

SEE MORE. CREATE MORE. SAVE MORE.

# Do More with Splunk.

From your friends at

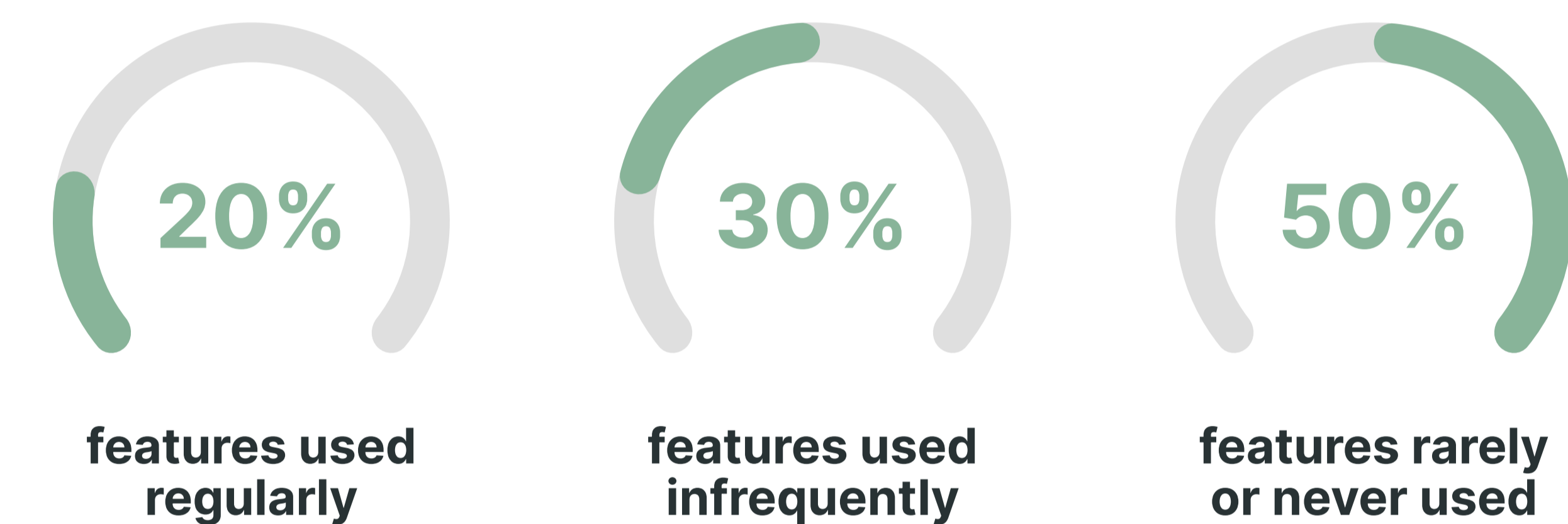


But “offensive” moves?

The companies that fared best in a downturn were those that focused on maximizing what they already had. This approach to improving operational efficiency had the same net effect as reducing headcount or slashing expenses without actually doing those things at the same levels as their competition.

## Doing More

Regardless of economic conditions around us, the reality is we could all use some help in getting more from what we’ve got. The [average utilization of a software platform](#) across all industries looks something like this:



Take a moment to let that sink in. What is your company’s annual investment in the Splunk platform? What could it mean to your organization if you could unlock that 50-80% of the platform that you may not be utilizing to the fullest?

The key to your future success will be found in unlocking the underutilized potential of the most amazing security and observability platform available... and creating incredible outcomes in the process.



# Introduction

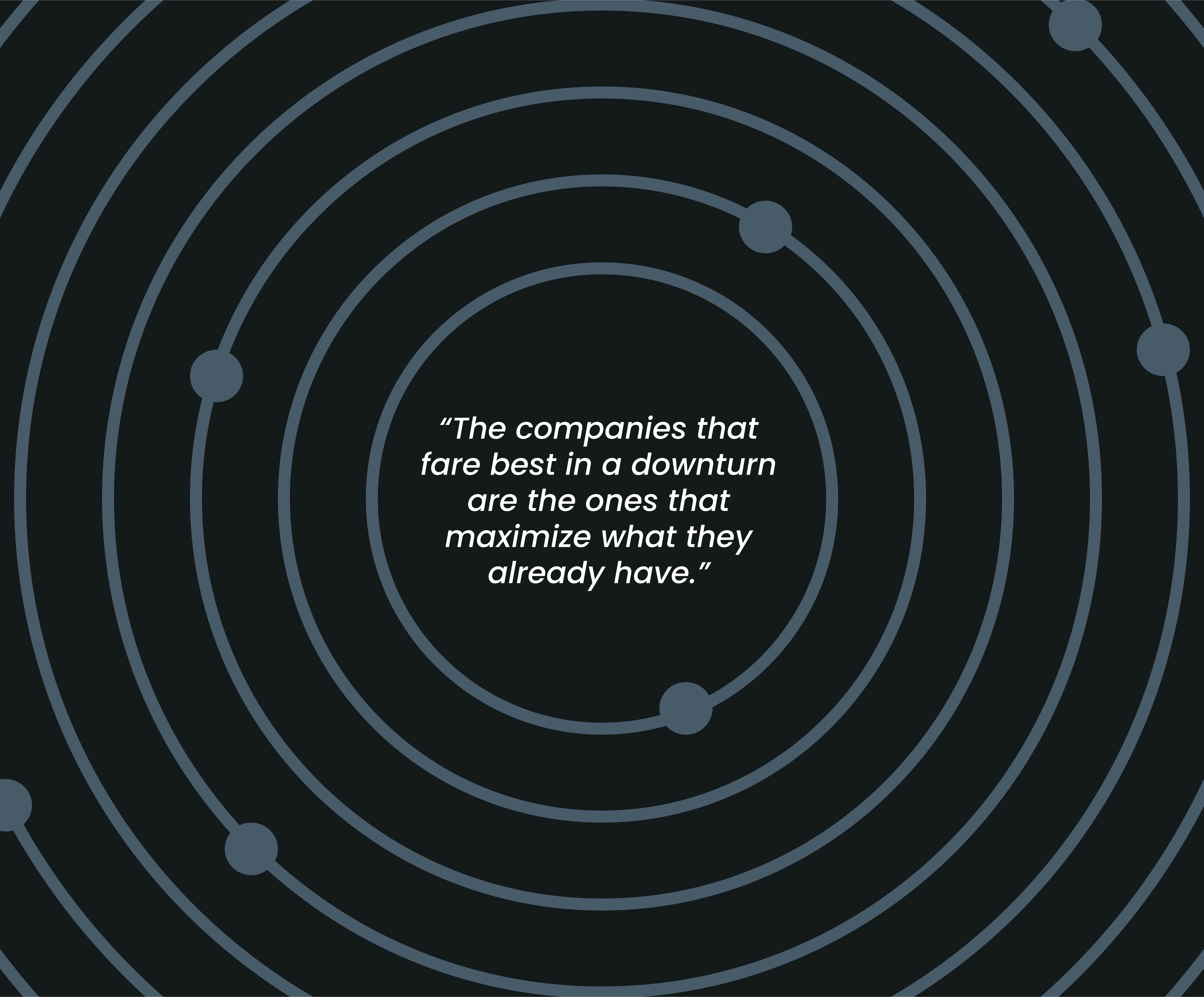
In every recession, organizations find themselves in uncharted waters — after all, no two recessions or downturns are the same. What worked for Company A during the early 2000’s recession may or may not work for Company B facing the economic downturn ahead of us today.

What organizations can do, however, is identify the patterns and behaviors of the companies that managed to thrive in challenging economic times. Harvard Business Review [conducted a year-long study](#) of nearly 5,000 companies and their behaviors in the periods immediately preceding, during, and after an economic downturn.

While 17% of the companies they studied didn’t survive (for a wide variety of reasons), and the overwhelming majority were unable to regain their pre-recession rate of growth, 9% were able to gain ground and outperform competition.

## What Do the Winners Do Differently?

Harvard Business Review’s study effectively found that the key to coming out ahead, during and after a recession, is an adept combination of “defensive” and “offensive” moves. Defensive moves are those that are, perhaps, the most common response to a downturn — spend less and cut costs.



*“The companies that  
fare best in a downturn  
are the ones that  
maximize what they  
already have.”*

## CHAPTER 1

# What is a Splunk Creator?

Before we dive into our three primary topics, we want to set the stage by explaining a term you'll see used throughout this piece:

“Creator.”

Typically when we think of “creators,” we think of, well, creative occupations. Painters, designers, architects, and the like. Or maybe you think in more modern terms, such as YouTubers and TikTok content creators. But most individuals working with Splunk wouldn't consider the work they do with and in the platform to be creative.

Except... it really is.

Think about it for a moment. An architect or product designer gathers a list of requirements and then creates the best possible solution with existing materials, working within the budget and time constraints the client has laid out for them.

Isn't that exactly what you do each and every day in Splunk?

Someone needs an outcome:

*“We want a dashboard to view security incidents.”*

*“I need a visualization for revenue vs targets.”*

*“We need a way to collect Remote Work Insights.”*

And what do you do? What every creator does. You look at the available materials — the data you're pulling in to your environment — and then you begin to use the platform to create a solution. An outcome.

*A masterpiece.*

A dashboard in Splunk is more than graphs and charts and tables. It's the output of one of the most complex functions asked of any technical professional — telling a story with data.

*“Is our organization safe from threats today?”*

*“Are we delivering on our promise to our customers and stakeholders?”*

You tell those stories — and many others like them — every day with the solutions and outcomes you create in Splunk.

*Look at you go.*



with the platform, there are two critical questions you must address:



### **Question 1: Do you have an alerting system in place when critical data streams fail in your Splunk environment?**

Setting alerts for critical data streams is important for ensuring your dashboards and processes are up to best practices. You want to be the first person to know an issue has occurred so it can be solved before it becomes a larger problem.

Some may read that and think, “We check our data streams monthly or weekly, so we have a pretty good idea of how healthy our data pipeline is.” But what about those moments when a data stream or forwarder goes offline in between those manual checks?

*Maybe it’s not important data... but maybe it is.*

If you’re using Splunk for compliance, even a few moments of downtime can cause huge problems down the road. If you’re using Splunk for security, you know all too well how much meaningful (and dangerous) activity can occur within even a few minutes.

Alerts are best practice for a reason. Your team and those throughout the organization who rely on Splunk dashboards and visualizations for day-to-day operations, security, insights, and decision-making have to be able to trust the data. If your alerting isn’t strong, that means you could be missing data. And bad data is worse than no data at all.



### **Question 2: If you’re using Splunk Enterprise Security (ES), are you confident you’re ingesting all the appropriate data to get the most from your investment?**

Splunk ES is an incredible tool, but depends on being fed the proper data for it to really shine. Without the ability to ensure you have full coverage for your priority data and clear eyes on that data’s acceleration, you could be leaving yourself vulnerable. The continuous security monitoring, advanced threat detection, and your ability to rapidly investigate and

## CHAPTER 2

# See More: Data Awareness in Splunk

Every beautiful dashboard and impressive visual Splunk is capable of producing is, ultimately, driven by two things: data and search.

And while search is the primary driver behind the analytics and visualizations in Splunk, all the perfectly written and executed searches in the world can’t help you if you’re missing the most important resource of all — quality data.

If you’ve ever put together a Lego® set, you know you’ve got to have all the pieces if you’re going to be able to build the Lego Death Star. Even one missing piece could leave you frustrated and incapable of building what you set out to create.

In short: you have to know what data you’re working with, and that you have all of it.

### **Data Awareness Defined**

“Data awareness” refers to your organization’s ability to look at the infrastructure bringing data into your Splunk environment, the visibility you have (or don’t have) when there’s a failure in your data pipeline, and the health of your forwarder infrastructure.

To get the most from Splunk, and to empower you to do more

respond to threats is all contingent on priority data being fed into the system.

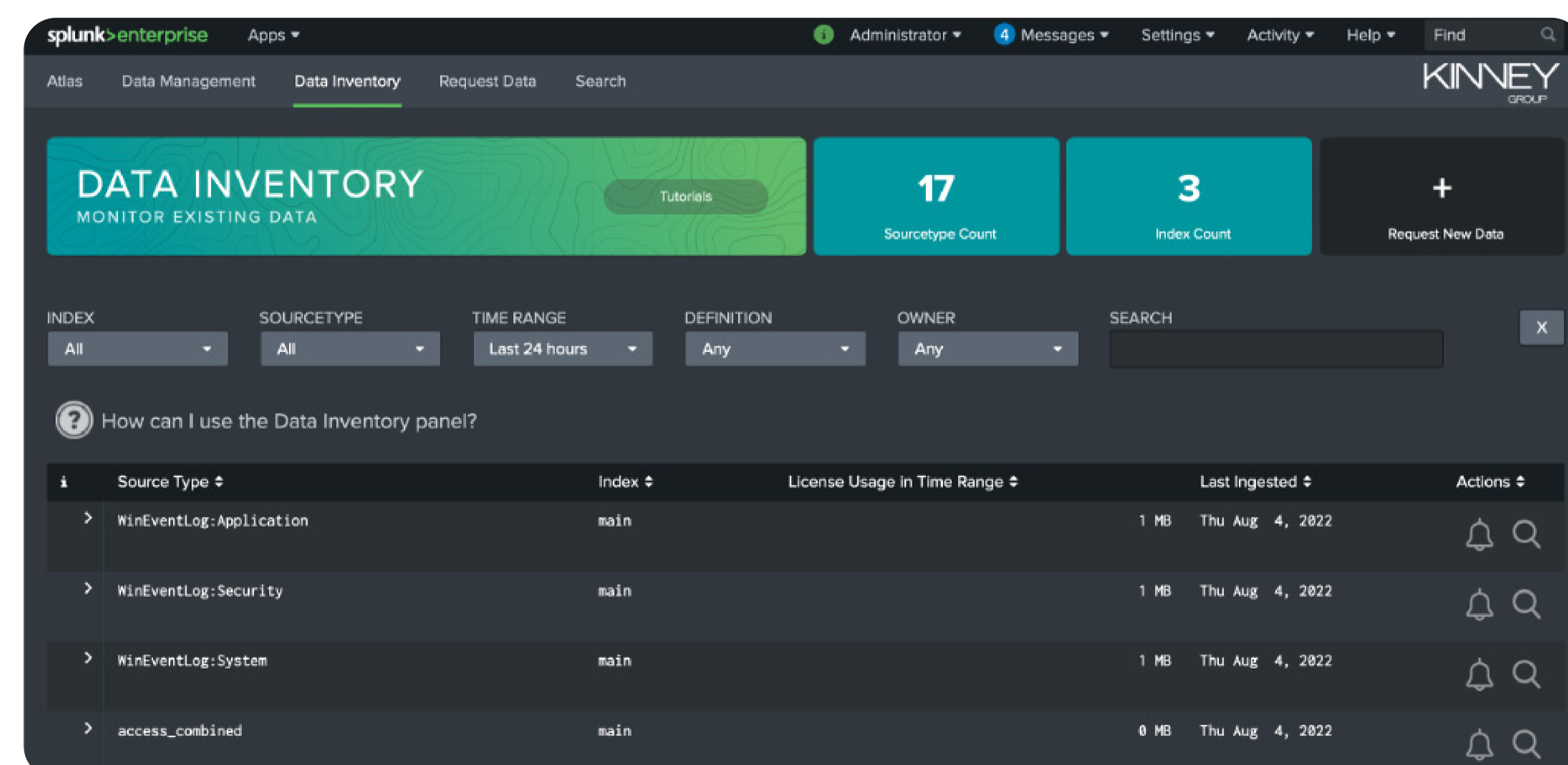
At a minimum, without that information, you're certainly not maximizing your use of ES (or the dollars you've invested in the platform).

## Solving Alerts

It's possible that you can manually create alerts for any number of situations and needs within Splunk. Once again, that's the power of having such a versatile platform at your fingertips. The downside to that approach, however, is that it's time consuming and requires, many times, a degree of technical proficiency with Splunk that many internal teams lack.

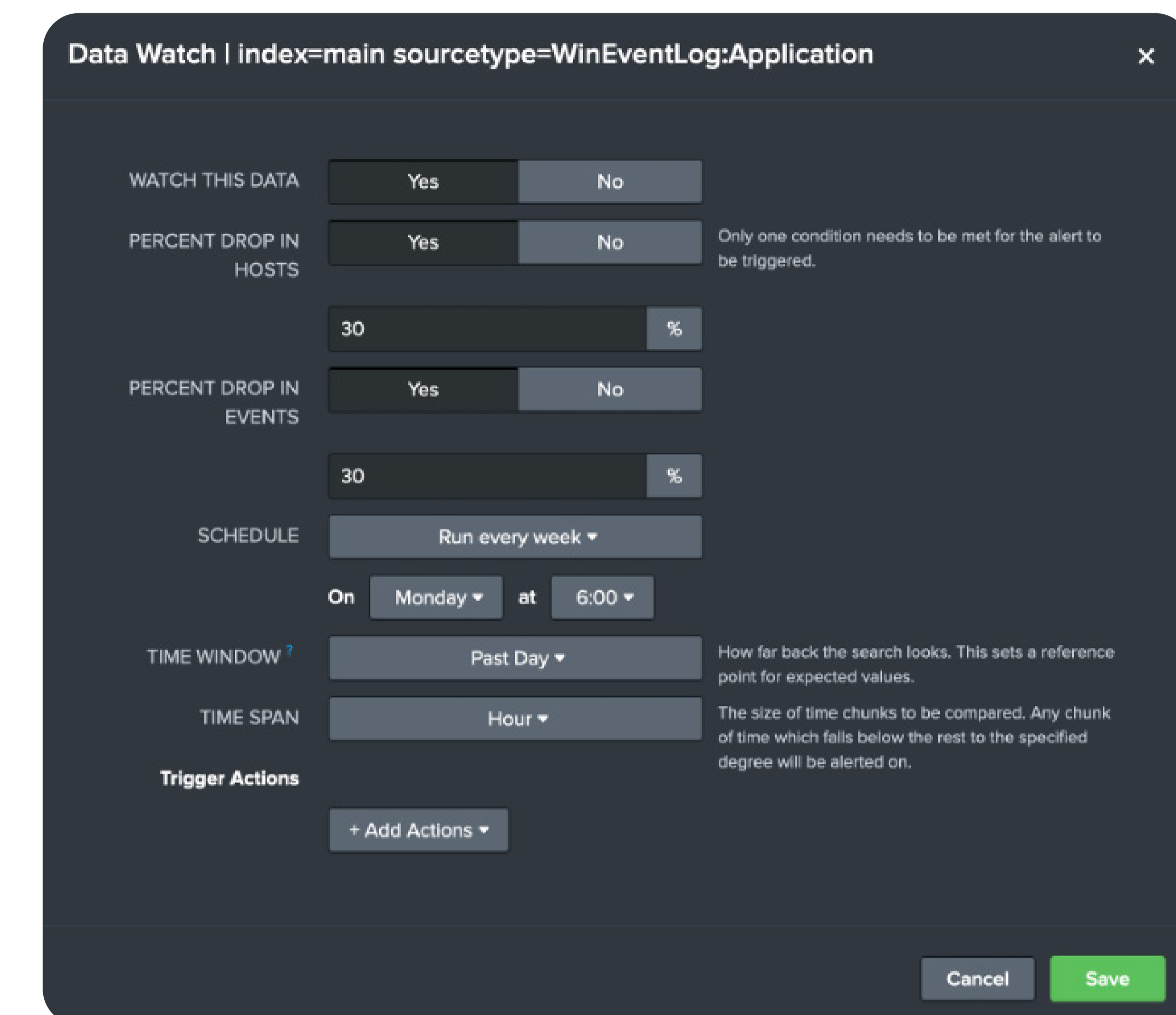
What would be ideal is a single pane of glass that shows a complete inventory of every sourcetype in your Splunk deployment. Even better would be if that inventory could also show how much data is being received by that sourcetype, its status, a use case or description, admin notes, who owns it... you get the idea. And the cherry on top of this magical solution would be a push-button simple way to create an alert for that sourcetype.

This is exactly what the Data Management application within the Atlas Platform provides.

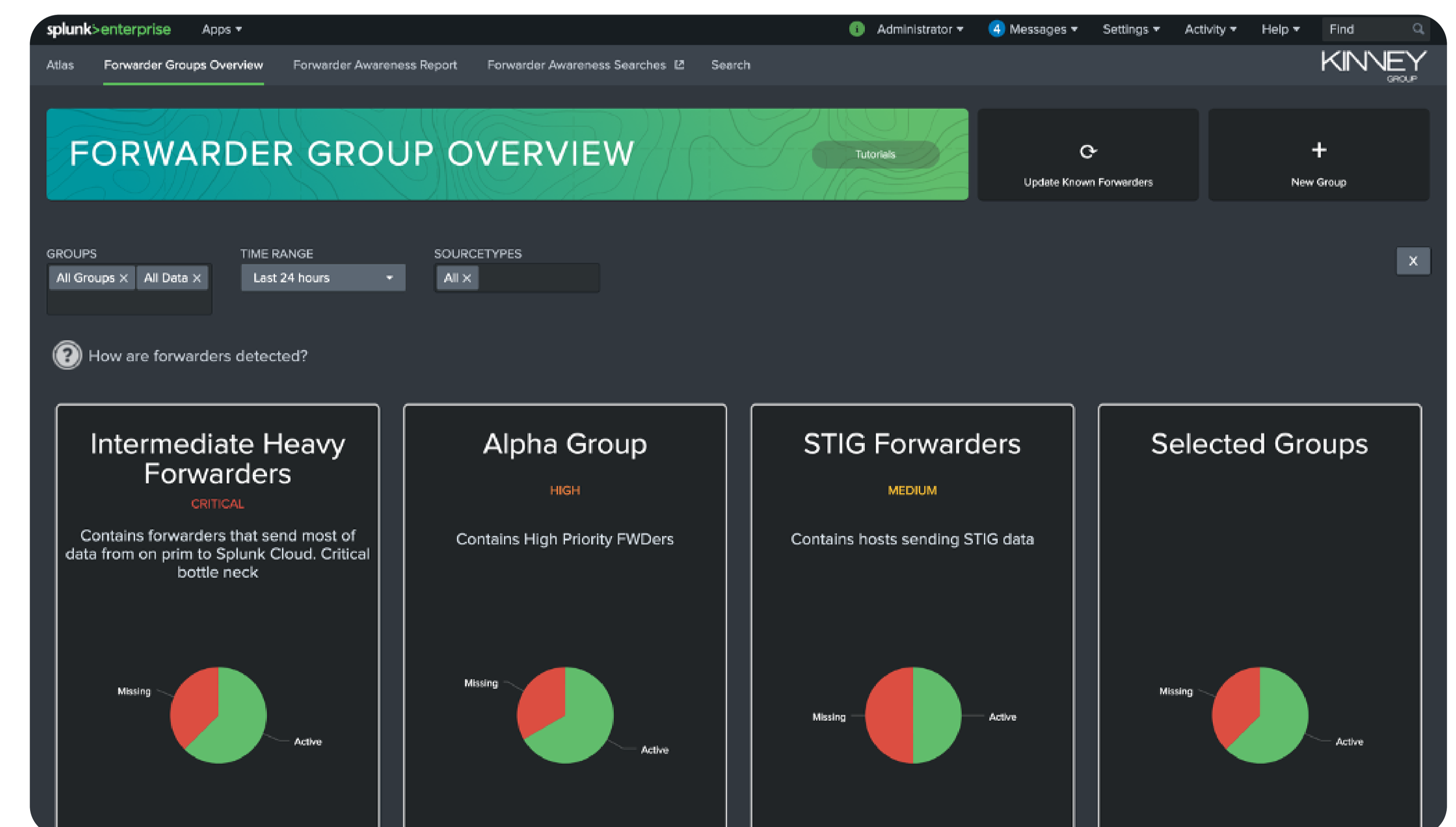


The Data Inventory component of Data Management allows you to easily see every sourcetype, the last time it was ingested, how much of your license that data is utilizing, and a host of other important information.

Utilizing the Data Watch feature by clicking on the alert icon inline with this information, you can also utilize Splunk to keep a watchful eye on the sourcetype and alert you when there's a certain percentage drop in hosts or events:



Of course, watching sourcetypes is only a piece of the puzzle. You also need a way to provide that same level of protection and visibility to your forwarders. This is where the Atlas Forwarder Awareness application swoops in to save the day with a system-wide overview of forwarder status that you can group however you wish, with the ability to dive into each group for details.



Within each group, you'll have visibility into missing forwarders, the SSL status of each forwarder, the version

of Splunk each forwarder is running, and a variety of other information that allows you peace of mind that data is reliable and being brought in to your environment properly.

Lower Data Coverage, and Lower Data Acceleration. The takeaway is an easy to understand and actionable report that tells you, with certainty, if you're getting the most and doing the most with your investment in Splunk Enterprise Security.

## Wrapping Up

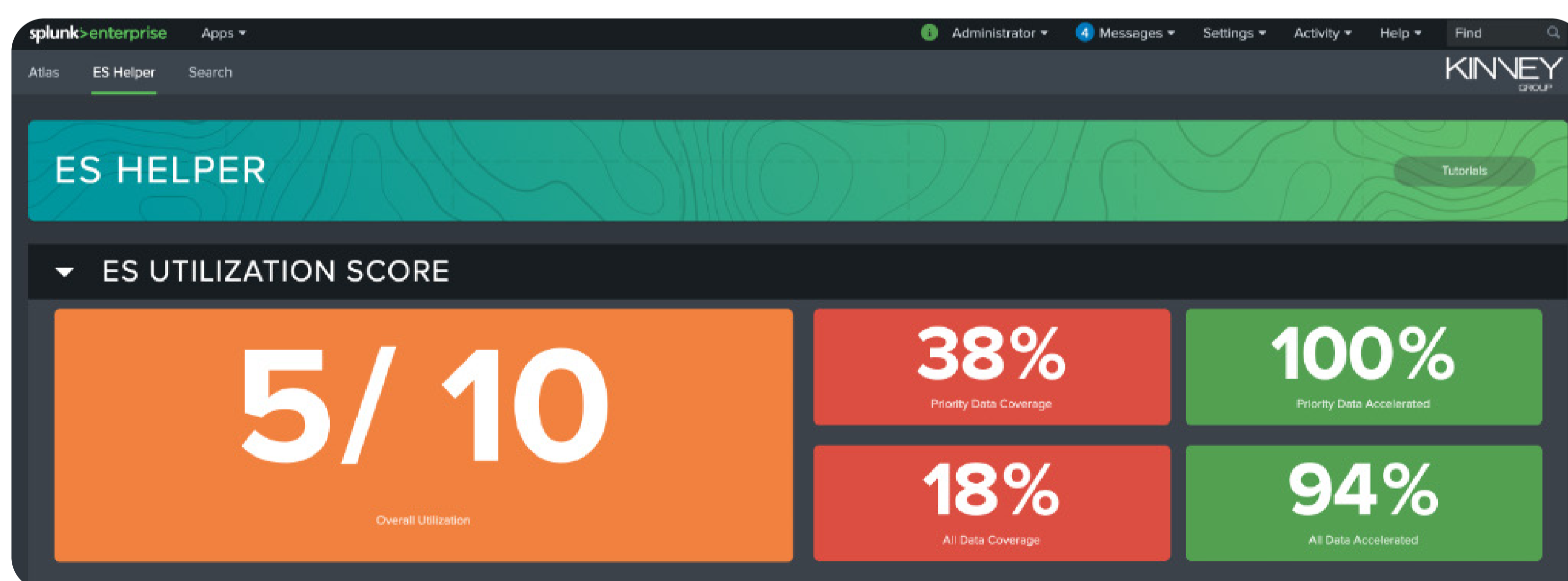
Whether it's a comprehensive understanding of your sourcetypes, data models, and forwarders or getting more from Splunk ES, the value of Data Awareness can't be overstated. Downloading the free Atlas Assessment application from Splunkbase is the perfect way to see if Atlas is the right fit to solve these challenges in your environment. Still not convinced? A free 30-day trial of Atlas will provide you with the opportunity to see for yourself.

| Hostname                            | GUID                                 | Forwarder Type      | IP           | SSL Enabled | Splunk Version | OS      | Last Connected | Architecture | Receiver Count | Connection Count | Average KB/s | Average Events/s | Uptime |
|-------------------------------------|--------------------------------------|---------------------|--------------|-------------|----------------|---------|----------------|--------------|----------------|------------------|--------------|------------------|--------|
| atlas-universal-forwarder-group-1-0 | D1781874-1203-4312-8093-8E420F084F32 | Universal Forwarder | 10.42.1.168  | false       | 8.1.3          | Linux   | 17:38:18 PM    | x86_64       | 1              | 57               | 87.29        | 256.83           | 68.1   |
| atlas-universal-forwarder-group-9-0 | 94051888-8D48-48FF-93DA-5D7530F93A3C | Universal Forwarder | 10.42.4.58   | false       | 8.1.3          | Linux   | 17:21:11 PM    | x86_64       | 1              | 57               | 85.39        | 249.66           | 67.2   |
| atlas-compliance-prod-pe-server     | 988780E7-9F37-4148-9788-65BA6A13DC1E | Universal Forwarder | 10.42.4.0    | false       | 8.2.4          | Linux   | 17:38:18 PM    | x86_64       | 1              | 2888             | 1.27         | 8.69             | 100.1  |
| WIN-0080BJP233                      | CC22E41E-85F1-4520-ACD5-F86CE1F5C3F6 | Universal Forwarder | 172.16.11.39 | false       | 8.2.5          | Windows | 17:38:18 PM    | x64          | 1              | 2893             | 0.64         | 8.42             | 100.1  |
| puppet                              | 17701386-1978-4729-AF94-22F9500759C9 | Universal Forwarder | 10.42.4.0    | false       | 8.2.0          | Linux   | 17:38:18 PM    | x86_64       | 1              | 1955             | 0.52         | 8.57             | 100.1  |
| WIN-380XLU713F                      | C14F4C68-8071-4189-8D96-333C2DA37864 | Universal Forwarder | 10.42.4.0    | false       | 8.2.5          | Windows | 17:38:18 PM    | x64          | 1              | 2885             | 0.11         | 8.12             | 100.1  |

## Solving Enterprise Security

As stated, Enterprise Security depends on the right data — and especially priority data with clear eyes on acceleration of that data.

That's why we've developed the Atlas ES Helper application to guide the process and ensure you have the coverage you need and you're utilizing the platform effectively.



In addition to a comprehensive inventory of ES-related data models, the power of ES Helper is its ability to give you an understanding of your environment's overall utilization, data coverage, and acceleration at a glance.

The proprietary ES Utilization score is based on scoring your system's Priority Data Coverage, Priority Data Acceleration,

## CHAPTER 3

# Create More: Bridging the Splunk Usability Gap

Splunk provides some of the best tooling and capabilities available to really control, analyze, and take advantage of big data. But you don't build such a powerful and expansive platform over a decade without it being a bit technical, and even difficult, to fully utilize.

This technical hurdle — what we lovingly call the “Usability Gap” — can stop Splunk adoption in its tracks or stall an existing deployment to its ruin. By clearing the Usability Gap, however, a Splunk environment can prosper and deliver a fantastic return on your investment.

So it begs a question — “what is the Usability Gap, and how do I get across?”

### How to Recognize (and Overcome) the Gap

What exactly makes up the steep cliff sides of the “Usability Gap?” Well, these symptoms can manifest themselves in any Splunk deployment or client ecosystem, and is caused just as much by human elements as technical blockers.

The key to any good Splunk deployment is a properly focused

admin. Many admins or admin teams were handed Splunk as an additional responsibility instead of a planned and scoped aspect of their job. This disconnect can lead to under-certified admins who lack the time and experience needed to quickly solve issues and incoming requests from Splunk users.

Splunk users can also be underequipped and undertrained. While formal training is available for users with Splunk Fundamentals certification and other online training, they may not meet the user where they are, and those solutions lack the benefits of in-person training with real, actionable data. These issues can be big blockers for learning Splunk and increase the time it takes for users to become confident with the system.

If you're still not sure if you have a Usability Gap issue, check the activity found on the system itself. If your Splunk search heads are getting little action from users and admins, you know for a fact that something is coming between your users and their Splunk goals.

### What a Gap Means for You

What are the consequences of a Usability Gap?

*Wide-ranging with significant impacts.*

With a lack of focus and experience, admins are going to be severely hampered in achieving outcomes with Splunk. When technical issues arise with the complex Splunk ecosystem, or a unique data set requires attention, admins will have to carve out time to not only work on the issue at hand but learn Splunk on-the-fly as well. Without the proper support, progress slows and a lack of Splunk best practices is to be expected in these deployments.

Users without a watchful or knowledgeable eye will be left to their own devices. This can lead to poorly created searches and dashboards, bad RBAC implementation (if implemented at all), or worse — no movement at all. Without a guiding hand and training, the technical nature of Splunk will eventually cause users to misconfigure or slow down the platform, or just not adopt such an imposing tool. These issues together can lead to a peculiar event, where Splunk is labeled as an “IT tool for IT people.” This is far from the truth, but if users are not properly trained, and admins don't have



time to be proactive, only the technical savvy or previously experienced will be able to utilize the investment.

While some outcomes will be achieved, many organizations will realize their significant investment isn't aligned with their outcomes and will drop Splunk altogether, putting all the effort and time invested to waste.

## Mind the (Usability) Gap

Fortunately, there's an easy answer for solving these problems and bridging the Usability Gap in your environment — the Atlas™ Platform for Splunk. Atlas is geared towards increasing and speeding up Splunk adoption and enabling Splunk admins to do more with their investment. Let's look at the elements of Atlas that help bridge the Usability Gap!

The Atlas Application Suite, which is a collection of applications and elements that reside on the search head, helps admins improve their deployment, and zero in on giving users a head start with achieving outcomes in Splunk. One such application is the Atlas Search Library.



Search Library gives users an expandable list of Splunk searches that are properly described and tagged for discoverability and learning. Using the Search Library, a Splunk User can create a library of knowledge and outcomes when it comes to the complex nature of Splunk's Search Processing Language. This greatly accelerates skill sharing and education around SPL — one of Splunk's biggest roadblocks.

Another element is the Atlas Request Manager. This

application greatly increases the usability of Splunk by quickly linking admins and user with a request system built into the fabric of Splunk itself. Admins no longer need to spend time integrating other solutions, and users receive a robust system for asking for help with creating dashboards, Splunk searches, onboarding data, and more — all within Splunk!

Last, but certainly not least in bridging the Usability Gap, is Atlas Expertise on Demand. Expertise on Demand (EOD) is a lifeline to Kinney Group's bench of trusted, Splunk-certified professionals when you need them most. EOD provides help and guidance for achieving outcomes in Splunk, and can lead the charge in educating your admins and users about all things Splunk. With EOD, your admins and users have all the help they need to maximize their Splunk investment.

## Wrapping up

The Usability Gap is too big a problem to ignore. Frustrated users, overtaxed Splunk admins, and a clear lack of outcomes await any Splunk team that ignores the clear symptoms and issues presented by the Usability Gap. Hope is not lost, however! The Atlas platform is purpose-built to help you get over the hurdles of adopting and expanding Splunk. With incredible tooling to simplify searches, SPL gaps, and managing requests, not to mention Expertise on Demand, Atlas provides admins with the support they need and Splunk users with the attention they deserve for education and meeting their Splunk goals.



*Splunk is **not** just an  
"IT tool for IT people."*

*Create more value in Splunk by  
making it more accessible and  
easier to use by "non-Splunkers."*

## CHAPTER 4

# Save More: Reducing Costs with Splunk

In preparation for a potential economic downturn, organizations tend to look internally to determine where costs can be reduced, what platforms are enablers for weathering an economic storm, and what should be cut.

The same is true for organizations that use Splunk to manage data. Since 2013, our team has helped hundreds of commercial and public sector organizations with their implementation of Splunk, both on-prem and in the cloud. From many customers, we hear a recurring refrain of “Splunk is expensive.”

Our first reaction to this comment tends to be:

*“Splunk is expensive? Relative to what?”*

Before Splunk, getting real-time analytics from disparate critical systems to address security, operations, and observability was tough. Regardless of macroeconomics, the labor market, or anything else external to an organization, businesses must be vigilant about optimizing security systems. That means optimizing the software, hardware, and, surprisingly, budget.

We understand the “Splunk is expensive” observation our clients have made in the past. If your organization is not

getting enough tangible returns on its Splunk investments, then Splunk is expensive, regardless of how good the technology is in theory.

## Optimize Splunk, and Turn It Into a Cost Reducer

You can look at “reducing costs with Splunk” through two lenses:

1. Reducing the costs associated with deploying, operating, and sustaining investments in Splunk technologies
2. Harnessing Splunk as a cost-reduction engine

Harvard Business Review identified two criteria of “winning” organizations — those who take “defensive” measures such as cost cutting without going too far, and those who know how to “offensively” improve operational efficiency.

While Splunk licensing costs are the easiest target for reduction efforts, they could ultimately be the most costly for your organization.

Knowing how to proceed requires an “eyes wide open” approach that allows you to view the costs associated with Splunk holistically. Of course, this requires a number of things to be true of your environment:

- You know what data is being utilized within your environment
- You know how much of your license is being utilized by the data you’re ingesting
- You understand the impact of search concurrency on your environment’s resources
- You have certainty that what you do know about your environment is accurate (if you’re under license, but have 20% of your forwarders that aren’t sending data, for example, you’re missing critical decision data)

The problem, of course, is that there is no “easy button” in Splunk for these kinds of operational insights. Getting answers to questions such as these requires an in-depth understanding of the platform and architecture (and an undergraduate degree in economics).

## An Easier Way to Create Cost Savings

In 2021, we released Atlas — the Creator Empowerment Platform for Splunk. Purpose-built from the ground up to help customers in their Splunk journey, Atlas empowers Splunk creators to reduce the costs associated with Splunk with clear eyes.

Addressing lens #1 referenced above, we suggest pursuing a “1-2 punch” using the Atlas platform.



**First, diagnose the health of a Splunk environment via the Atlas Assessment application, available free on Splunkbase.** Using Atlas Assessment, customers can get visibility into areas of cost reduction and optimization for Splunk technologies, whether on-prem or in the cloud. Remarkably, Atlas Assessment returns actionable insights in less than 30 minutes.



**The second punch is using the Atlas platform to address the identified areas of improvement that have been illuminated by the Atlas Assessment.** Not sure if Atlas can help? We offer a full, 30-day trial of the Atlas platform absolutely free. Our experience is that Atlas Assessment, combined with the Atlas platform, provides tangible optimization and cost-reduction results for any Splunk implementation. And you can get started without spending a single dollar.

More specifically, customers find that Atlas reduces Splunk operating costs in the following manners:

- **License optimization:** Whether the license is based on data ingest or workload, Atlas specifically identifies how any Splunk Enterprise or Splunk Cloud license can be optimized for maximum ROI.
- **Operational optimization:** Atlas streamlines the daily operation and sustainment of Splunk implementations. These capabilities provide direct labor savings, while at the same time freeing valued personnel to spend more time creating analytics value from Splunk.
- **UX and adoption optimization:** Splunk admins and users are the “creators” that drive organizational value from Splunk. Atlas helps drive adoption by making the use of Splunk much easier. More people using Splunk means more value for your organization.

## Splunk as a Powerful Cost Reduction Engine

All systems and applications produce log data. And Splunk is the best platform on the planet for turning log data into insights for security and observability. Since we began using Splunk in 2013, we’ve found that Splunk can help organizations reduce the sprawl of siloed, single-use tools and monitors.

As organizations look to reduce costs, we encourage them to take a hard look at their entire landscape of software tools. If Splunk can deliver the outcome, why does an organization need another tool to deliver the same results?

When we optimize a Splunk environment using Atlas, we magically create additional Splunk capacity with existing license investments. This newfound added capacity can then be leveraged to help any organization reduce their footprint (and costs) associated with the sprawl of single-use tooling.


## Reducing Costs Now for Weathering a Potential Storm

With Atlas and Atlas Assessment, we can deliver tangible cost savings immediately, and do so through the two lenses referenced above. Now is the time to prepare for the potential of an economic storm brought on by a recession. Atlas can help get you prepared.

Is Splunk expensive? Yes — it sure can be if it isn’t optimized and delivering tangible returns for the organization.

Is Splunk expensive when fully optimized with Atlas? NO! When running correctly, Splunk is the most powerful platform of its kind in the industry. Splunk customers have chosen wisely. We argue that once customers get Splunk optimized, it can be one of the most powerful cost-reduction weapons any organization can have.





*Is Splunk expensive  
when fully optimized?*

*NO.*

## CHAPTER 5

# Wrapping Up

So, let's review.

1. Companies that thrive are the ones that know how to make the most of what they've got at their disposal, maximizing operational efficiencies while driving out unnecessary costs.
2. Splunk gives you the ability to create powerful solutions for your organization, but the dashboards and visualizations you create are only as good as the data you have available. The ability to "see more" in Splunk depends on the absolute certainty you have the right data — all of it — reporting in.
3. The ability to "create more" powerful solutions depends, in part, on your ability to get others in your organization using the platform. That means you need to make day-to-day usability throughout your organization as simple and painless as possible. No small feat for a highly-technical platform like Splunk.
4. You can "save more" with Splunk through effective license management, maximizing operational efficiencies, and making the platform more useful to more people in the organization.

If the statistics we talked about in the introduction hold true for Splunk and it's possible your organization could be missing out on 50-80% of the value Splunk has to offer, then one of the best things you could do — recession or not — is activate

that untapped potential for your organization.

While it's possible to "go it alone" when creating these outcomes in Splunk, why not lean on the power of the Atlas platform to accelerate your results and unlock the untapped potential of Splunk?

With Atlas you'll instantly be able to:

- See how much of your license each data type is consuming
- Find out who's using which data types (or if they're utilized at all)
- Launch powerful SPL searches KGI's curated library (or add your own)
- View all your forwarders (and see what's missing) from a single pane of glass
- Monitor data sources and eliminate "dark" or missing data
- Get on-demand Splunk help from a real person, when you need it most

All with push-button simplicity in a beautiful, easy-to-use interface. Not to sound like a clichéd tech company, but we really do believe you're going to love it.



THE CREATOR EMPOWERMENT  
PLATFORM FOR SPLUNK.

**30 DAYS FREE.**

**REGISTER**



© 2023 Kinney Group, Inc.

Splunk is the trademark of Splunk, Inc.. Other names are trademarks of their respective owners. This documentation is provided "as is" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose, or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Kinney Group, Inc. shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information contained in this documentation is subject to change without notice.

Kinney Group, Inc., 4 Carter Green, Suite 250, Carmel, Indiana, 46032

DMWS eBook 3-20922