Enterprise Data Protection Solutions, Explained

What You Get with Six Leading Vendors

Forcepoint

Brochure

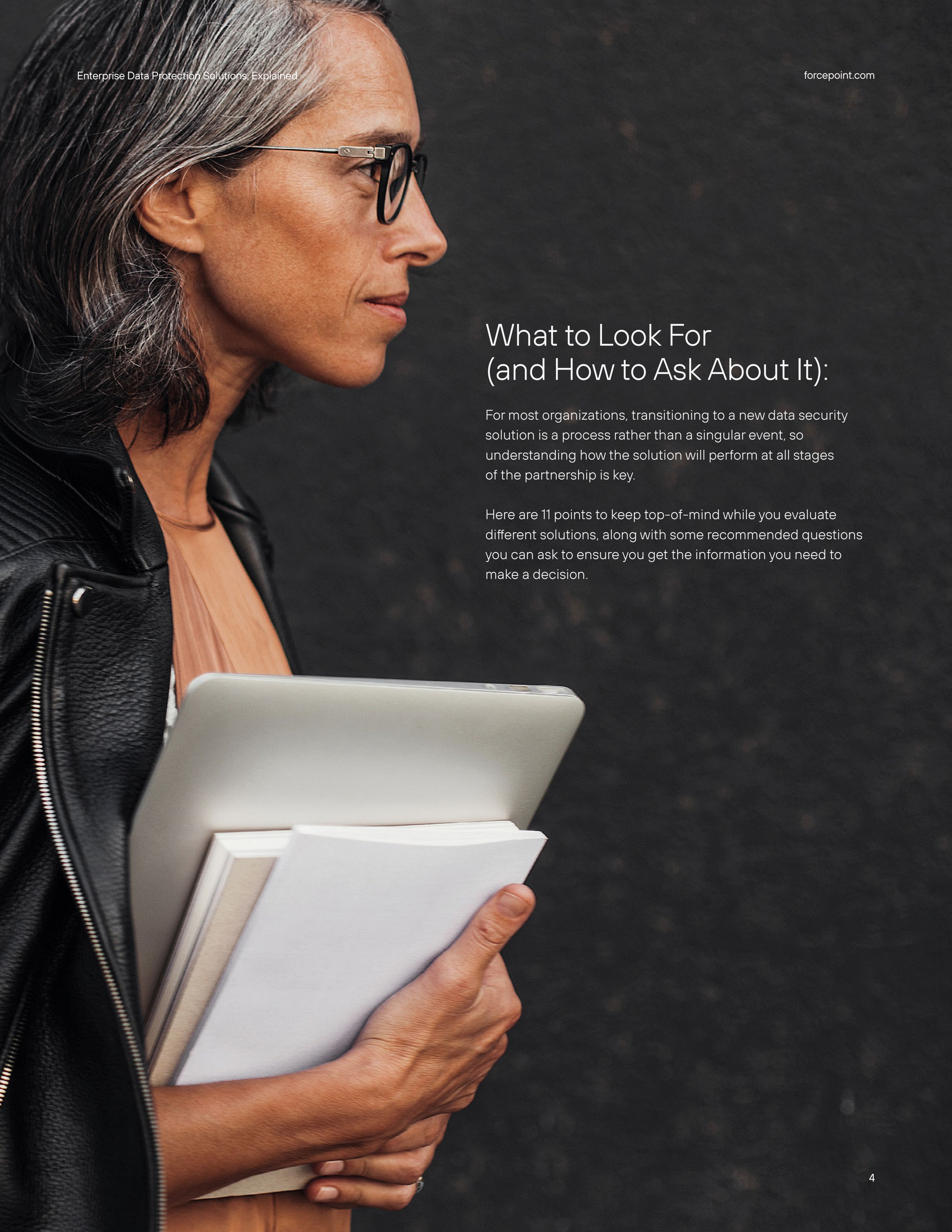
forcepoint.com

What’s Inside:

The value of data protection in business today is hard to overstate, tied to critical assets like intellectual property, competitive advantage, brand equity, financial stability, and customer trust. With so much at stake, choosing a new data protection partner—or replacing an existing one—is a significant decision. That's why we've created this guide to take the guesswork out of evaluating the leading enterprise solutions and help you choose with confidence.

In it, we'll cover:

- Key criteria to look for when weighing different solutions
- Questions to ask to ensure you're getting a clear answer
- Side-by-side comparison of enterprise data protection solutions



What to Look For (and How to Ask About It):

For most organizations, transitioning to a new data security solution is a process rather than a singular event, so understanding how the solution will perform at all stages of the partnership is key.

Here are 11 points to keep top-of-mind while you evaluate different solutions, along with some recommended questions you can ask to ensure you get the information you need to make a decision.

Ease of Implementation

Bringing on an enterprise data protection solution shouldn't feel like starting from scratch, so consider its compatibility and integrability with your current solution and ask how it will interface with systems you already have in place. Additionally, advisory services that help you control access to toolsets and implement new policies that work for you with little (or no) modification can be extremely helpful in shortening your time-to-value.

Support and Services

To accelerate the time it takes to start realizing value with a new solution, you'll likely need to learn how to use it while also making preparations for deployment across your business. Having a direct line to an account manager who can advise you on how to leverage the detailed capabilities of your new toolset can be key to shortening your time-to-value. Additionally, a full-service option to manage, evaluate, and optimize your setup continuously can help ensure you get the most value.

Ask:
Will we have a Customer Success Manager or Technical Account Manager who is **dedicated to our organization?**

Deployment Models

Many organizations prefer to deploy data protection on-premises to start, but making sure you have a solution that can support cloud or hybrid capabilities as well will provide the opportunity to scale and help avoid slowdowns in the future.

Ease of Use

Depending on a collection of different tools to protect data in your network, at endpoints, and in the cloud can be cumbersome to manage and can create gaps and inefficiencies in your strategy. Look for a solution that gives you visibility into how all your data is used, moved, and protected, at the user level.

Ask:
Will we have **one centralized view** of policies across the entire enterprise?

Compliance

Achieving regulatory compliance means organizations need to be able to audit all capabilities independently, produce reports, and control the flow of data based on pre-built policies. Having an easy way to look back into activity—by user, not by siloed event—is the best way to go above and beyond in compliance and will help you confidently manage the process.

Ask:
Is it simple to manage the reports I need for audit and compliance?

Audit & Block

Check for capabilities that can retroactively audit data loss incidents and proactively block data from being compromised in the moment—on all channels. This ensures that you can learn from past incidents and use them to optimize your blocking policies in the future.

Visibility into User Activity

Being able to track activity to the individual user is critical for monitoring exfiltration across channels including email, cloud, web, and endpoint, as well as for identifying credentials that were compromised via phishing or other such attacks.

Ask:
Can I detect threats at the user level?

Customization Flexibility

Any custom applications you use to facilitate collaboration with other organizations, partners, or third parties should be represented in your data protection strategy. Ensure that your new solution has the ability to implement controls for those apps in a timely manner.

Ask:
How broad is your cloud application visibility, and does it include custom apps?

Roadmap

The nature of data security threats is evolving every day, so a dynamic solution that's built to grow with the needs of the market is critical. Even if a solution has what you need now, always ask about what they have planned for the future to ensure you understand their level of commitment to innovation and adaptation.

Analyst Performance

Analysts such as Gartner and Forrester have visibility into different solutions' features, capabilities, product roadmaps, and more—details that you would be very lucky to find on a website or even a sales call. These will make it simpler for you to compare different tools in a consistent manner.

Pricing Transparency

The way different solutions are packaged can be complicated, and some features—even a provider's flagship offering—may not be included in all licenses. Ensure that the ones that are most important to you are covered in any price you're quoted.

We've given you a lot to consider here, but understanding what different solutions include—as well as *how* they address your needs—will help ensure that you stay excited about your new solution as you use it. You'll want to dig into every point in detail, but this overview will help you figure out where to start asking questions.

Charting Your Options

	DIGITAL GUARDIAN	FORCEPOINT	MCAFEE	NETSKOPE	PROOFPOINT	SYMANTEC
Alert prioritization	●	●	●	●		●
Automated policy enforcement	●	●	●	●	●	●
Cloud app protection		●	●	●	●	●
Cloud protection		●	●	●	●	●
Compatibility with classification vendors		●				
Converged network and endpoint protection	●	●	●			●
Database support flexibility		●	●			●
Data discovery across all environments		●	●			●
Data protection integration across web, email, network, endpoint, and cloud		●				
Drip DLP		●	●			●
Native behavioral analytics		●				
Native remediation		●	●	●	●	●
On-prem, cloud & hybrid deployment	●	●	●			●
Off-network policy enforcement		●				
Risk-adaptive protection		●	●			●
Risk-based policy enforcement		●				
Single-console control across all environments		●	●			●
Structured and unstructured data fingerprinting and optical character recognition	●	●	●			●
Uniform policy enforcement		●				●

Solution Summaries

Digital Guardian is a data protection provider that can be deployed on-premise, in the cloud, and in a hybrid model. Environment set up takes just as much effort and time as their peer set, but doesn't offer such a robust feature set. Organizations with more straightforward data protection needs would benefit most from their offering.

McAfee has recently shifted their focus from web security to "cloud/data security," providing robust data and antivirus solutions with separate consoles to control networks, endpoints, and the cloud. Its feature set prioritizes threat-centric policies that are consistently enforced, regardless of user behavior.

Netskope is a CASB solution with URL filtering capabilities, focused primarily on protecting against data exfiltration from the cloud. It has limited cross-environment capabilities and provides the most value to organizations who are looking to augment their existing solution set with cloud security.

Proofpoint is a cybersecurity solution dedicated to protecting data usage in mobile or remote environments including cloud, email, web, and social media. It has strength in email security and addressing phishing concerns, and is most valued by organizations seeking a cloud-centric solution.

Symantec is a comprehensive data protection provider with robust cross-environment capabilities. It enforces security policies in a uniform fashion across environments regardless of user behavior or risk level. Mid-market organizations may find that managing it requires significant investment of time and talent.

The Forcepoint Difference

Forcepoint’s unique combination of converged cross-environment data loss prevention, behavioral analytics (UEBA), and risk-adaptive policy enforcement is the most comprehensive data security solution for companies undergoing digital transformation, now or in the near future. We are the only partner that can dynamically adjust and enforce policies based on user risk, preventing exfiltration events, reducing false alerts, streamlining workflows, and keeping precious resources focused where they’re most impactful.

First Steps with Forcepoint

Forcepoint's phased implementation process is designed to shorten partners' time-to-value. A robust library of pre-architected policies to govern safe data usage on your network, at endpoints, and in the cloud ensures that you can stand up your new solution in a timely manner, with complete customization abilities to allow ongoing optimization.

What We Provide

- The industry's most extensive library of prebuilt, customizable policies to speed your implementation across cloud, endpoint, and network
- Personalized account management rooted in our understanding of your timeline and needs
- A direct line to industry experts with ongoing guidance on data protection best practices

How You Benefit

- Proactive security posture allows an organization to go beyond audit-only based on risk to prevent data loss within your organization
- Employee productivity is increased by allowing unfettered access to data across all channels when user risk is deemed low
- Thoughtful implementation partnership with industry experts allows you to realize returns on your investment quickly

Are you ready to learn how Forcepoint would approach risk-adaptive, human-centric data protection for your organization?

Connect with one of our experts to start talking about your unique needs.

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.