How to Migrate Your SIEM to Devo

EBOOK

DEVO

Introduction

Today, many companies want to modernize their SOC by moving their SIEM to the cloud. That means the vast majority of our customers are replacing a legacy solution — often an on-premises one — with Devo. The primary driving forces behind these migrations are usually cost and scalability. Legacy solutions often are prohibitively expensive to maintain effectively and/or cannot scale to the levels of data ingestion modern businesses require. Therefore, the majority of our engagements are "Devo migrations" rather than "Devo installations."

The Devo technical services team has helped hundreds of customers migrate successfully from legacy solutions. Usually, new Devo customers are migrating from Splunk, Elastic, QRadar or ArcSight. Regardless of the incumbent solution, we have found that all SIEM migrations can be categorized into one of two major types: ***carbon copy*** and ***value-based***. Each type has two different execution options: ***parallel*** and ***cutover***.

This document explains each migration type and execution method and identifies the risks, benefits and associated timelines so you can make an educated decision on the best method for your organization.

Migration Types

Let's start by taking a close look at **carbon copy** migration. This is when the customer attempts to migrate every piece of content from their legacy product into their new SIEM. This means every single alert, query, dashboard, and use case must be documented in detail so it can be replicated within the new platform. Customers who prefer the carbon copy approach are generally happy with the performance of their current SIEM but are looking to minimize costs. The typical goal of this approach is to reduce the amount of retraining necessary for IT or security teams since they will be operating the same use cases and visualizations post-migration.

Unfortunately, organizations that choose the carbon copy approach are unlikely to maximize the value of Devo simply by replicating existing content. The goal of a migration should be to leverage the benefits of Devo to improve the organization's overall protection profile. From an implementation timeline perspective, this is the most time-consuming and expensive migration type as it requires the reimplementation of all content either by the internal team or the Devo services team.

Carbon Copy Migration Pros:

- Lowest business risk since the overall protection profile is unchanged
- Reduces training burden since the use cases are identical to the legacy product

Carbon Copy Migration Cons:

- Most expensive and time-consuming method
- Only provides the same overall business value as the legacy product
- This approach may be impossible since not all legacy products allow visibility into how their out-of-the-box detections function

The second migration method is known as ***value-based***. This option is often the choice of customers who are primarily interested in the value and use cases a new SIEM can bring to their SOC, rather than just copying existing functionality and use cases from their legacy product. Customers who prefer value-based migrations generally are dissatisfied with the overall performance of their existing SIEM, especially if it has been compromised.

The primary goal of this migration type is to extract the maximum value out of the native capability of the new SIEM by creating a new protection profile for the organization. This approach does slightly increase the risk to the business because the new solution may not have an exact 1-to-1 match with all the legacy SIEM's use cases but offers a higher protection profile and superior value overall.

From an implementation timeline perspective, this approach generally is significantly faster and less expensive than a carbon copy migration because it does not require an extensive services engagement to copy existing content. Value-based migrations generally take about half the time of carbon copy migrations. They are best for customers with a tight timeline for migrating to a new solution

Value-Based Migration Pros:

- Most expensive and time-consuming method
- Only provides the same overall business value as the legacy product

Value-Based Migration Cons:

- Could increase business risk if all use cases are not covered
- Could require more training time for end users

Execution Methods

Once a customer has decided which migration type is best for their business, the next decision is which execution method to use. The least risky execution method is a **parallel migration**. When executing a parallel migration, the customer runs their new SIEM alongside their legacy product for between 30 and 180 days. This provides time for the customer to validate their new SIEM against the legacy solution, minimizing business risk.

Another key benefit of a parallel execution is it can reduce or eliminate the need to migrate historical data for compliance purposes. Historical data migration often is a very time-consuming and expensive process. A parallel migration does require advanced budgetary and staffing planning. The customer needs to decide to move off their legacy SIEM in advance of its license expiration and to budget for the parallel operation of both products for the desired time.

Parallel Execution Pros:

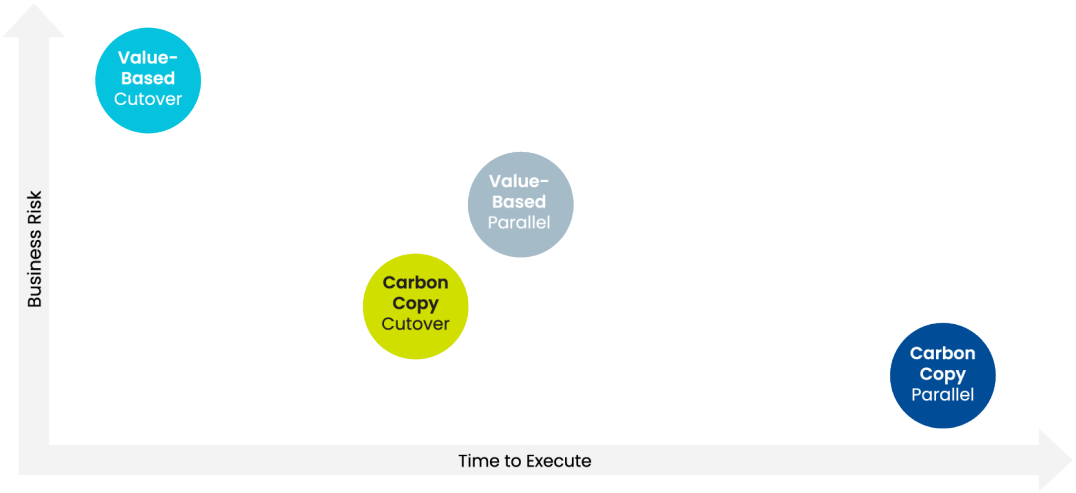
- Lowest business risk
- Reduces or eliminates the need for historical data migration

Parallel Execution Cons:

- Requires advanced planning and budgeting
- Increased cost to run both products in parallel
- Cannot be done for customers with just a short time before their legacy SIEM license expires

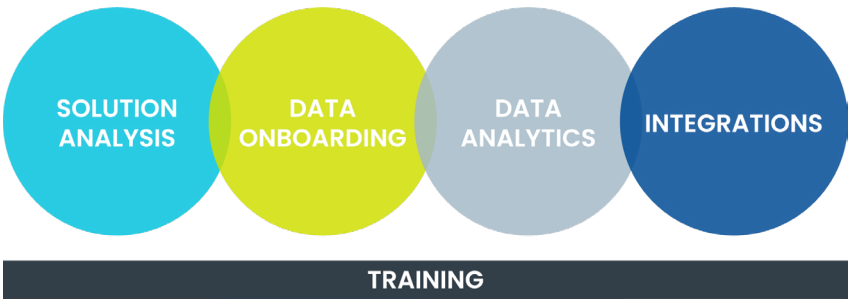
The second method of executing a SIEM migration is the **cutover** method. This involves performing a hard cutover from the legacy product to the new SIEM without parallel operation.

A cutover execution is faster but dramatically increases business risk due to issues that may arise in the data source redirection process. It also does not allow the customer to benchmark their new SIEM against the legacy solution to ensure the new product is performing as expected or to assess the overall protection profile the new SIEM provides. Due to the increased risk of this migration type, Devo strongly discourages this approach unless a parallel migration is not possible for schedule or cost reasons.



The 4-Step Devo Migration Process

Throughout hundreds of SIEM migrations, the Devo technical services team has developed a four-step process to ensure success with whichever migration type and execution method you choose.



STEP 1: The process begins by achieving a complete understanding of what the customer wants to accomplish with their SIEM migration. This includes understanding timelines, budget, migration type, and execution method. The outcome of this step should be a mutually agreed-upon plan for what the success of the migration means to their organization.

In a carbon copy migration, success may be a 1-to-1 mapping of the legacy SIEM to Devo. In a value-based migration, success may be a set of functional use cases or scalability tests to validate the new implementation. Regardless of the criteria, the customer and Devo teams must be aligned on the definition of success and understand each other's roles and responsibilities to ensure success. To achieve a successful migration, a best practice is to identify experts from Devo and the customer to serve as the project manager and technical lead. These individuals will be responsible for coordinating and executing the remaining steps.

STEP 1 - SOLUTION ANALYSIS TASKS

CUSTOMER	DEVO
Provide list of data sources	Develop data ingestion plan
Identify any content to be migrated	Provide specs for on-premises components
Provide queries for alerts to be migrated	Review source list and provide feedback and recommendations
Provide screenshots of dashboards	Create mapping of legacy content to Devo
Provide use case details	Agree upon completion criteria
Identify completion criteria for the project	Deliver project plan

STEP 2: Next comes the work of adding your data sources to Devo. This requires the project team to collaborate and prioritize sources based on business value and anticipated volume and develop a source ingestion strategy for pulling in the data from each source. When executing a parallel migration, the data sources will be ingested into both SIEMs simultaneously. This gives customers time to validate the performance and parsing of the data before cutting off their legacy SIEM.

STEP 2 - DATA INGESTION

CUSTOMER	DEVO
Install on-premises components per data ingestion plan	Provide support for installation of on-premises components
Configure data sources to send to Devo	Validate ingested data against parsers
Provide credentials for cloud-based sources	Develop new parsers as required
Verify data parsing	Activate cloud collectors with provided credentials
	Develop new cloud collectors, as required

Step 3: This is where customers begin to extract significant value out of Devo. It also is the part of the project where the process diverges depending upon whether it is a carbon copy or value-based migration. For customers who select the latter method, this step involves the deployment and activation of Devo's native content including out-of-the-box alerts, dashboards and applications.

For customers who opted for a carbon copy migration, the project team will have to assess and begin translating all content and use cases from the legacy product to Devo. It is generally at this stage where the burden shifts from the customer to the Devo services team to get the content activated or migrated effectively and efficiently.

It is important to note that when translating content from one SIEM to another, an exact translation is not always possible. Different SIEMs use different query languages, syntax, and data models. Therefore, the process of translating content is manual and requires technical resources capable of understanding how each use case is being accomplished and then being able to replicate that same use case in the new product.

STEP 3 – USE CASE IMPLEMENTATION	
CUSTOMER	**DEVO**
Validate that translated content meets requirements	Translate legacy content into Devo

STEP 4: This is where the migration paths reconvene as the joint customer and Devo team wraps up the migration by implementing integrations with any required third-party tools. These can include ticketing systems, identity and access management (IAM), security orchestration and response (SOAR) tools, and more. Not all customers will require this step, but when needed it is often a critical step to ensure their existing workflow and compliance policies remain intact.

STEP 4 – INTEGRATIONS	
CUSTOMER	**DEVO**
Provide information as required for third-party integrations	Enable integrations with third-party products
Perform configurations in third-party systems to facilitate integrations	Provide documentation and support for enabling third-party integrations.
Validate that integrations meet requirements	

One remaining critical item is training. This is one of the primary obstacles cited by organizations considering a SIEM migration due to concerns about a decline in staff productivity while they come up to speed on the new product. In the Devo migration process, training occurs at every step, and we deliver it in three different ways.

Comprehensive Training

Devo customers receive unlimited access to our extensive self-paced online training as part of their license. Upon completion of the online training curriculum, users have the opportunity to become Devo Certified.

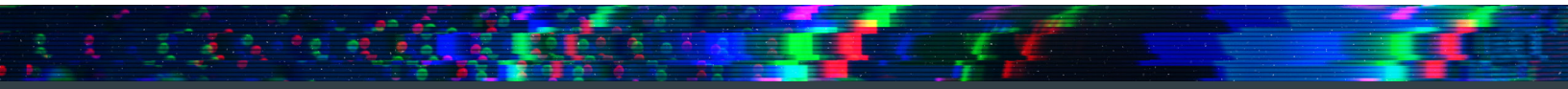
Customers also have the option to purchase custom instructor-led training workshops, which can be tailored to their specific needs and use cases. It typically takes about two weeks for a new user to become comfortable operating the Devo Platform, including the ability to run queries and build custom dashboards and alerts. Training employees to become experts and certified in the Devo Platform costs about 90% less than it would with competitors such as Splunk.

The Bottom Line

At this point, your head is probably swimming with all of the different options, approaches, benefits and challenges of executing a SIEM migration. The main question that every customer wants to ask is "OK, but really how hard is it?" SIEMs are complex software (and occasionally hardware) that are a vital component of an organization's security and network operations. Ripping out and replacing such a critical component is never easy. Any vendor that claims the process will be completely pain-free is not being honest. With that said, the process often is less painful than many expect, and there are things that you can do now to set yourself up for as pain-free an experience as possible.

- **Anticipate in advance:** Do not wait until your SIEM license is about to expire before deciding to move to a new platform. If possible, give yourself a minimum of three months to allow for parallel operation and tuning of your new system.
- **Understand your needs:** You likely have had your legacy SIEM for several years during which time you probably built up a lot of unnecessary content. Don't waste your time or money by paying a vendor's services team to migrate content that is not critical to your business.
- **Accept change:** Understand that your new SIEM is not going to operate exactly the same as your legacy product. You are migrating for a reason. Pick the new SIEM that best matches your workflow, needs, and skill level of your team.
- **Seek to improve:** Performing a 1-to-1 carbon copy migration is going to leave you essentially with the same product you had. Talk with Devo about how you can improve your overall state so when your migration is complete you are in a better place than when you started.
- **Make — and follow — a plan:** A successful SIEM migration requires that both the vendor and customer have a plan and adhere to it. Understand what the resource commitment will be from your side. Identify your project manager and technical lead and involve them in the conversation early.

Want to find out more about Devo? Click **here** to schedule a demo or reach out to your local Devo team to set up a session to discuss which migration plan is best for your organization.



Devo USA
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.