FORTRA™

The CISO's Guide to Enterprise Security Migration

Why Read This Ebook?

Security solutions need to work for both your business and your employees. But if you find that your solutions interrupt workflows or aren't adequately protecting your data, making timely and efficient changes before a security incident occurs is crucial. Read this eBook for tips on navigating the migration process without compromising security.

Just **1 in 10** organizations says their current security solutions fully meet their needs.

Nearly **9 out of 10** companies have insufficient budget space to implement effective cybersecurity systems.

Table Of Contents

PART ONE

Key Steps Before You Talk to Any DLP Vendors

Why Companies Stick With Broken Security Solutions

Information security professionals are tasked with evaluating, implementing, supporting, and perfecting a myriad of solutions. The challenge comes when one (or more) of those solutions no longer meets the needs of the business. Here's 5 common reasons why these solutions remain in use long after they've outlived their usefulness:

1 Lack of Trust

2 Exhaust Old Before New

3 Skills Shortage

4 Cultural Divides

5 Budget

Next, we'll explain each and how to address them... →

Why Companies Stick With Broken Security Solutions

1) Lack Of Trust:

Organizations often use security solution-related buzzwords to sound more trustworthy and knowledgeable than they actually are, leading to mistrust in the market.

What to do about it:
Focus on your organization's needs now and in the future, and ask the vendor how they can address those needs in your language, not theirs!

2) Exhaust Old Before New:

When new security requirements arise, it's only natural to see if your organization's existing security technologies can be further tuned to address those needs.

What to do about it:
Be ruthless when it comes to your security solutions and their ability to meet organizational needs. It may be time to find new ones unless you can prove that your current solutions can adapt to new requirements.

3) Skills Shortage:

New technology projects take time to research, test, purchase, provision, operate, etc., but organizations may not have the time or resources to go through such a lengthy process.

What to do about it:
Look to external sources that have done the research to get you started. Peers, online review sites, analyst reports, and calls can save you hours of trial and error.

4) Cultural Divides:

As your organizational model shifts and newer technologies are required, this may generate a divide among the traditional IT functions.

What to do about it:
DE&I efforts within your business can help drive fresh ideas and thinking to solve new problems. Try to second-guess thoughts that hinder progress like "that's not how we've done it in the past…"

5) Budget:

Deploying a new security solution can be expensive. That's why it's critical to determine whether or not the benefits of the new solution will outweigh the cost of investment.

What to do about it:
Gain an understanding of how your organization makes money and tie new solutions to that as directly as possible. Get business line leaders to advocate for you.

“We Don’t Have Time To Do It Right, But Plenty Of Time To Do It Wrong!”

> *When providing secure access to public cloud apps for remote or mobile users, an alarming 34% of survey respondents said they must publicly expose private apps in the public cloud in order to provide access.*
>
> *– 2023 Zero Trust Security Survey from Cybersecurity Insiders and Fortra*

Why You May Need To Make A Change

Regardless Of What You, As An Information Security Professional Can Control, There Are Certain Factors That May Force The Decision For You:

- Underperforming Solution
- Business Model Evolves
- New Attack Vectors
- More Secure Solutions
- Lack of Vendor Support
- Lack of Mobility
- Lack of Insights & Information
- Lack of Integration Support
- Compliance Requirements
- Lack of Skills Internally

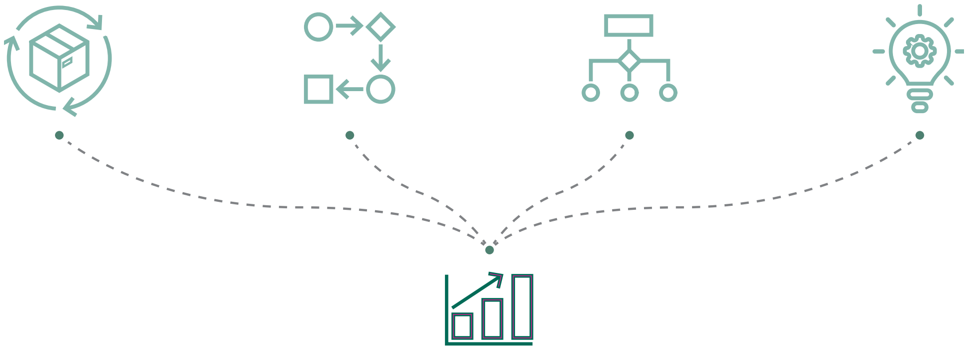
Next, we'll explain each and how to address them... →

PART TWO

How To Gain Confidence & Support To Make The Change

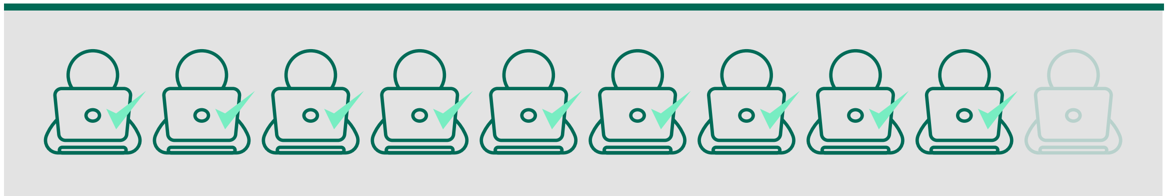
TIPS from the Experts

Enterprise security is not about deploying and maintaining tools. It is **about knowing how your business runs,** what data and apps are vital for it to add value to its customers, while fostering a strong risk management strategy to protect those assets.



Process First, Technology Second

Getting your process in order first helps you focus on what matters most – what you and your business need – not what a vendor has to offer.



Almost 9 out of 10 of buyers want to self-serve part or all of their buying journey.

Due to the pandemic, **33% of buyers** spent more time researching products before making a purchase this year.

49% of buyers spent time doing extra research because of data security concerns.

Source: TrustRadius - The 2021 B2B Buying Disconnect

Process First, Technology Second

- 30% of organizations deploy more than 50 cybersecurity-related tools on their networks, and nearly a quarter of those organizations deploy more than 100 tools.
- Deploying more solutions does not always lead to greater cyber resiliency, however, as 37% of organizations believe they have too many security solutions in place.
- Meanwhile, 33% of organizations believe they don't have enough security solutions in place, while only 30% believe they have the right number of solutions to achieve cyber resiliency.
- Rather than fixating on the number of security solutions your organization deploys, focus your organization's efforts on the decision-making process instead.

Source: "IBM Cyber Resilient Organization Study 2021"

> *Mature security teams are investing heavily in a couple key categories. So as an organization, I would ask, "Where am I not investing, and why?" Understand your points of weakness and your risk in those areas, and get a strategic plan around trying to solve those gaps.*
>
> *– Cary Hudgins*
> *Director of Product Management, Fortra's PhishLabs*
> *CISO Perspectives: Data Security Survey 2022*

What to do Before You Contact Any Vendors

The list of things to do before contacting a vendor can seem daunting, but it will prove beneficial and prevent the "changing the tire while driving" scenario that leads nowhere good.

1. Define the problem you are trying to solve and the criteria you intend to use to judge the solution
2. Establish what matters to the various stakeholders – what the CISO cares about and what the VP of Sales cares about may be very different, but you need a common language to evaluate
3. Create a scoring system on functionality that allows people to adjust weightings
4. Set milestones for the internal process and the external process
5. Create a cross functional project team
6. Seek guidance from peers. Look to similar and dissimilar roles/industries
7. Look to online reviews
8. Seek industry analyst guidance, many of whom are regularly briefed by vendors
9. Make a short list of vendors you're interested in
10. Develop an RFP (Request for Proposal) document

TIPS from the Experts

Having a ton of market leader security tools will not make your enterprise secure or prevent a breach if they’re not deployed properly.

You need to first arm yourself with knowledge of where your critical data resides and the systems that store it in order to fully utilize these solutions for maximum protection.

PART THREE

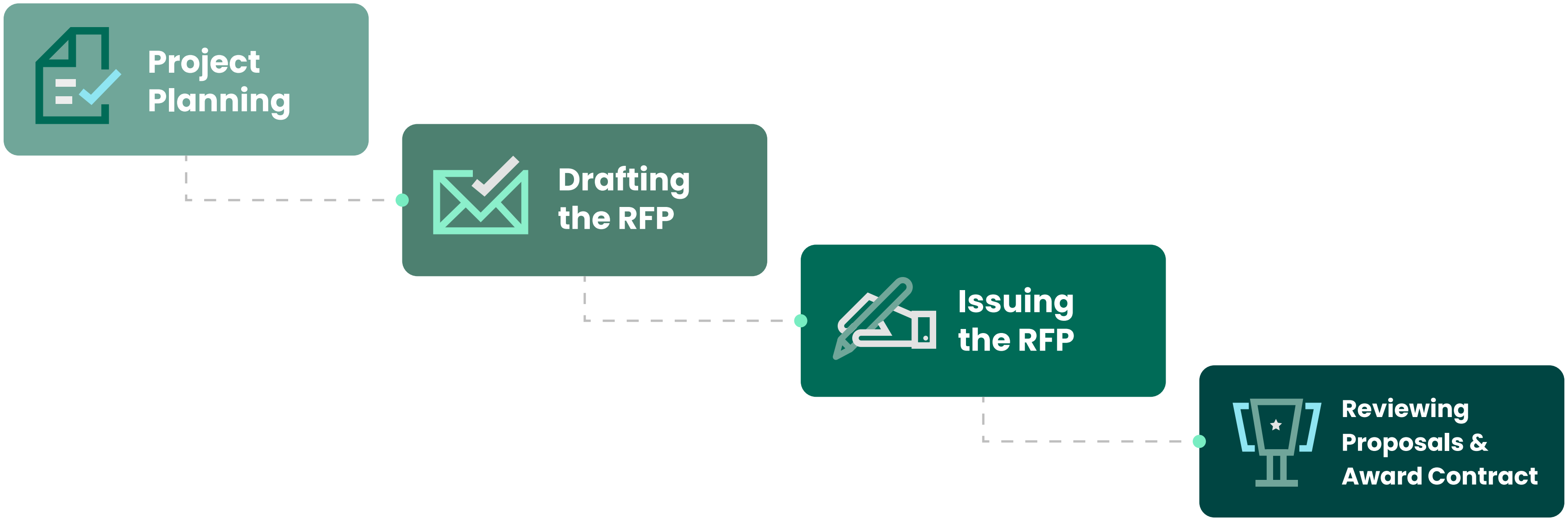
Structure Your RFP Process For Success

An RFP is a Lot of Work... It Doesn't Have to Be

Bite off as much as you can, whatever prep you do will pay dividends to the business and improve the overall decision-making process.

1. RFPs help meet organizational needs & forces you to define requirements
2. Allows for comparison of one system/solution to another using consistent criteria
3. Gets control of product demonstrations
4. Gets you to think about return on investment
5. Produces an organized selection methodology

Structure Your RFP Process for Success



Project Planning

Drafting the RFP

Issuing the RFP

Reviewing Proposals & Award Contract

Project Planning

Project Planning

1. **Requirements Scope** - Start by examining the features of the existing software that are used and rewriting them into requirements. Look to the broad base of people within the business to ensure you get the full picture. From the admins to the end users, each has a role to play in defining the scope This process of reverse engineering requirements from the existing features is critical to ensure you don't regress on functionality when you see something new and exciting in a potential replacement platform and ignore what you use today.

2. **Alignment with Business Strategy** – How does your business operate today? What are the things that make it unique? Are you a highly seasonal, retail business where even a few minutes of downtime during the holiday shopping crunch can mean millions? Align the project with the business goals, calendar, and future plans. Are there any major shifts planned? Be aligned with the leadership team and use security solution as a growth accelerator!

3. **Budget** – You never have enough time or money but knowing how much you have sets the guardrails on the project. Don't evaluate a $100mm solution when you have a $100k budget. It wastes your time and creates unrealistic expectations. Understand how that money can be spent too. Opex vs Capex can drastically change budgeting.

> *"Software selection is like painting a building. The real work is in the preparation, not the selection."*
>
> *– Unknown*

Project Planning

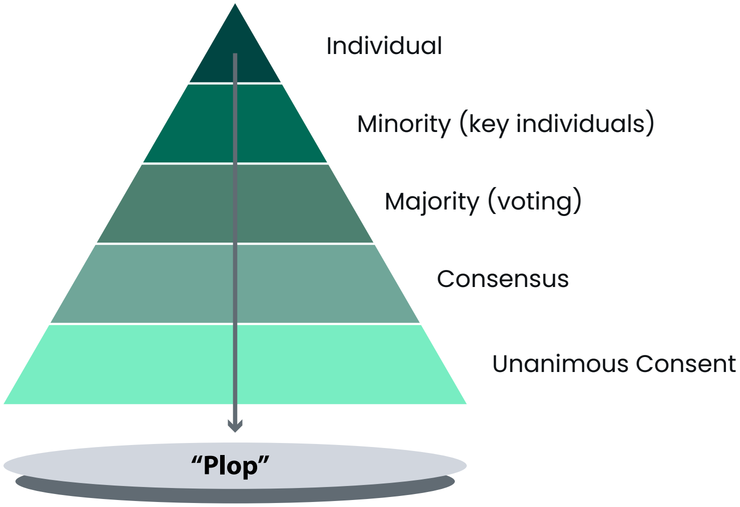
4. **Timeline** – What compelling event, if any, is driving the evaluation and how can you respond as quickly as needed to address it. If you've been breached, the timeline may be accelerated, if a business peer has been breached, there may be even higher urgency. Transparency throughout the business will avoid nasty surprises. Timelines should be set up front but be realistic about them and allow for slippage when the inevitable happens.

5. **Stakeholders and Review Panel** - Who is going to be part of the evaluation process and the decision process. More input is good, to a point. You need technical and non-technical people involved. Each party should know what their level of involvement is and how the final decision will be made. The RACI model can help organize the roles and keep the order. Get them on board and involved early.

6. **Scoring Criteria and Review Process** – How will the points be assigned and how will the weighting work? Who wants what, and how important is that to them? Does anyone have override authority? Who breaks the tie if it happens? How will you document the procedure so that when the time comes all know what to do and stay to a consistent process? A blend of quantitative/yes/no and qualitative questions allows for objective and subjective data and will give you a more complete picture of capabilities.

Project Planning

The Six Types of Team Decisions



Drafting The RFP

1. **Introduction**
2. **Statement of purpose**
3. **Background information**
4. **Scope of Work**
5. **Project Schedule**
6. **Contract Terms and Conditions**
7. **RFP Timeline and Review Process**
8. **Requirements for Proposal**

Drafting the RFP

Set the stage for the RFP with the details that you and the team already agreed upon, but that the potential vendors have no insights into, yet. The more thorough you are here, the better tailored the responses will be. You'll also eliminate vendors that can't compete.

- Who is the lead, who else is involved
- Why is this happening and why now?
- What's important for the vendors to know?
- How do you box in the project?

The nuts and bolts of an RFP, such as schedule, T's & C's, and other requirements are a great filter. The last thing you want is to invest time with a vendor, award them the business, and have them tell you that their delivery timelines are well outside your window.

Issuing The RFP

1. **Creating the Shortlist of Vendors**
2. **Distribution to Networks**
3. **Take 60 Seconds for Yourself**
4. **Coordinate Responses and Answer Questions**
5. **Receive Submissions**

Issuing the RFP

Getting a proper response means delivering the RFP to the right selection of vendors. You need to make the list manageable, but comprehensive enough to get a feel for the breadth of capabilities. Be sure to give a reasonable and equitable time to respond. Once it's out there, you can take a breath for a minute before the questions come back from the vendors and the responses come in.

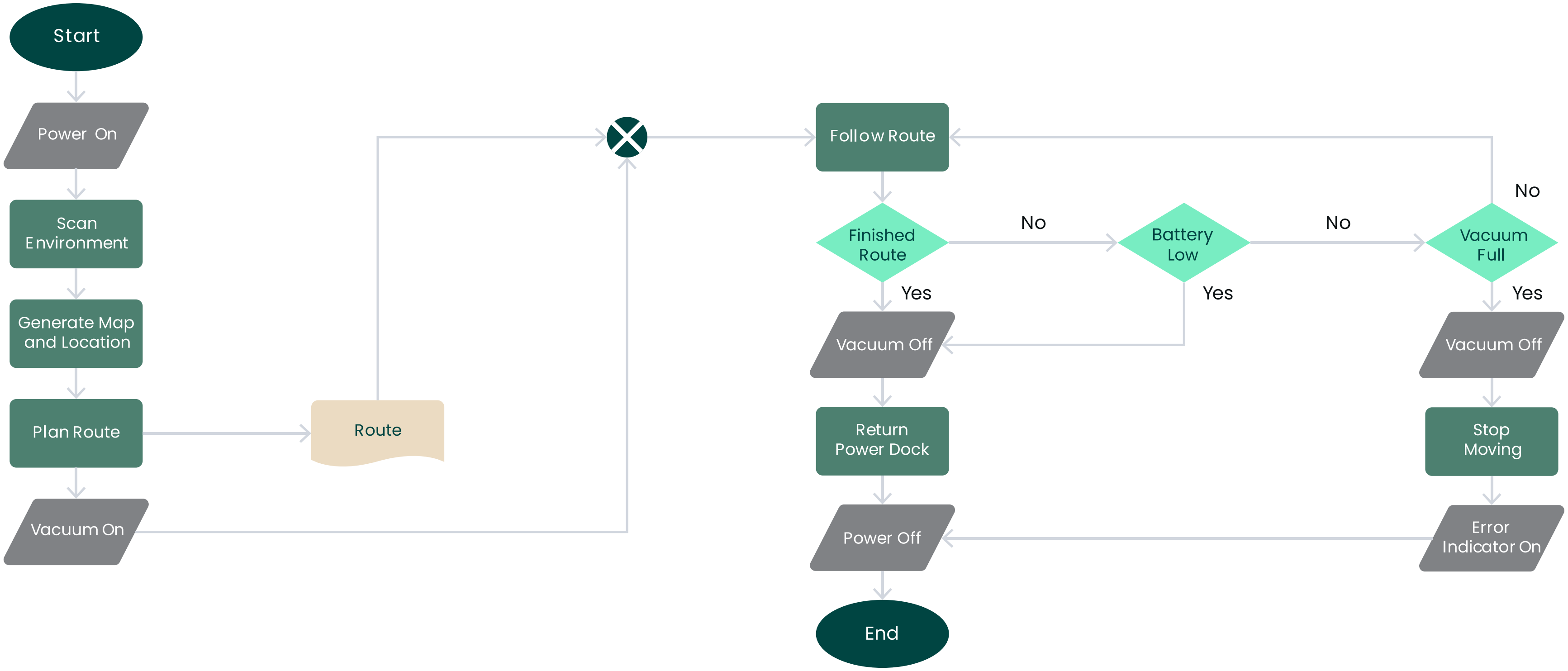
TIPS from the Experts

Use conferences and exhibitions you attend intelligently. InfoSec conferences can be beneficial if used in the right direction. Arrive with a plan to view each product you're interested in.

Virtual events add a new wrinkle. They can be helpful given most are now free and none require the time away, but the lack of face-to-face conversations adds new challenges.

Don't Get Stuck in Analysis Paralysis

The reason you invested time up front in the RFP process was to have a plan ready to go when the responses came in. Now you can execute (and refine if needed) on that plan. Even if you need to modify, you have something to start with and that the other stakeholders provided input on and bought into early in the process.



Reviewing Proposals & Award Contract

1. **RFPs Scored**
2. **Finalists Selected**
3. **Interviews & Reference Checks**
4. **Best and Final Offers Submitted**
5. **Contracts Awarded**
6. **Final Legal Clarifications Complete**
7. **Other Bidders Notified**

Reviewing Proposals & Award Contract

Refer to your scoring matrix you created early on and begin the process of scoring, then ranking each of the vendors based on their submitted answers. How do the vendors rank relative to what's most important to your business needs? If you want to eliminate some bias, you can have a neutral party in your business receive and anonymize the responses. Any questions back to the vendors should be aggregated then submitted together.

Once you're happy with the scoring, you rank them and select the finalist(s). Depending on the scope of the project reference checks, interviews, price negotiations, etc are all the final stage before awarding the winner.

The vendor's provided references are good, but use your own personal network to find unofficial references to boost comfort level.

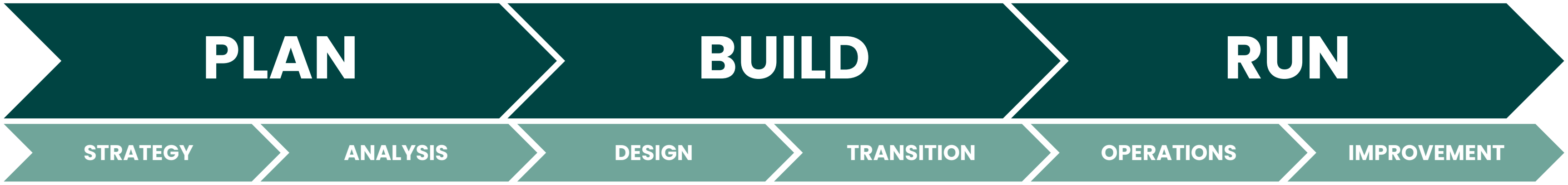
Once you and the selection committee are satisfied with all the responses and have decided on the winner, you get to make one of the teams happy. Depending on the breadth of the contract, some final legal work may be needed, but given the time invested thus far, both sides should be eager to come to an agreement on any issues and get down to business.

Alas, with any competitive situation, there are those that didn't win the bid. Common courtesy suggests you notify them all in a timely manner. Some may request a feedback call with you to inquire areas they needed to improve. The decision about that rests with the team, though it does help the vendor learn what gaps they have and if they can even address them.

PART FOUR

Putting It Into Production

Develop A Migration Plan For The New Technology Being Deployed



You and the team have spent time researching the business needs, documenting them in the RFP, evaluating the responses, and finally, selecting a winner. Don't let all that hard work go to waste, make sure you and the vendors have a migration plan before you do anything else. The three big phases, Plan, Build, and Run have 6 sub-phases.

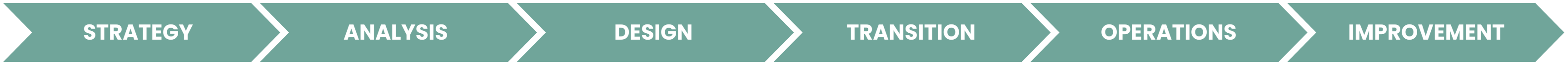
Plan – Work with the vendor's team and your project team to document key elements of the deployment. Dedicating time here will help keep the process on track and prevent "shelfware." What data types are being protected, how are they classified, how are alerts/alarms defined, who resolves them and how, when will you kick off the project, when will you cut over, what are the escalation steps (on both sides) if issues arise that are not being properly addressed. A security risk assessment is a key item in the Plan phase, especially when deploying security solutions!

Build – Put your plan into action! Work with the architects to get the design right and put the new solution into play, often times alongside the old. (as much as possible; there are occasions where technology conflicts will arise, precluding a side-by-side approach). Do as much testing as you can in a sandbox, then roll out in smaller, but increasing numbers to validate as you go.

Run – It's go time! The operational phase requires you and the team (and the vendor!) to be ready to take over responsibility as you outlined it. Even in a managed security program, the organization needs to commit resources to own, operate, and handle the internal side of the project. Tracking improvement in the business outcomes that you tied the project to is key to show ROI. If you are struggling to get the ROI you expected, work with the vendor to determine where things went astray. Were your assumption up front off base? Did something change internally (or externally – Hello, COVID, I'm looking at you) that altered the environment?

Migration Planning

Need more detail about the discrete items within each of the 6 subphases? Here’s a list to get you started, each business and project will have some elements that are unique, and your priorities might be shuffled around but this is a starting point to have the discussion with your team and the vendor’s team. Ultimately the communication at every phase of the project is what drives success (and lack of communications often contributes to a bumpy or failed roll out).



STRATEGY

- Assessment & Profiling
- Prioritization
- Data Requirements & Classification
- Business Logic & Infra Dependencies

ANALYSIS

- Detailed Migration Plan
- Estimate Effort
- Security & Risk Assessment

DESIGN

- Network Topology
- Migrate
- Deploy
- Validate

TRANSITION

- Pilot Testing
- Transition to Support
- Release Management
- Cutover & Decommission

OPERATIONS

- Staff Training
- Monitoring
- Incident Management
- Provisioning

IMPROVEMENT

- Monitoring-driven Optimization
- Continuous Integration & Continuous Deployment

TIPS from the Experts

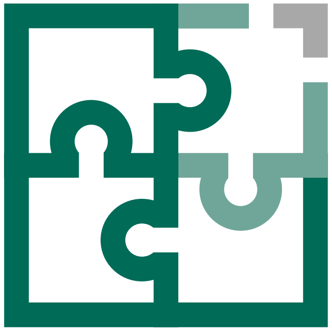
Approach security from an enterprise perspective—building architectures that allow improved visibility into network activities avoids potential blind spots that hackers can infiltrate and ensures data protection in a world where traditional security borders no longer exist.

PART FIVE

How To Avoid Migration Pitfalls

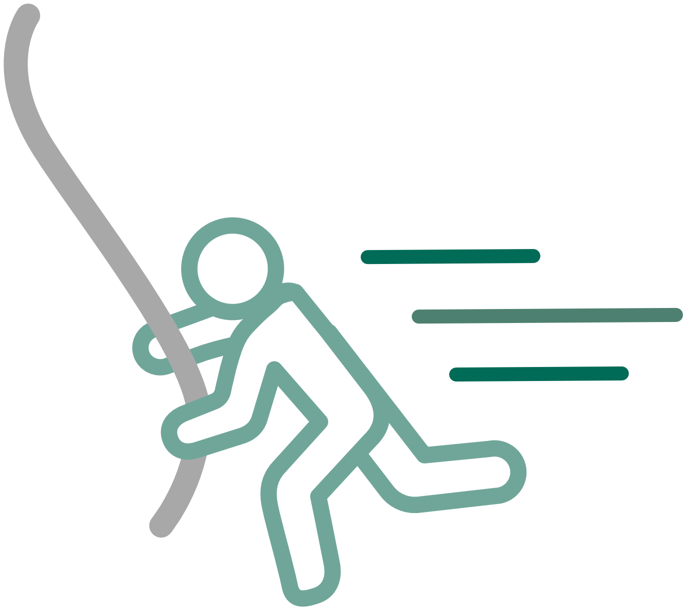
Don't Let All Your Hard Work Go For Naught

Enterprise technology migration projects can often be months of upfront effort, proposal writing & evaluation, decision-making, and implementation. Here's some guidance from experts on where things can go wrong and how to address them before you find yourself in a "what went wrong" meeting with the executive team.



Common Migration Pitfalls

- **Not preparing a long-term migration roadmap with accountable deliverables**
  - Put names down next to roles, dates and deliverables. When everyone owns something, no one does.
- **No contingency plan for migration team members quitting the organization**
  - Staffing changes are inevitable; have a succession plan prepared—at least mentally—in case people do leave during the project. Be ready to pick things up to keep on track during any transition to a new person.
- **Not keeping thorough documentation throughout the process**
  - Keep good records of configurations, settings, etc throughout the process so you can refer to them when needed. Electronic notebooks make it even easier to search back and find things.
- **Not testing thoroughly at each phase of the migration**
  - Even if the 1st few phases of the deployment are going well, stick with your pre-defined testing plan. As the roll out expands, scale issues can become apparent. The last thing you'll want is to rely on early success, deviate from the plan to go whole scale deployment and run into company wide problems.
- **Not involving in-house experts (even if migration is being handled by vendor)**
  - You likely hired people on your team to have in-house expertise for certain things, so don't hesitate to rely on that knowledge. Your vendor may try their best, but no one knows your company like you and your employees do.



PART SIX

Why Fortra's Digital Guardian?

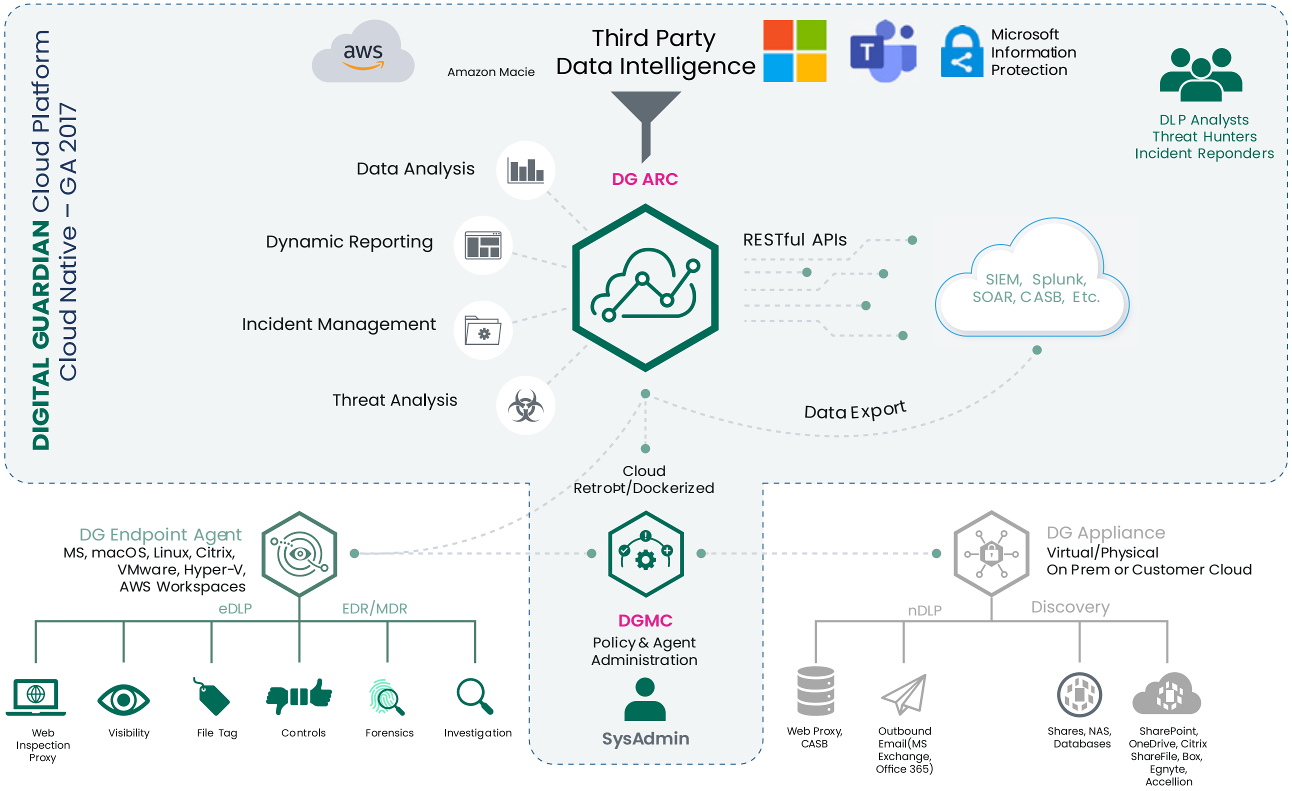
The Only Cloud Delivered Data Protection Platform

FREE DOWNLOAD

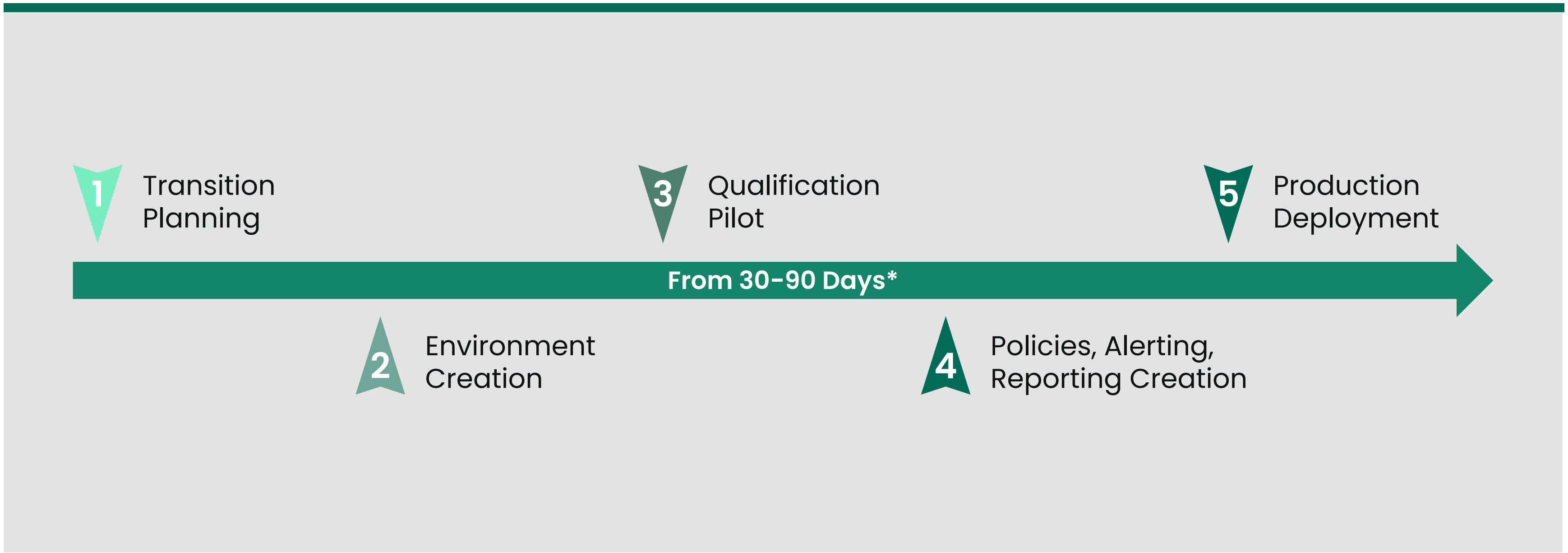
Digital Guardian Platform Technical Overview

Data protection is at the core of our company mission. The DG Data Protection Platform detects threats and stops data exfiltration from both well-meaning and malicious insiders as well as external adversaries.

- Data Loss Prevention
- Managed Detection & Response
- Data Discovery
- Data Classification
- Analytics
- Reporting
- System Management



Proven 5-Step Methodology: Speeds Migration and Eliminates Data Protection Gaps



Fortra's Digital Guardian team is with you throughout the entire process. From the initial planning stages, through build-out & testing, and ultimately production deployment, we'll combine our team's data protection experience with your business knowledge to get you operational quickly.

No-Compromise Data Protection That Stops Data Loss

CLOUD-DELIVERED

Powered by AWS, Digital Guardian delivers simplified deployment, low overhead, and elastic scalability for increased return on your security spend.

CROSS PLATFORM

Coverage for your Windows, macOS, or Linux operating systems and all your applications, both browser based and native.

FLEXIBLE CONTROLS

Fine-grained controls, ranging from log & monitor to automated blocking, help protect data before it's lost.

DEEPEST VISIBILITY

We see everything that happens to your organization's sensitive data.

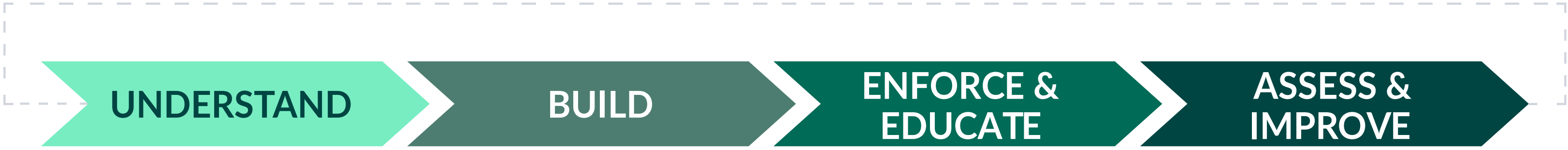
NO POLICY, NO PROBLEM

Our "unknown risk" approach enables you to see where sensitive data is located, how it flows, and where it is put at risk - all without policies.

COMPREHENSIVE CLASSIFICATION

Only Digital Guardian provides content, user, and context-based data discovery and classification.

Proven Data Protection Framework



UNDERSTAND

BUILD

ENFORCE & EDUCATE

ASSESS & IMPROVE

Understand

- What data you need to protect
- When sensitive data is at risk

Build

- Smart policies & controls
- Based on REAL data usage
- Enterprise wide knowledge how business operates

Enforce

- Flexible & Automated controls

Educate

- Real-time prompts increase employee awareness and educate users on proper usage

Assess

- Advanced analytics & reporting

Improve

- Determine next level data protection

Our four part data protection program framework has proven successful for hundreds and hundreds of our customers.

- **UNDERSTAND.** It's essential to understand what data you need to protect and when that data is at risk. We help you do this with a combination of enterprise data discovery, data classification, data loss prevention, and endpoint detection & response.
- **BUILD.** With the understanding of how data is used, where it flows, and where it's at risk you can build smart polices and controls based on real data usage patterns.
- **ENFORCE AND EDUCATE.** Our solution enables you to educate users in real-time, making them aware of when they might be violating polices. This can be a game changer. We also help you apply enforcement controls that can stop bad actors before the data gets out.
- **ASSESS & IMPROVE.** You can't improve what you don't measure. We give you the mechanisms to continuously assess, iterate, and improve your security policies and procedures.

Use Data Visibility Insights to Engage Business Leaders

Anyone with DLP experience will tell you that DLP isn't just a security or IT initiative. Success depends on support and sponsorship from the business leaders. This is pure common sense. But we have a unique view on how to engage them.

The standard process is to sit down with the business leaders to define all data classification schemes and protection policies in advance. What do we recommend instead?

Start by sharing real discoveries from your "Quick Win" about where sensitive data resides and how it's being used. This will get the attention of your enterprise's business leaders. It will make it much easier for them to understand the risks to the business. And it will make it much easier to collaborate with them. That's exactly what John Graham, former CISO of Jabil did.

> *"Digital Guardian [Data Loss Prevention] helped us changed the conversation with business unit leaders."*
>
> *–John Graham, former Chief Information Security Officer, Jabil*

JABIL

CASE STUDY

Jabil's Quick Win

JABIL

SITUATION: Jabil is a Fortune 100 contract manufacturer. The company was at risk of large financial penalties if customer NDAs were violated due to a security incident.

SOLUTION: Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations. They immediately realized that users copying large data files to USB drives was far more common than anyone expected. Digital Guardian's detailed egress reporting on the data leakage from USBs enabled Jabil's security team to have more productive conversations with business unit leaders. These exchanges focused not on defining what data was considered sensitive, but rather on how data from specific servers was being used (in this case copied to USBs) by users.

RESULTS: By providing business leaders real-world information on how data was being used (or misused), Jabil was able to identify and classify their most sensitive data faster and more efficiently. This was a dramatic improvement over a more traditional discovery and classification approach.

Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations

MORE INFO

Read the full case study here.

CASE STUDY

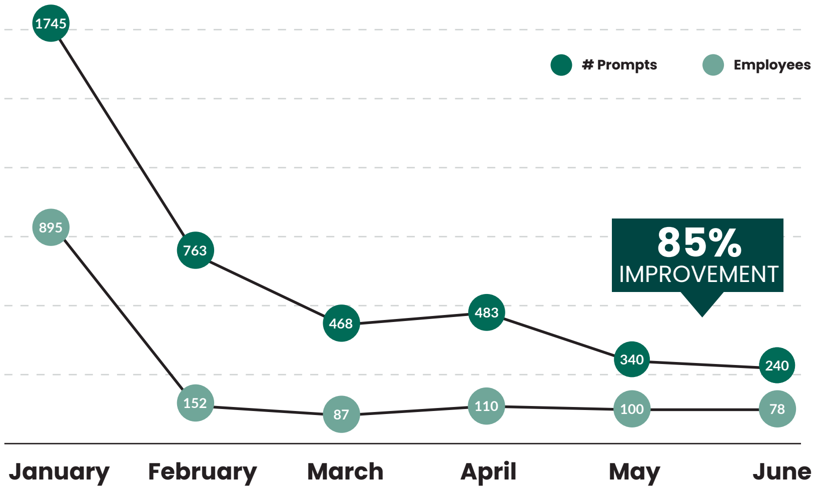
The Power of Real-Time User Education

SITUATION: The company is one of the largest managed healthcare providers in North America. Despite spending more than $1M annually on HIPAA compliance training, an internal audit identified a significant risk of non-compliance. The training had failed because it was a specific event not reinforced through ongoing processes. Users were not diligent about using the company's VPN, where data protection controls were enforced. Remote users routinely traveled with the sensitive data they needed to do their jobs.

SOLUTION: The company's auditors recommended stricter controls, both on and off the corporate network. The company needed to change user behavior when interacting with sensitive data, reinforce existing policies as data was used, and create a culture that held users accountable for their actions. Digital Guardian helped by enforcing connections through the company's VPN, applying policies in real time based on network awareness, and prompting users who violated data use policies. Users are presented with a prompt screen that requires them to acknowledge the appropriate company policy and provide justification to continue.

RESULTS: Within six months, the healthcare provider reported an 85% decrease in prompts to users, indicating a significant increase in both policy awareness and secure employee behavior.

UNAUTHORIZED TRANSMISSION OF PHI DATA



WATCH A VIDEO

Watch a video on driving security using real-time user education.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.