eBook

Rethinking Data Protection: The Human-centric Approach

Table of Contents

Traditional Cybersecurity in the Multi-cloud Era

Mobile devices and cloud-based applications that empower teams to work anywhere have been a boon for business productivity, agility, and innovation. However, this new way of working presents new challenges for cybersecurity teams.

1.87 Billion

Mobile workers around the globe by 2022, representing 42.5% of the global workforce

87%

Companies that rely on employees having access to mobile business apps from their personal smartphone

59%

Organizations that have a formal BYOD policy

50%+

IT spending for shadow IT in large enterprises

Traditional Cybersecurity in the Multi-cloud Era

The Truth About Traditional Data Security
Traditional cybersecurity was hinged on event-centric responses: Build a wall at the perimeter, control what passes in and out through that wall, and respond when something suspicious happens. That was the defense, and it was relatively straightforward to implement.

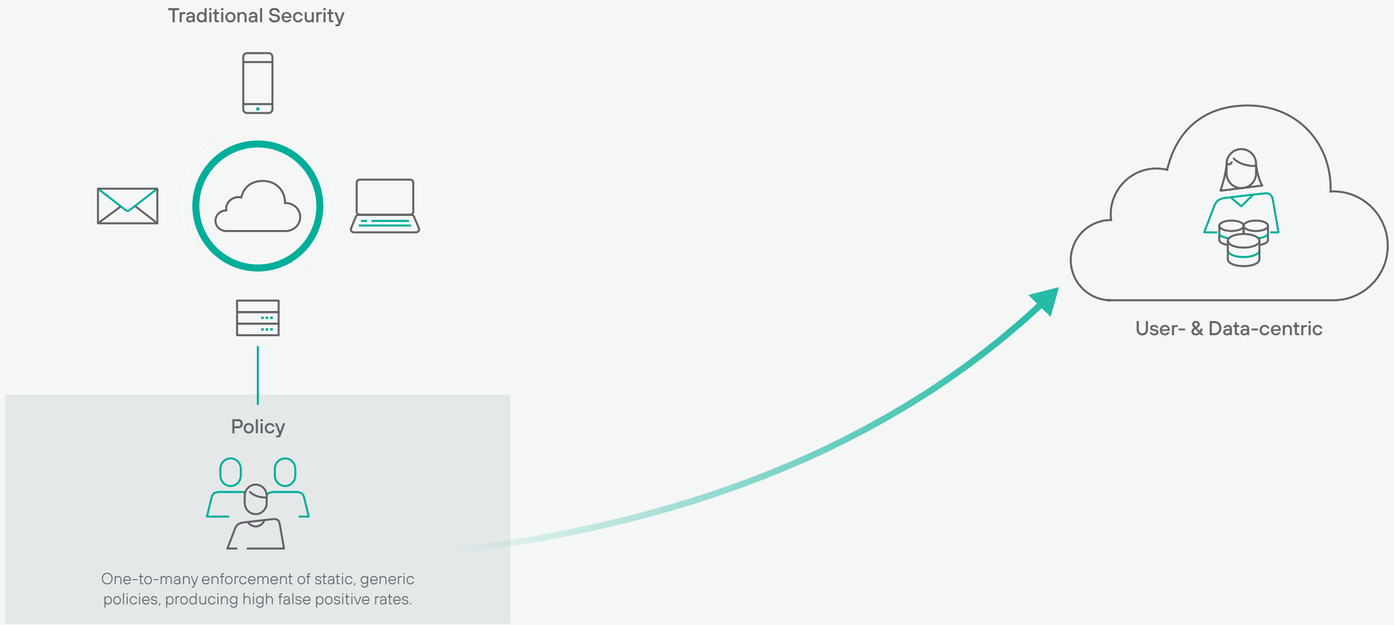
But fast-forward to today and the traditional perimeter defense method no longer works, primarily because of two big changes in business: the rise of mobile employees and the wide adoption of cloud services. While cyber activity was once easy to classify as "good" or "bad," now there are gray areas. This presents a problem for event-centric security's static policies, forcing them to make calls about cyber activity without context.

The result? An overload of flagged activities overwhelms security teams who have no way to discern which warrant investigation and which do not.

Traditional Cybersecurity in the Multi-cloud Era

An Event-Centric Approach:

- → Trusts rigid, static policies in a dynamic environment
- → Decides what's innocent or suspicious at a single point in time
- → Includes limited control of data movement
- → Lacks visibility into the activity that poses the greatest risk



Pre-2000 — Event-centric → **2010** — Human-centric → **2020**

Traditional Cybersecurity in the Multi-cloud Era

Fixed Policies Based on Predefined Rules

Let's look at an example: Kate is a research chemist who will be giving a presentation to senior leadership. She tries to copy her slides to a USB stick as a backup. But then, this happens:

Kate, PhD
Research Chemist

Traditional DLP

BLOCKED

POLICY

Block files from being copied to USB drives, alert IT of the transaction / activities

How Kate Feels

- Frustrated that this simple task is blocked
- Determined to find a workaround

Result: The system trying to protect her data becomes ineffective.

Traditional Cybersecurity in the Multi-cloud Era

How the Security Team Feels

- ⟶ Anxious to track down this new alert
- ⟶ Overwhelmed with thousands of alerts already awaiting response

Result: The team turns off the DLP policy because it creates too many false positives.

You can see how static, event-centric policies to block or allow access to data are annoying to users, burdensome to administrators, and ultimately, don't get the job done. And in the new normal, with employees working from everywhere and data stored outside your networks, it's time to make a change.

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

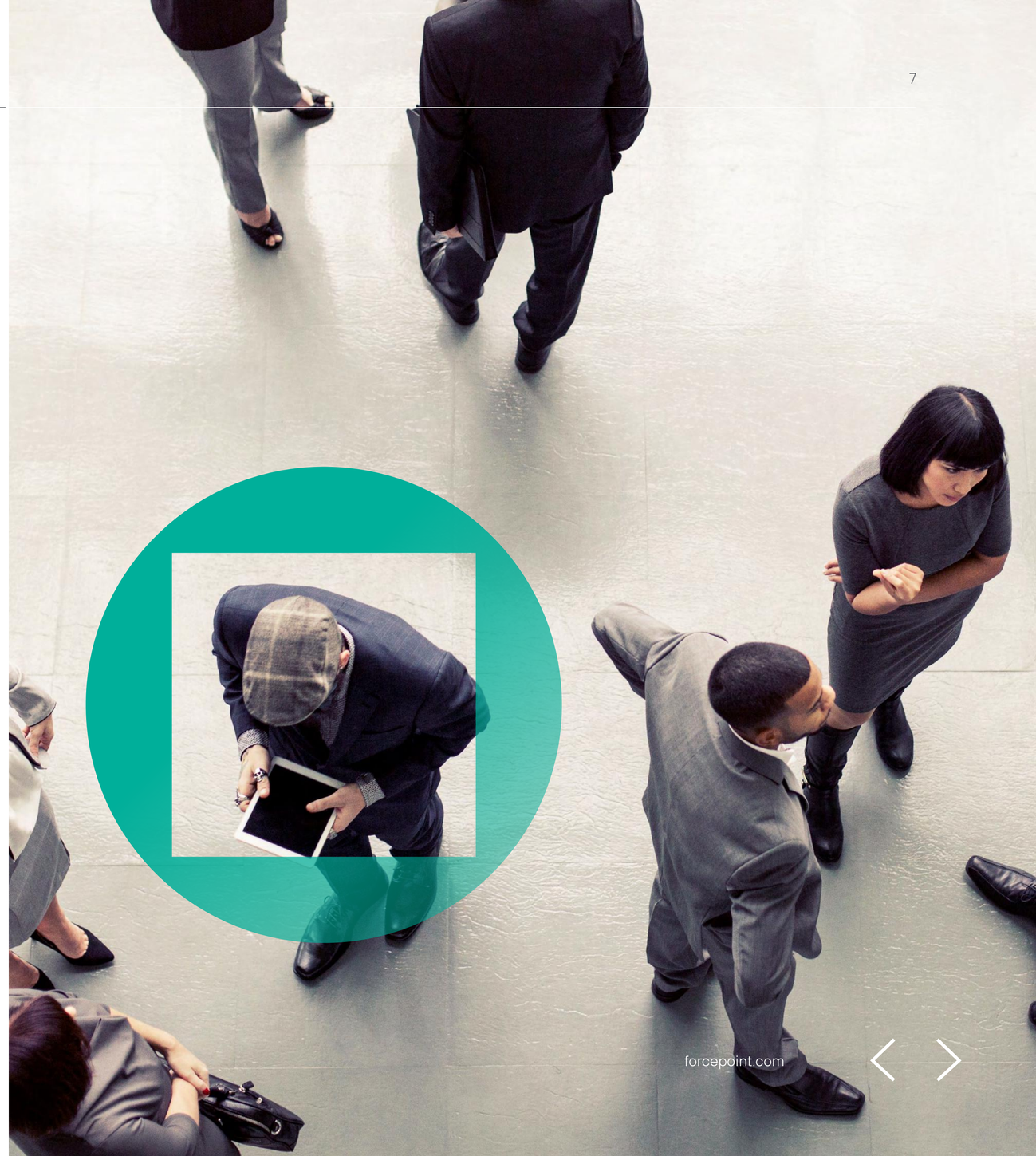
Traditional DLP
Block it or Allow it

Current policies are far too rigid to be effective

The Gold Standard: People at the Center of Cybersecurity

Instead of trying to mold the traditional approach to fit the realities of today, we need a new approach that focuses on the constants: people, data, and where they come together to conduct business.

Putting humans—not events—at the center of cybersecurity allows us to use events as context to understand what the user is trying to do with data. Knowing why actions are taken makes it much easier to distinguish business-as-usual from suspicious or malicious activity that warrants investigation, helping security teams focus their attention where it's needed most.

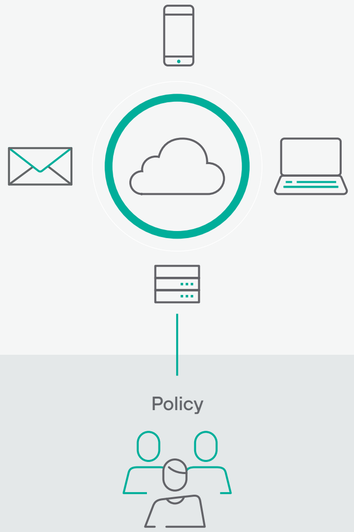


The Gold Standard: People at the Center of Cybersecurity

A Human-centric Approach:

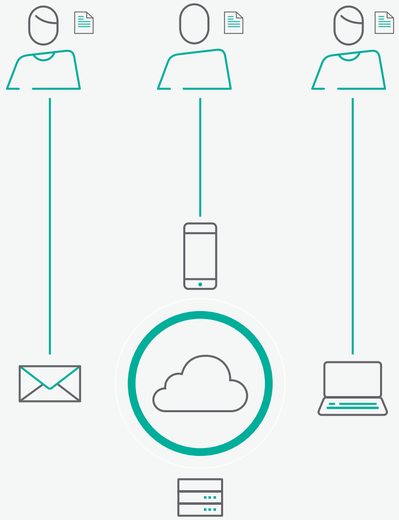
- → Includes enterprise-wide visibility (network, endpoints, and cloud)
- → Detects people who pose the greatest potential risk for more proactive & accelerated responses
- → Decides what is innocent or suspicious based on behavior in context, reducing false positives
- → Leverages intelligent data security to revisit decisions as you and your machines learn

Traditional Security



One-to-many enforcement of static, generic policies, producing high false positive rates.

Human-centric Security



One-to-one enforcement of different policies based on the risk, enabling automation.

Pre-2000 — Event-centric → **2010** — Human-centric → **2020**

The Gold Standard: People at the Center of Cybersecurity

Let's look at Kate's example again through a human-centric lens:

Kate, PhD
Research Chemist

Low-Risk Group

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

POLICY

Encrypt fingerprinted or sensitive files to USB drives but **allow** others to be copied

High-Risk Group

Kate gets a supplier query about an order she doesn't remember placing and logs into the supplier's website to check. Shortly after, Kate begins accessing sensitive formulation data and attempting to download it to her local system in bulk. (Kate may have been phished.)

POLICY

Observe Kate's every user and machine details and **block** all data transfers or copies

Human-centric protection provided the context we needed to understand both scenarios fully and respond appropriately.

Context
We know if Kate, our employee, is compromised or malicious in each scenario.

Action
We "freed" Kate and didn't prevent her from getting her work done.

Policy Enforcement
We can take intermittent steps such as Allow, Audit, or Observe based on risk level to granularly enforce policy.

The Safe Choice for Data Protection

Human-centric data protection empowers companies to solve the fundamental challenges of traditional data loss prevention and safeguard regulated data sources, critical intellectual property, and other sensitive information.

Forcepoint Dynamic Data Protection recognized as the Best Data Leakage Prevention (DLP) Solution in the Trust Awards category at the 2019 SC Awards

With intelligent analytics, unified policies, and flexible enforcement at its core, human-centric data protection provides the end-to-end architecture needed to prevent the security incidents of today—and in the future as your organization continues to evolve.

Forcepoint

About Forcepoint

Forcepoint is a strategic cybersecurity partner, entrusted to safeguard organizations while driving digital transformation and growth. Instead of a static one-size-fits-all approach that stifles innovation and creates vulnerabilities, Forcepoint is attuned to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of enterprise and government customers in more than 150 countries.

Learn more about Dynamic Data Protection at forcepoint.com/data-protection