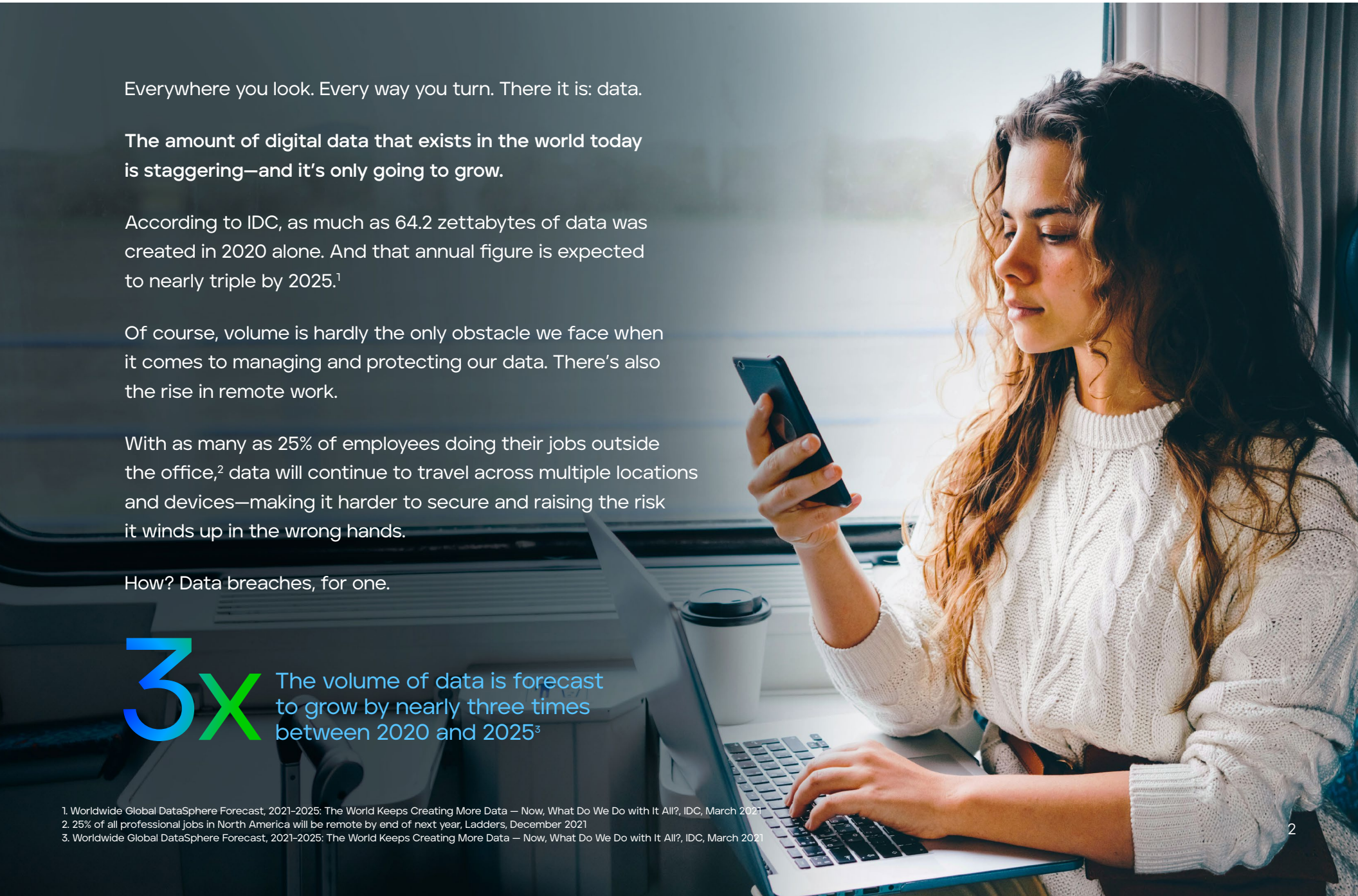
Make your DLP decision with confidence

A buyer's guide to choosing the right data loss prevention solution

Trellix

Data here. Data there. Data everywhere.



Everywhere you look. Every way you turn. There it is: data.

The amount of digital data that exists in the world today is staggering—and it's only going to grow.

According to IDC, as much as 64.2 zettabytes of data was created in 2020 alone. And that annual figure is expected to nearly triple by 2025.[1]

Of course, volume is hardly the only obstacle we face when it comes to managing and protecting our data. There's also the rise in remote work.

With as many as 25% of employees doing their jobs outside the office,[2] data will continue to travel across multiple locations and devices—making it harder to secure and raising the risk it winds up in the wrong hands.

How? Data breaches, for one.

3x The volume of data is forecast to grow by nearly three times between 2020 and 2025[3]

1. Worldwide Global DataSphere Forecast, 2021–2025: The World Keeps Creating More Data — Now, What Do We Do with It All?, IDC, March 2021
2. 25% of all professional jobs in North America will be remote by end of next year, Ladders, December 2021
3. Worldwide Global DataSphere Forecast, 2021–2025: The World Keeps Creating More Data — Now, What Do We Do with It All?, IDC, March 2021

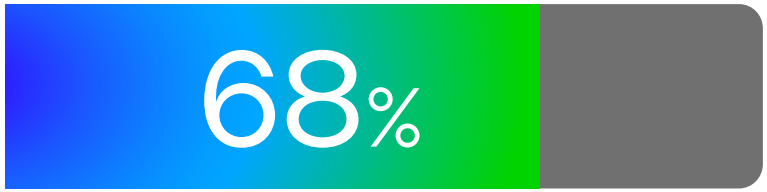
Data breaches can happen any number of ways:

- Employees taking inadvertent actions
- Hackers exploiting system vulnerabilities
- Nation-state actors attacking other countries

Regardless of how they occur, data breaches are an unfortunate reality many organizations must face. Especially today. Since 2020, data breaches have skyrocketed by 68%.[4]

This uptick in threats has gone hand in hand with a rise in regulatory requirements.

No matter their industry, organizations must comply with the latest data regulations and laws. Failure to do so could result in harsh penalties and fines. Those that operate in highly regulated industries—like finance, healthcare, and energy/utilities—face a particularly high cost for non-compliance.



The number of **data breaches** is up more than 68% since 2020[5]

4, 5. 16th Annual Data Breach Report, Identity Theft Resource Center® (ITRC), January 2022

The creation of complexity

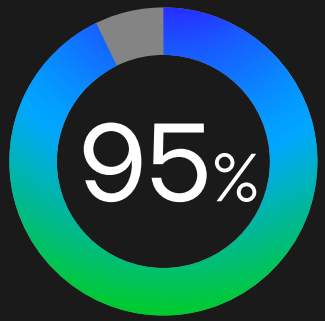
Simply put: more data + more remote workers + more threats + more regulatory requirements = more complexity

Many organizations today lack visibility into their most sensitive data. They struggle to control and manage data from devices to the cloud. They face great difficulty preparing for new data privacy laws.

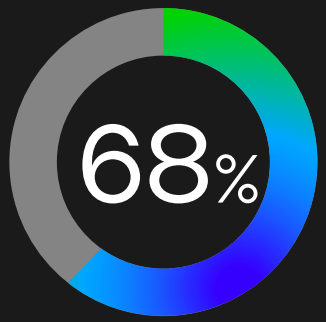
But they don't have to.

In the following pages, we'll open your eyes to the wonders of data loss prevention (DLP). If you don't already have a DLP solution, we'll show you why you need one. And if you're still relying on a lackluster, disjointed tool, we'll tell you why it's time to upgrade. Most important, we'll outline **the six must-haves you need to look for when considering a new DLP solution.**

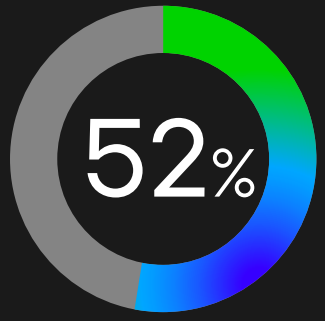
More data, more problems



of organizations cite the need to manage unstructured data as a challenge[6]



of business leaders say their cybersecurity risks are increasing[7]

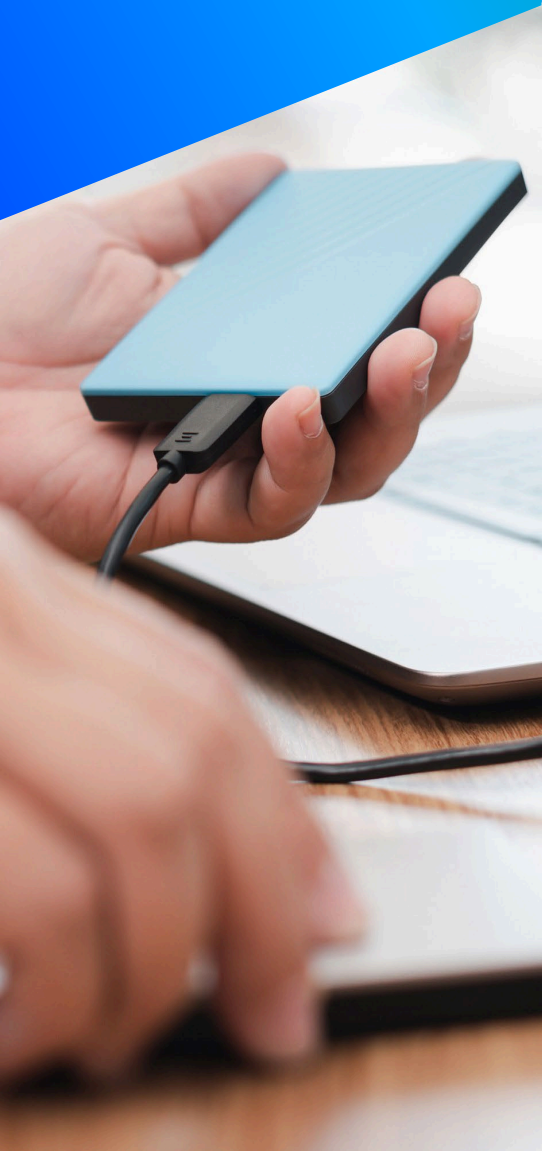


of organizations believe SecOps is more difficult today than two years ago[8]

6. Big Data Goes Big, Forbes, February 2019 7. The Cost of Cybercrime, Accenture, 2019 8. SOC Modernization and the Role of XDR, Enterprise Strategy Group, June 2022

Must-have #1

A robust compliance toolset



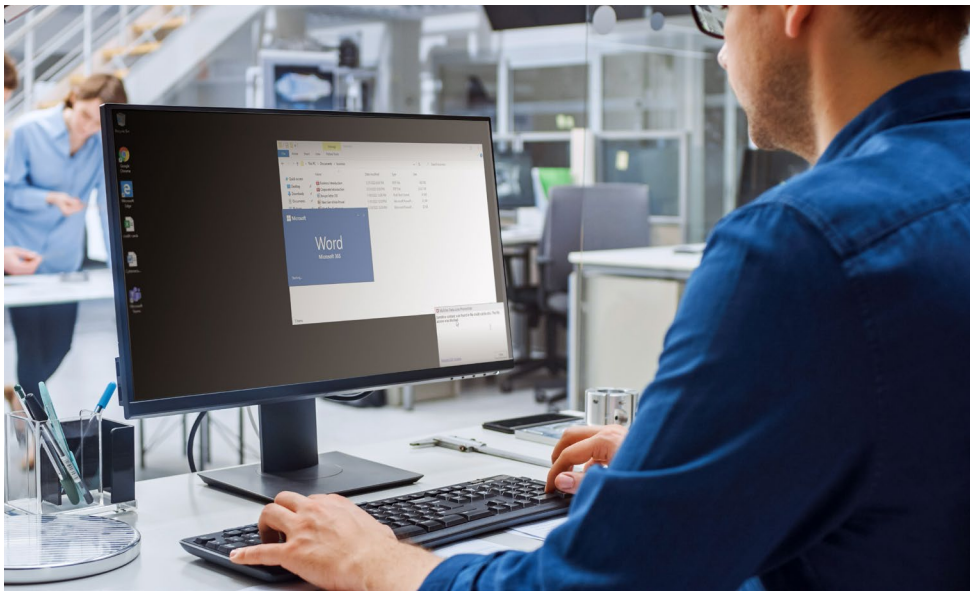
In today's business world, there are few things more valuable than customer data. Collecting information from current and prospective customers enables organizations to:

- Offer better services
- Create better products
- Provide better experiences

Clearly, data is a powerful tool. But with great power comes great responsibility.

Fail to protect your customers' information—and there could be serious consequences. Namely, financial ones. Non-compliance issues have cost some companies hundreds of millions of dollars.[9]

These costly penalties can do a lot more than just hurt your bottom line. They can lead to a significant loss in customer trust and irreparable damage to your reputation.



9. Amazon Gets Record $888 Million EU Fine Over Data Violations, Bloomberg, July 2021

Maintaining regulatory compliance

Today, there's a long list of regional regulations your organization must follow, including:

- The **General Data Protection Regulation (GDPR)** if you do business in the EU
- The **Act on the Protection of Personal Information (APPI)** if you have customers in Japan
- **Various state data privacy laws** if you sell to consumers in the United States

Then, there are industry-specific regulations, such as:

- **The Energy Policy Act** for energy/utility companies
- The **Gramm-Leach-Bliley Act (GLBA)** for financial institutions
- The **Health Insurance Portability and Accountability Act (HIPAA)** for healthcare providers

These aren't even exhaustive lists—and it's a lot to keep up with. With regulations constantly changing, organizations must be able to continually adapt. For many, the only way to do that is with a comprehensive DLP solution.

$888 million

is the single largest data protection fine ever levied against a company[10]

Does your current DLP product tick all the boxes?

The best DLP solutions enable you to:

- Automate content- and context-based classification
- Monitor and protect sensitive data, such as PCI, PII, and PHI
- Stay on top of policy changes with regularly updated rulesets
- Follow regional and industry guidelines with out-of-the-box compliance tools
- Empower employees to manually classify documents, adding another layer of security
- Conduct native, automated, customizable reporting to ensure you're staying compliant

10. Amazon Gets Record $888 Million EU Fine Over Data Violations, Bloomberg, July 2021

Must-have #2

Clear and complete visibility

Seeing is securing. At the very least, it's a pivotal first step. **For your data to stay protected, you need to have eyes on it.**

But considering the sheer amount of data your organization has to manage—combined with the countless other duties your SecOps team gets bogged down with—that's easier said than done.

On average, it takes 287 days for security teams to identify and contain a data breach.[11] That's too long.

Every second a threat's active in your network, you raise your risk. You increase your odds of exposing your customer's confidential information, your company's intellectual property, and more.

The right DLP solution can help—in a couple ways. When you offer security analysts a single-pane management view, they can:

1. **Gain greater visibility.** With a broader perspective of all your data, SecOps staff can more easily manage and protect your information.

2. **Increase efficiency.** Rather than switching between multiple apps, security experts can quickly detect, prioritize, and respond to incidents, all in one location.

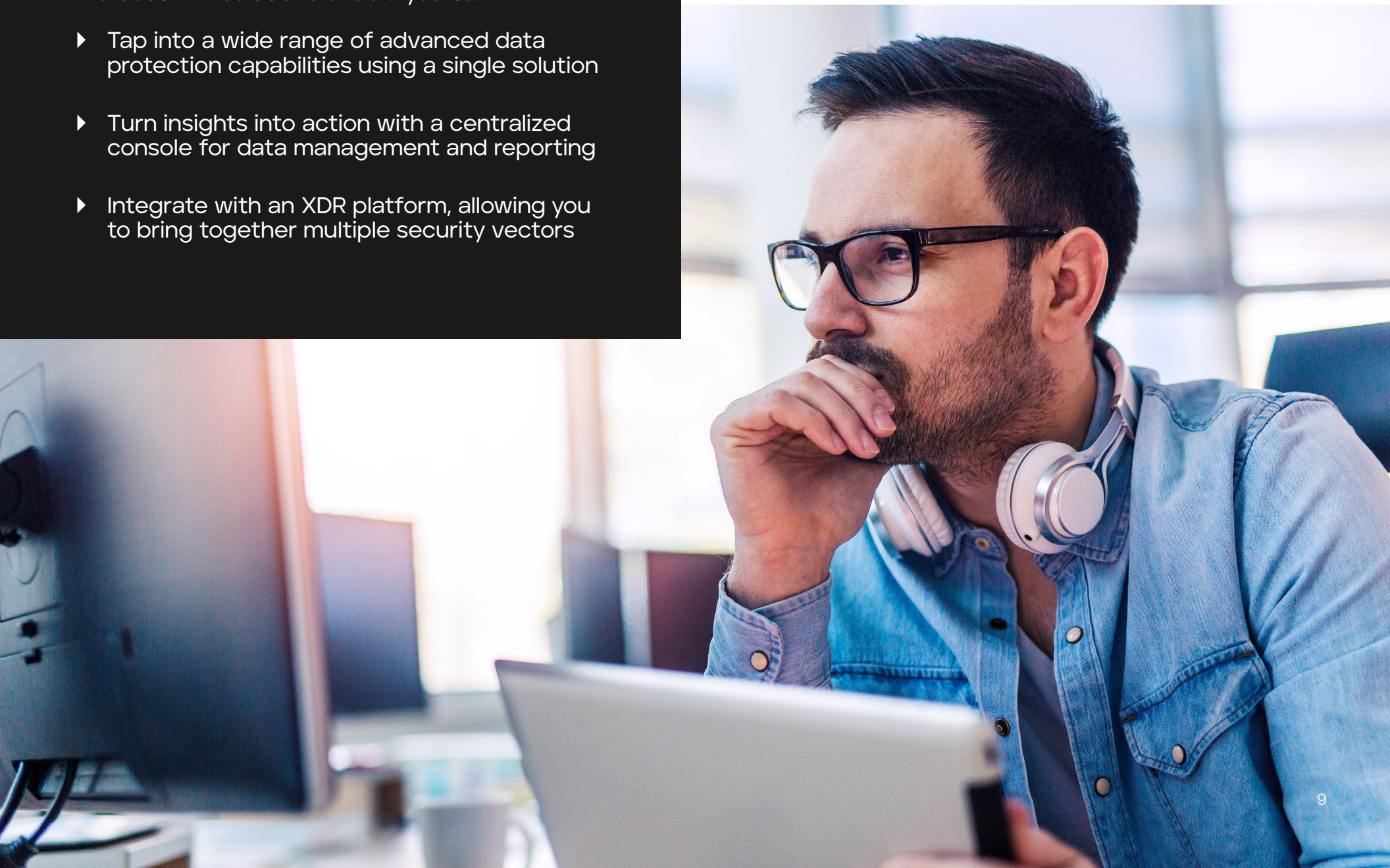
Why settle for just a small peek at your data —when you can see the big picture instead?

11. Cost of a Data Breach, IBM, 2021

Does your current DLP product tick all the boxes?

The best DLP solutions enable you to:

- Tap into a wide range of advanced data protection capabilities using a single solution
- Turn insights into action with a centralized console for data management and reporting
- Integrate with an XDR platform, allowing you to bring together multiple security vectors



Must-have #3

Simplified deployment and management

In cybersecurity, time is always of the essence. **The longer it takes you to implement your new DLP solution, the less time your tool's up and running—and the more time your data is vulnerable to attacks.**

Just imagine:

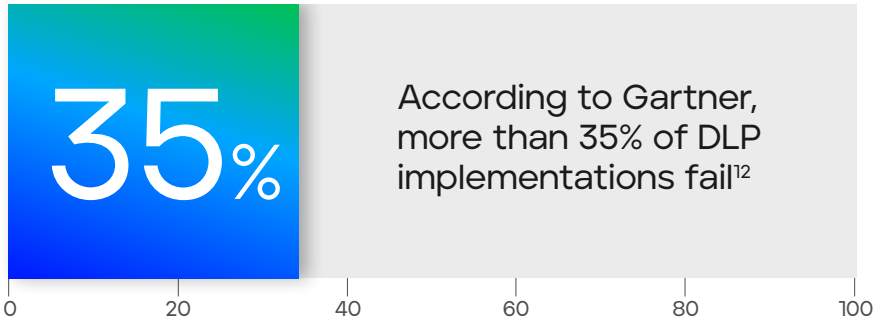
After months of research, you finally choose a DLP solution. It has all the features you could ever ask for—and then some. But there's a catch: it's incredibly hard to deploy.

So hard, it took your former colleague's organization over a year to stand it up. And your IT environment may be even more challenging.

Slowly, your implementation timeline grows:

- 9 months
- 12 months
- 18 months

Which means you'll have to continue relying on that outdated DLP solution you wished you could upgrade in the first place, at least for the foreseeable future. That very same product you were so desperate to move on from because it lacked the power to keep your data protected.



According to Gartner, more than 35% of DLP implementations fail[12]

12. Build a Successful Data Loss Prevention Program in 5 Steps, Gartner, February 2022

GARTNER is the registered trademark and service mark of Gartner Inc., and/or its affiliates in the U.S. and/or internationally and has been use herein with permission. All rights reserved. Graphic created by Trellix, based on Gartner research.

Long, laborious DLP implementations aren't the only thing you have to worry about. Perhaps an even bigger consideration should be how easy your product will be for your employees to operate every day.

The SecOps team responsible for managing your DLP solution? They already have enough on their plate:

- Monitoring threats
- Investigating incidents
- Remediating attacks

Protecting your organization from harm is a high-stress job that requires their full attention. Distractions are the last thing they need.

But choose the wrong product, and that's exactly what they'll get. Buried in false alerts—triggered by systems that are overly sensitive to user behavior—they could wind up spending too much time on noise and too little time on critical threats.

Don't worry, though. Not all DLP implementations are destined to fail. And finding a product that you can quickly operationalize, and customize in hardly any time at all, is entirely possible.

Does your current DLP product tick all the boxes?

The best DLP solutions enable you to:

- Stand up your product in weeks, not months
- Operate your system with minimal employee training
- Integrate with an XDR ecosystem, featuring native and open technologies
- Manage all policies from a centralized console, from monitoring to remediation
- Leverage built-in, customizable workflows, so you can get up and running fast
- Ensure accurate data detection with structured and unstructured data fingerprinting
- Take advantage of artificial intelligence and machine learning to stay ahead of threats

Must-have #4

Universal data protection

DLP solutions have come a long way in recent years. In the not-too-distant past, permission controls were far less sophisticated.

Essentially, a gatekeeper—someone like an IT administrator—would decide who was restricted from or permitted to view and share certain information.

There were two options:

1. Block access
2. Allow access

Easy, right?

But times have changed. **Today's workplace calls for a finer balance between protection and productivity.** Organizations house their intellectual property on the very same servers where employees keep their not-so-private resource materials.

These items—whether a financial plan, a to-do list, or a happy-hour invite—require different classifications. And your SecOps teams must be able to provide the right level of access to the right people under the right circumstances.

Secure your public and private data

With a modern DLP solution, you can **protect all your data, wherever it lives:**

- In the cloud
- On your network
- At your endpoints

And it doesn't matter if your information is in motion, at rest, or in use. You can be confident your data's secure.

The truth is, no data is created equal. Organizations maintain hordes of harmless information on their servers.

But for every press release meant for widespread distribution, there's a proprietary product plan intended for only a few select people to see. For every piece of marketing collateral meant for public consumption, there's a customer's social security number expected to remain private.

The more sensitive data you possess, the more important it is to have an effective DLP solution.

Data states, defined

In-motion data

Data that's actively traveling between locations—through email or IM.

At-rest data

Data that's reached its destination—in cloud storage or a shared folder.

In-use data

Data that's currently being accessed—through an open document or USB device.

Does your current DLP product tick all the boxes?

The best DLP solutions enable you to:

- Discover sensitive files, including OST and PST
- Educate employees on the proper handling of sensitive data
- Include unified rulesets between your endpoint and network
- Integrate with any commercially available email and web gateway product
- Prevent unauthorized external devices from connecting to your corporate network
- Prioritize and protect data with a wide set of controls using data classification models
- Monitor, detect, and defend across multiple vectors, including email, web, endpoint, and network

Must-have #5

Effective incident insight, response, and remediation

A variety of forces can do you harm—from phishing and spear phishing to ransomware attacks. But threats infiltrating your organization from the outside aren't all you have to be on the lookout for. There are a host of dangers lurking inside your organization, too.

Today, negligent employees are the root cause of most insider incidents.[13] Usually, it's because they:

- Fail to secure their devices with two-factor authentication
- Forget to update their software and install necessary security patches
- Ignore the company's security policies by sharing sensitive information on their personal devices

Any one of these actions can leave your organization's confidential data exposed. Then what?

The top 3 causes of insider threats[14]

1. Inadvertent or accidental employee behavior
2. Malicious outsiders stealing data by compromising insider credentials or accounts
3. A disgruntled employee manipulating the organization's systems, tools, or applications

13, 14. Cost of Insider Threats Global Report, Ponemon Institute, 2022

Every moment matters

When an insider or outsider threat strikes, you need to act. And fast.

You need to tap into the insights you have at your disposal to investigate your incident. You need to respond at a moment's notice to put an abrupt end to the attack. And you need to remediate the breach to limit any damage.

Research shows that SecOps teams take as long as 20.9 hours on average to respond to an incident once it's been detected.[15] That's nearly a full day.

The right DLP solution can help your organization accelerate that response by providing you with greater visibility and control over your entire threat landscape.

Not only that—a top-notch DLP solution empowers you to get to the bottom of what happened in the first place using detailed forensics. Plus, it allows you to modify your controls, so you can avoid similar fates in the future.

15. Voice of SecOps, Deep Instinct, 2021

Does your current DLP product tick all the boxes?

The best DLP solutions enable you to:

- Prevent and respond to both insider and outsider threats
- Mine data with forensic search capabilities to help catch critical data theft
- Differentiate between an organized campaign and a user mishandling sensitive data
- Support protocols like SMTP, IMAP, POP3, HTTP, LDAP, Telnet, FTP, IRC, SMB, and SOCKS
- Fine-tune policy control and forensics by capturing and ingesting data-transfer event information

Must-have #6

A strong, productive partnership

Choosing a new DLP solution isn't just about selecting the right technology. Yes, it's crucial to find a product that fits your every need—one that's chock-full of the various features your organization craves. But it's about way more than that. **It's about selecting the right partner, too.**

For the foreseeable future, you'll rely on your partner. You'll work side by side with their employees, seeking their guidance and expertise as you implement and use your product.

The level of support you receive from your partner should be top of mind as you choose a DLP provider.

According to Forrester, good customer service is the most important factor—outside of price and product—when deciding what to buy.[16]

In times of trouble, it's especially important for your partner to be there for you.

83%

of people agree that good customer service is a key factor when deciding what to buy[17]

16, 17. Getting to Know Your Customers, Forrester, May 2019

Find a partner you can count on

Can you imagine?

Two weeks into your DLP deployment, you notice a problem: a malicious app has accessed your privileged data. You stop the attack manually. But when you try to analyze the event information, your solution shuts down—again and again—preventing you from finding out the root cause of your attack.

You reach out to your partner by phone. No answer.

You shoot your sales rep an urgent email. No response.

You head to your partner's website for help. Nothing but bots.

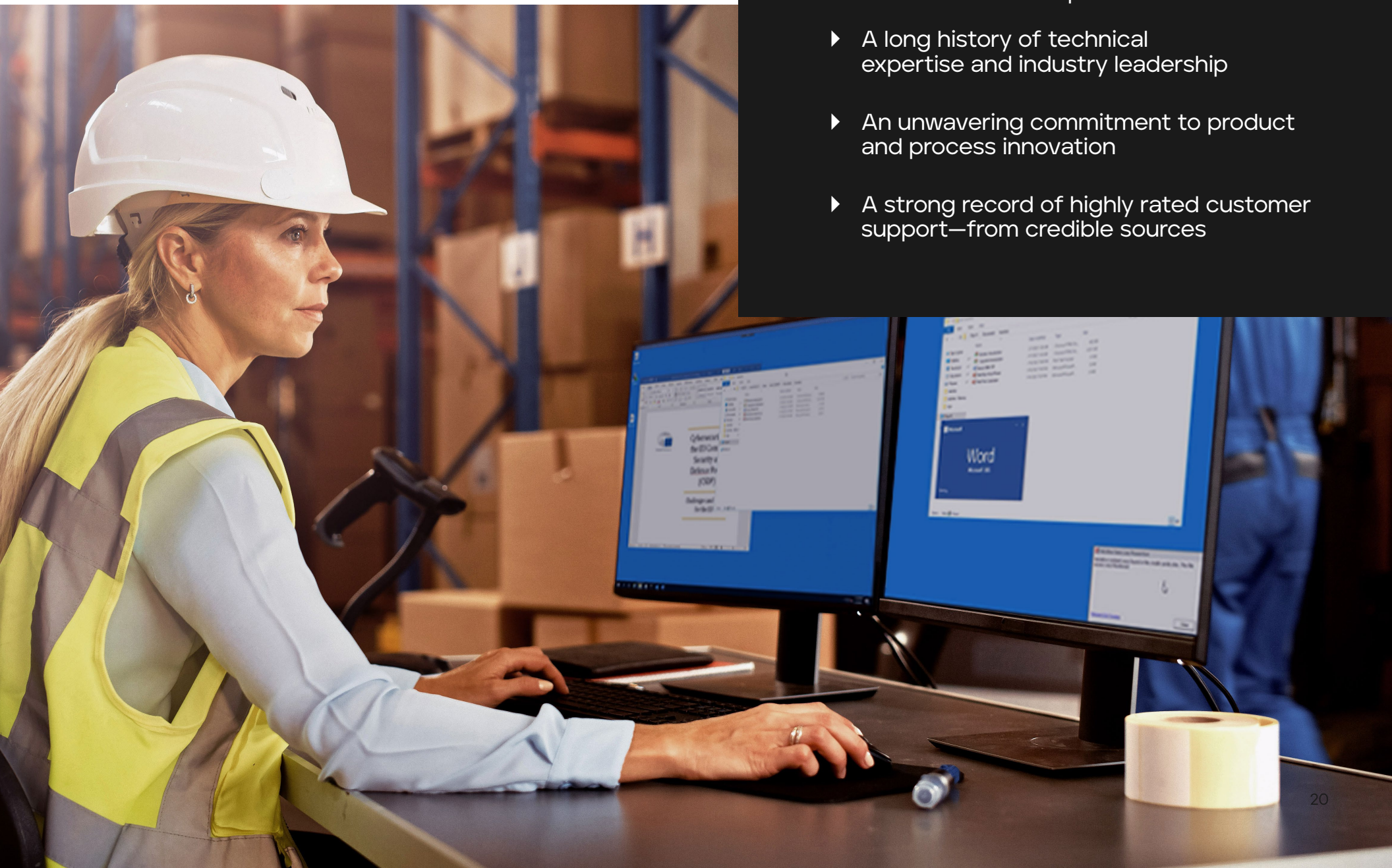
Worse yet: What if you discover that your partner is lacking in the innovation department? The solution they delivered is fine for the present. But in the face of today's rapidly evolving threat environment—is it truly fit for the future? There's no way you should have to adopt a new solution every few years to keep up.

The right DLP technology partner will never let you down like that. You can depend on them for steadfast support and tireless innovation, whether you have a simple question about a rarely used product feature or need more sophisticated threat intelligence.

Does your current DLP product tick all the boxes?

The best DLP solution provider should have:

- A long history of technical expertise and industry leadership
- An unwavering commitment to product and process innovation
- A strong record of highly rated customer support—from credible sources



What makes Trellix DLP different?

Choosing a DLP solution isn't a decision you should take lightly. In the face of today's dynamic threats, protecting your data is vital. Keeping your information safe can be the difference between your organization flourishing or floundering. So you need to make sure you make the right choice.

As far as we're concerned: **your search for a preeminent DLP solution is over.**

Trellix offers exactly what you need. We combine the best-in-class technologies and extensive expertise of two industry leaders: McAfee Enterprise and FireEye. This enables us to deliver a whole new standard of data security.

And every day, we continue to build upon our solid foundation—investing in our threat research, growing our product portfolio, and advancing our solution capabilities.

Our comprehensive DLP suite includes solutions that span discovery, monitoring, prevention, and endpoint protection. By integrating our offerings, you can reduce the risk of data loss and strengthen your security posture.

Comprehensive visibility. Unified control.

Discover

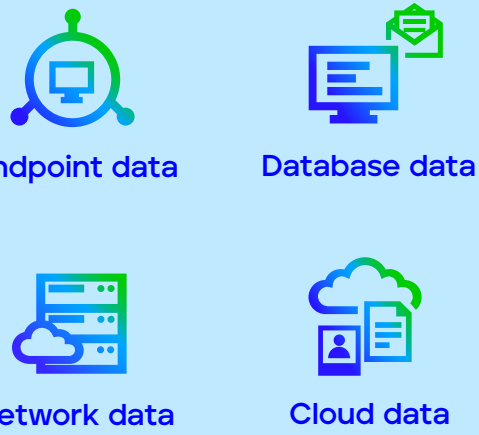
Easily locate, inventory, and secure your sensitive data.

Classify

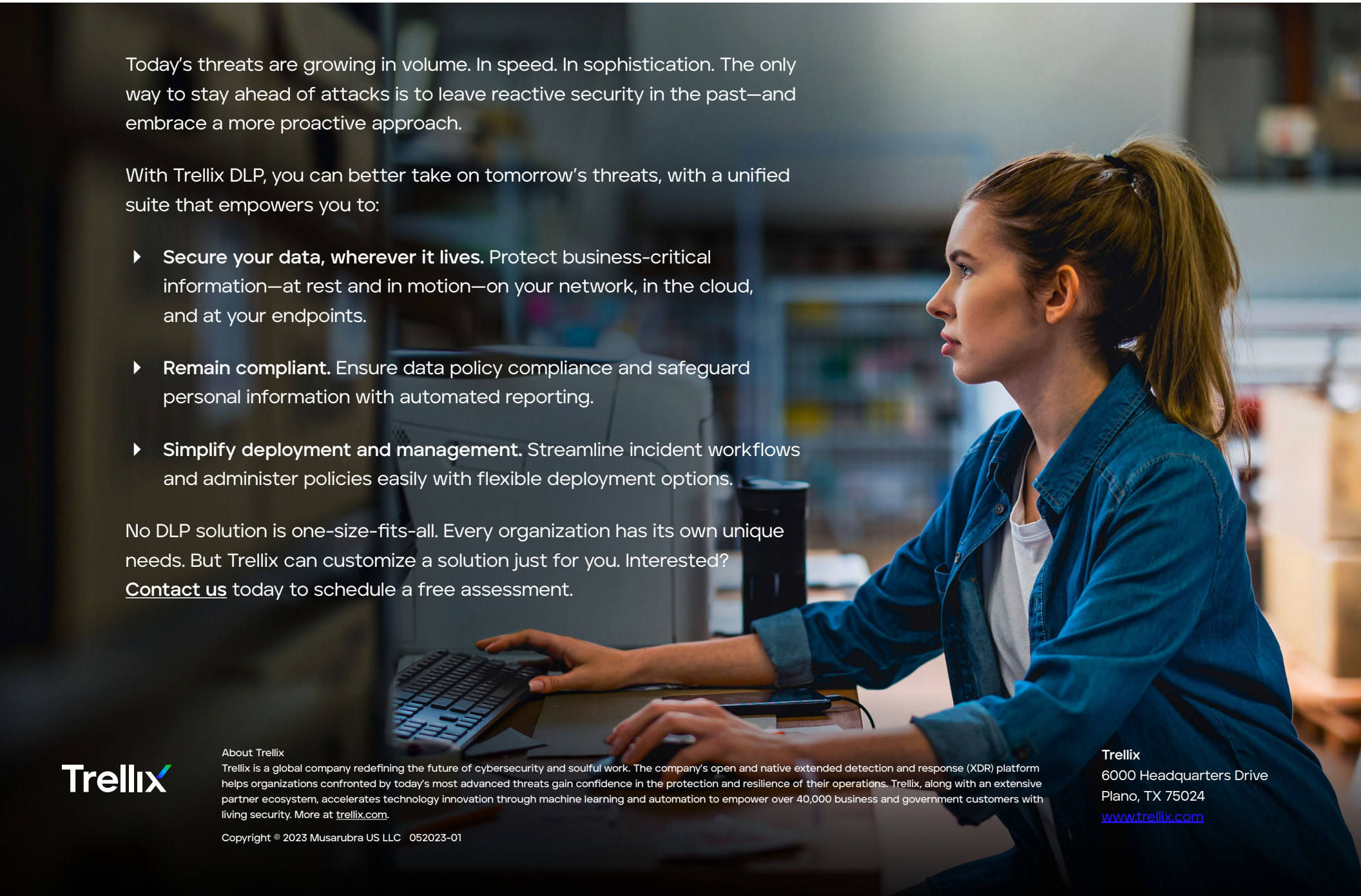
Add a layer of protection with manual or automated classification controls.

Protect

Educate employees and secure data across multiple vectors.



Take on tomorrow's threats with Trellix DLP



Today's threats are growing in volume. In speed. In sophistication. The only way to stay ahead of attacks is to leave reactive security in the past—and embrace a more proactive approach.

With Trellix DLP, you can better take on tomorrow's threats, with a unified suite that empowers you to:

- **Secure your data, wherever it lives.** Protect business-critical information—at rest and in motion—on your network, in the cloud, and at your endpoints.
- **Remain compliant.** Ensure data policy compliance and safeguard personal information with automated reporting.
- **Simplify deployment and management.** Streamline incident workflows and administer policies easily with flexible deployment options.

No DLP solution is one-size-fits-all. Every organization has its own unique needs. But Trellix can customize a solution just for you. Interested? **Contact us** today to schedule a free assessment.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at trellix.com.

Copyright © 2023 Musarubra US LLC 052023-01

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com