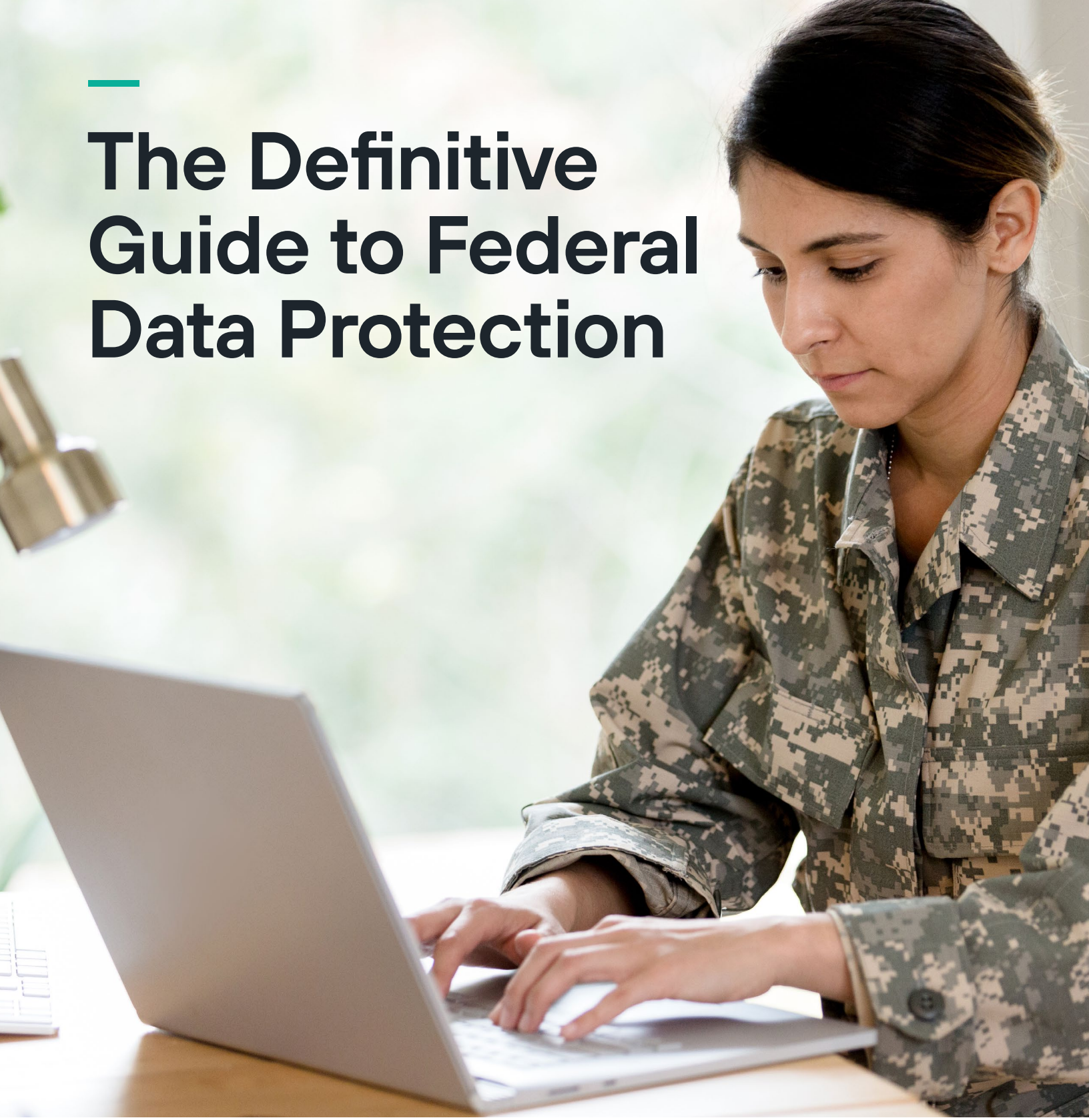
The Definitive Guide to Federal Data Protection



Forcepoint | immixGroup

Brochure

Landscape Overview

In some ways, the relationship between data security and productivity is complex and delicate. Agencies have to strike a balance with security that enables federal employees to do their job and support unique and multi-faceted missions and objectives.

But today, the issue is incredibly complex. While access to data is critical to agencies to support their missions, the U.S. Government Accountability Office (GAO) reported that 82% of agencies have difficulty managing competing priorities between operations and cybersecurity.[1] To compound that effect, the proliferation of mobile devices, far-flung client and contractor relationships, remote and roaming employees, and other factors result in data being stored and accessed in more places, by more people at any given time.

On the heels of this shift in data's role in the workplace, high-profile agency data breaches have helped make a new business case for data security. An agency data breach can affect millions of citizens, have economic impacts, and put agency employees' lives at risk. Breaches can also do critical damage to an agency's reputation and to citizens' trust in government.

Additionally, the Federal Information Security Modernization Act of 2014 (FISMA) identifies the agency head as the responsible official for her or his respective organization's cybersecurity posture, and Executive Order 13800 reinforces this responsibility.

31,107

Cybersecurity incidents endured by agencies in Fiscal Year 2018[2]

2.3 Million

Records breached at FEMA in a 2019 cyber attack[3]

38%

Of federal cyber incidents did not have an identified attack vector, suggesting limited situational awareness[4]

Amid all this, one thing has become clear: Empowering agencies and employees to perform in today's environment demands a shift in how we think about data security. In the constant state of change that has become our new normal, reactive policies are no longer enough to keep us safe. Let's explore how to take a proactive stance on data protection—and why it's the safe choice for agencies today.

82 percent of agencies have difficulty managing competing priorities between operations and cybersecurity.[5]

1,5 GAO report: Agencies Need to Fully Establish Risk Management Programs and Address Challenges GAO-19-384: Published: Jul 25, 2019. Publicly Released: Jul 25, 2019. https://www.gao.gov/assets/710/700503.pdf
2 https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf
3 https://www.wired.com/story/fema-leaked-the-data-2-million-disaster-survivors/
4 https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf

Elevating the role of data security

For many data security teams, days consist of cycles of receiving an alert, investigating it, and repairing the damage. Rinse and repeat. The problem? Inflexible policies frequently flag low-risk activity, resulting in "false positive" alerts. Investigating a daily avalanche of alerts places an immense burden on data security teams who already have more tasks and responsibilities on their plates than they have the bandwidth to fulfill.

Data protection technology that can read into the context surrounding cyber activity can lessen this burden for data security teams, helping them to focus their investigations on incidents which are truly threatening and filter out those that don't pose a real danger to the agency. And, by prioritizing their time more judiciously, this allows a security team to evolve its role within an agency from one that simply enforces rules to one that proactively leads the agency forward toward a safer, more efficient future.

Empowering professional growth

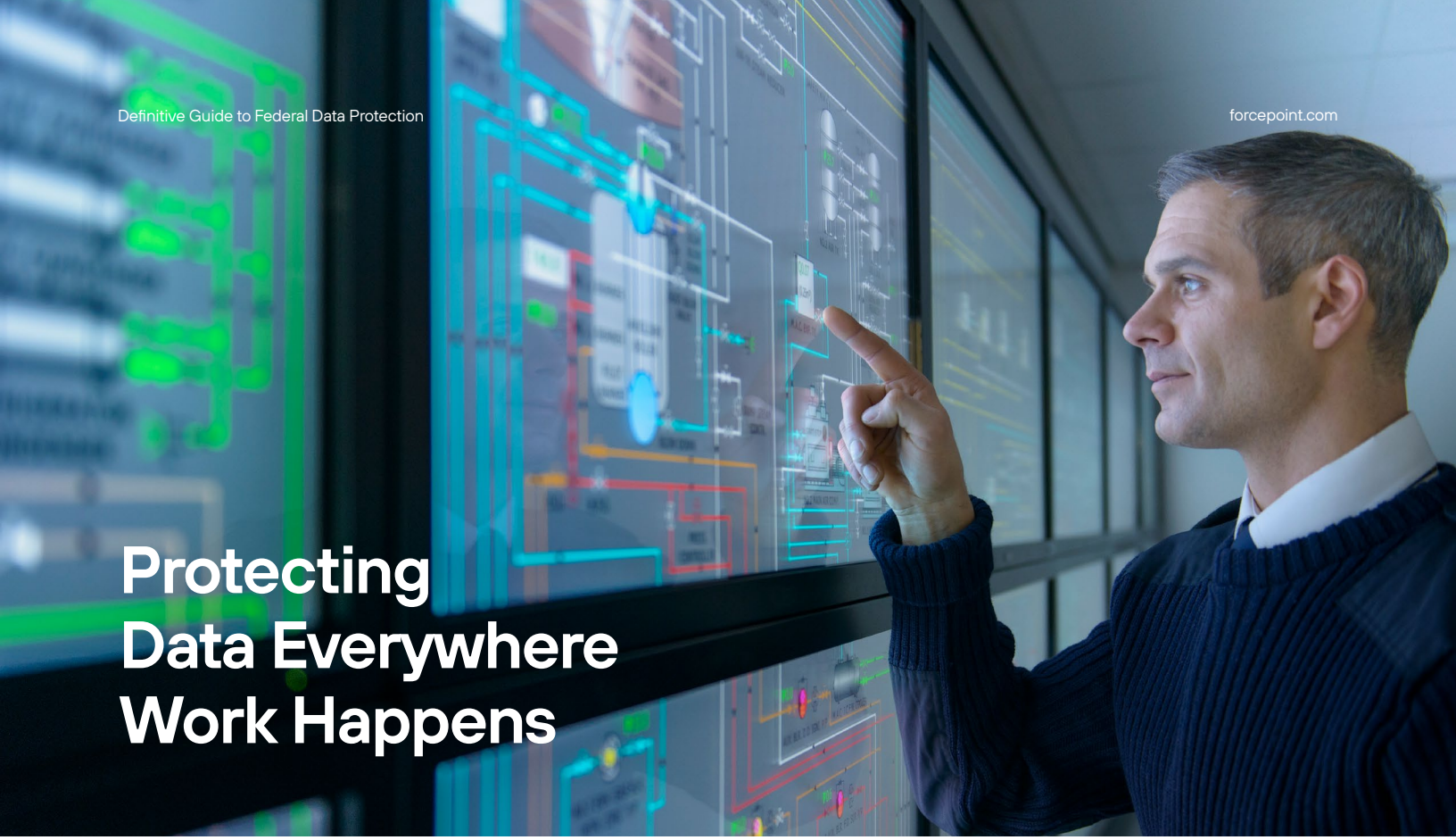
Data security experts who are not overrun with false alerts have the ability to coach and mentor other employees, contributing to their professional development and career trajectories.

Empowering agency missions

Security professionals who are able to find efficiencies in their own workloads can help pinpoint opportunities for meeting agency missions through smarter usage of data—or raise flags about data behaviors that may impede an agency's mission.

Empowering digital transformation

Streamlining investigations based on contextual understanding of data incidents allows teams time to optimize their policies and procedures to suit a cloud-powered data culture—enabling faster digital transformation.



Protecting Data Everywhere Work Happens

Traditional data loss prevention safeguards data at three access points: on your network, at endpoints, and increasingly, in the cloud. And that might be enough—if the people accessing that data stay within those perimeters. But increasingly, they don't, and as soon as the perimeter is crossed, data protection policies break. That means it's no longer enough to color inside the lines. Let's examine what can be done to work past this.

Implications of cloud transformation

Cloud migration isn't a question of "if." It's a question of "when." The demands of remote workforces and strategic partners only accelerate the timeline, pushing for more rapid cloud adoption. In a 2019 Forcepoint-sponsored Ponemon Institute report on "Cloud Adoption in the U.S. Federal Government", 65% of agencies surveyed said securing data is more challenging for cloud environments. Seventy-one percent of agencies said they are challenged to secure cloud usage based on lack of visibility and governance. Only 29% reported they have 360-degree visibility into the sensitive or confidential collected, processed, and/or stored in the cloud by agency.[1] These statistics demonstrate that agencies are not always in control of when and how they move to the cloud. But whatever the pace of cloud migration, entrenched security policies struggle to match it as they adapt to meet new demands.

One reason is that cloud application providers tend to prioritize portability, accessibility, and ease of use—but not necessarily the security of the data that's being made portable, accessible, or easy-to-use. They focus on a shared responsibility model in which they secure the infrastructure, but leave customers to secure data shared in the infrastructure. That means that, given the transitional, mobile nature of work today, it falls to you to build data protection that goes wherever your people do.

Humans are the new perimeter

How can you keep data secure when the people using it cross your lines of defense? It calls for a new perimeter: humans themselves.

Human-centric data protection allows data to be held in a secure environment which people can access from wherever they work. Plus, linking data security to a person's identity allows for policies that take personal risk level into account. This provides insight into intent—for instance, an incident involving a trusted long-term employee may be much less cause for concern than one involving a unvetted vendor or disgruntled ex-employee. Finally, monitoring for data security at the human level provides visibility into how people use data across different devices and applications, providing context that can help security teams better identify threats and learn from them.

1 https://www.forcepoint.com/form/thank-you-your-interest-whitepaper?form_id=1363&-file=41686&resource=31241&category=whitepapers

Making the Case for Human-centric Data Protection

Human-centric data protection is well-suited to the dynamic reality of agencies today—but just how much is it worth to yours? To answer this question, let's debunk the myth that plagues data security teams everywhere: that protection is the enemy of productivity. With the right tools and processes in place, each can empower the other.

Specific responses

Traditional data loss prevention tactics may simply block risky actions—say, a sensitive file being uploaded to the cloud. And, if such an action were taken by a disgruntled ex-employee or a short-term contractor, that response makes sense. More often than not, however, this isn't the case; It may be an employee simply trying to back up an important file or move it to a new computer. But traditional data security policies can't tell the difference, so they routinely blanket-block totally innocuous cyber activity—impeding productivity in the process.

Detecting risks at the human level makes it possible to consider the context and intent behind an action, enabling specific—not blanket—security responses. Not only does this reduce interruptions to employees' workflows, but it also lessens the investigation burden on security teams, allowing them to aid progress rather than blockade it.

Reduced vulnerability

Even an employee with no ill intent may become frustrated with blanket security policies that stand in the way of getting work done. So (still with no ill intent) they may try to find a workaround, bending the rules ever so slightly so they can get past the security blockade. In the last example, perhaps they'd break the file into smaller segments and email them to a personal computer so they can be saved to the drive after all.

This creates two problems. First, this sequence of actions may raise an even more urgent alarm than an attempt to save a file to a removable drive, because it indicates that a person is trying to circumvent security measures. It will likely need to be investigated, which takes time and resources. But perhaps more concerning is that workarounds like these, innocent though they may be, can introduce new vulnerabilities that undermine the security policies that prompted them in the first place. Human-centric data protection would allow for more flexible, appropriate policies, stopping this downward spiral before it starts.

Proactive stance

As any teacher, pet owner, or data security professional can attest, preventing a "mess" from being made in the first place is much more efficient than cleaning it up after the fact.

With the contextual clues and behavioral insights that human-centric data provides, it is possible to halt true threats before they inflict damage, while still allowing the agency to perform at the highest level. Employees can go about their days without tripping over inflexible security policies. Busy data security teams can accurately triage alerts and focus on resolving incidents that pose real risk. It's data security—without compromise.

The New Standard for Data Protection

The evolving nature of security threats means we need to adjust our mindset for keeping data safe—and that includes accepting that change is, and will always be, constant. That's why our core principles for data protection are built with the needs of tomorrow in mind:

1. A preventive, not punitive, culture of data security

The role of data security teams will grow from retroactively enforcing security policies to leading their agency and fellow employees toward safer data usage behaviors.

2. Human-centric risk assessment

Mobile and dynamic data usage demands security that accounts for the only constant: the user. This allows flexible security that adapts as a person's behavior and risk level changes.

3. Holistic view of data

Maintaining full visibility into data as it moves outside your network, across endpoints, or into the cloud gives contextual clues into intent, helping to inform fitting security responses.

4. Consistent policies regardless of environment

Establishing your security perimeter at the human level ensures that data is protected no matter where it's stored or accessed.

Are you ready for what's next on the journey to proactive data protection?

› **Check out our infographic,** 9 Steps to Success with Data Protection

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time 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 customers worldwide.

[Definitive-Guide-to-Federal-Data-Protection-Brochure-EN-IMMIXgroup] 21May2020