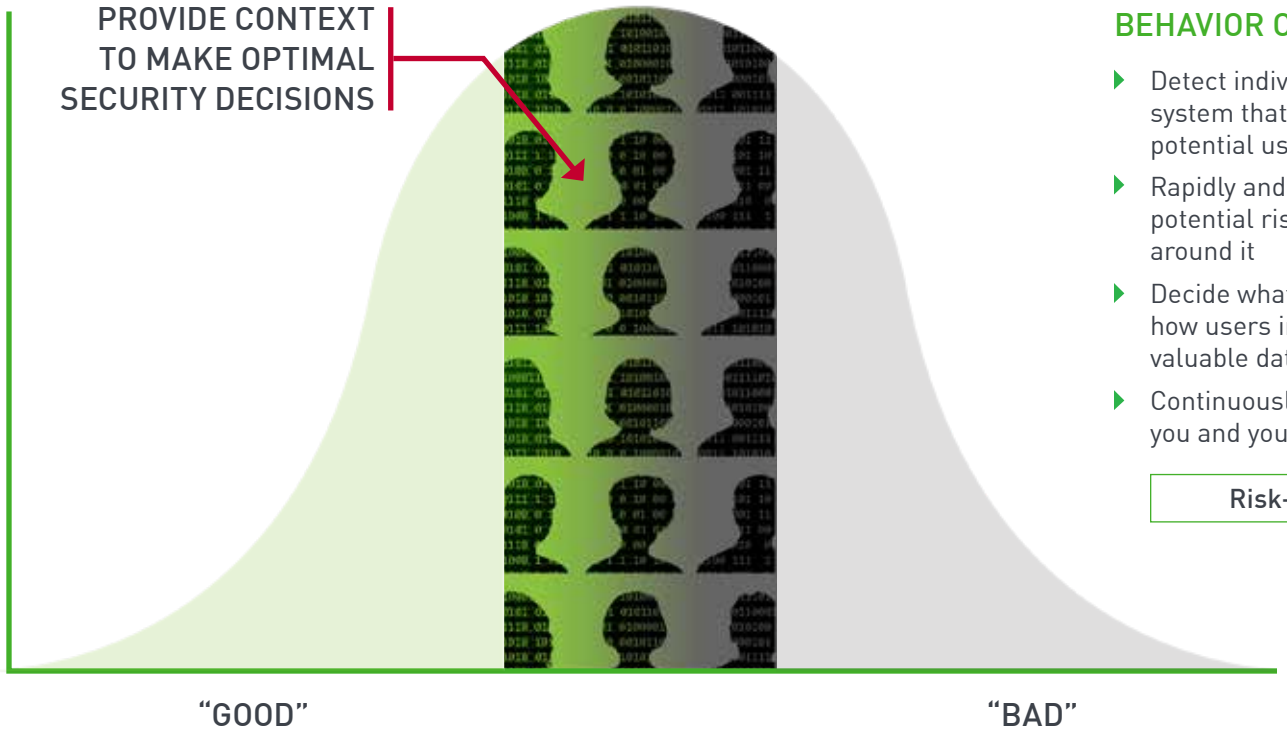
Current policies are far too rigid to be effective

An effective solution should cut through the noise of alerts and highlight early warning signals to **prevent** the loss of important data.

A New Paradigm

Instead of trying to extend the traditional, event-centric approach by adding more layers or crunching more data, we need a paradigm shift that places human behavior at the center of cybersecurity. Cybersecurity professionals need to focus on two constants—people and data—and where the two come together to conduct business.

It's much easier to classify an action once you understand why someone took the action. This is at the core of increasing the efficacy of security organizations.



BEHAVIOR CENTRIC

- Detect individuals interacting with system that pose the greatest potential user risk
- Rapidly and anonymously understand potential risky behavior and context around it
- Decide what is good or bad based on how users interact with your most valuable data
- Continuously revisit your decisions as you and your machines learn

Risk-Adaptive Protection

A New Approach: Dynamic Data Protection

Kate, PhD
Research Chemist

Low Risk Group

Kate is giving a presentation to senior leadership and tries to copy her slides to a USB stick.

POLICY

Encrypt fingerprinted files to USB drives but allow others to be copied

High Risk Group

Kate gets a supplier's query about an order she doesn't remember placing and then logs into the supplier's website to check on it. (Kate just got phished)

POLICY

Observe Kate's every user & machine detail and **block** all data transfers or copies anywhere

WHAT JUST HAPPENED?

In both approaches, the important data was protected.
With Dynamic Data Protection, more context is available.

- **Context:** We know if Kate, our employee, is compromised or malicious
- **Action:** We 'freed the good' and didn't prevent simple tasks from being completed
- **Policy Enforcement:** We can take intermittent steps such as allow, audit, or observe based on risk level.

By 2020, 25% of new digital business initiatives will adopt a CARTA strategic approach, up from less than 5% in 2017.

Source: Gartner, Top 10 Strategic Technology Trends for 2018: Continuous Adaptive Risk and Trust, David W. Cearley, Neil MacDonald, Mike J. Walker, Brian Burke - 8 March 2018

The Right Choice for Data Protection

By using Dynamic Data Protection, organizations can solve the fundamental challenges of traditional DLP deployments and more effectively protect sensitive information, including regulated data sources and PII.

This is the **first and only solution in the market of its kind**, and the only one that can automate policy enforcement to **dynamically respond to changes in risk** within an organization.

With intelligent analytics, unified policy, and orchestration at its core, only Forcepoint can provide the end-to-end, human-centric security architecture required for the security challenges of today and tomorrow.

The relationship between Kootenai Health and Forcepoint is only going to grow. I'm really impressed with the capabilities and level of protection the solution provides. I'm a Forcepoint customer because I choose to be. I don't know of another solution that does the job better.

- Michael Meline, Director of Data Security, Kootenai Health

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit **www.forcepoint.com** and follow us on Twitter at **@ForcepointSec**.

CONTACT

forcepoint.com/contact

[EBOOK_RETHINKING_DATA_SECURITY_EN] 800011.042618

For more information about Dynamic Data Protection, please visit: **forcepoint.com/dataprotection**