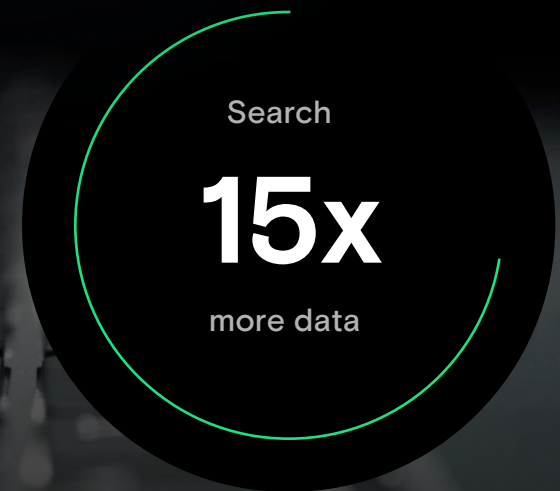


# Turn **dark security data** into real-time insight with **Splunk** on Sunlight

splunk>

SUNLIGHT

EDGE - CLOUD - ON PREM



Find out what you could save:

[sunlight.io/splunk-calculator](https://sunlight.io/splunk-calculator) ↗

## Security insight without the holes

Ensuring your data infrastructure is always secure, available and performant is now fundamental to your operations. You can't protect what you can't see, and for CIOs, CISOs and infrastructure leaders, real-time visibility into the security, health and performance of your business workloads that are running in your datacenters, in the cloud, and increasingly at the edge is critical.

## Dark Security data is a risk

However enterprises are struggling to collect, manage and draw insight from their security data in reasonable timeframes and within a reasonable cost – leaving much of the data 'dark' or unprocessed. This leaves them open to the potentially disastrous consequences of a cyberattack. Sunlight has worked with several customers looking to solve these challenges. At the heart of the issue is that the legacy infrastructure that runs Splunk itself isn't up to the task of pushing the huge volumes of data that must be collected, summarised and searched to generate the real-time alerts and reports that the security organisation needs to address the issue.

## A new architecture for Splunk

Sunlight engaged with independent expert Splunk consultants – to define a new architecture for Splunk deployments based on Sunlight's high performance infrastructure stack and to benchmark the results that could be achieved. This paper describes the transformational results they found and what it means for your organisation.

## What if you could

- Triple your Splunk user-base with no increases in infrastructure cost?
- Never miss an alert or have gaps in real-time dashboard and report data?
- Run hundreds of security use cases without worrying about performance?
- Reduce your Splunk infrastructure costs by over **65%**?
- Reduce your Splunk licence costs by over **50%**?

SUNLIGHT

Search

15x

More data

Reduce

50%

Of Splunk license costs

Reduce

65%

Of Splunk infrastructure costs



## Splunk is now your security command center

You have invested in Splunk because you know that providing secure and resilient IT in a large enterprise is a top strategic objective. Splunk allows you to reach deep into business areas across the enterprise, and you rely on Splunk Enterprise Security for monitoring and detection, incident response, threat hunting and vulnerability assessment. Splunk dashboards and reports give you a 30,000 foot view of what is going on across the entire estate.

## You now have a bigger attack surface to protect

Your organisation likely has hybrid infrastructure - in your own datacenters, in multiple cloud locations and perhaps even at the edge - in branch offices or factory floors. In a post-covid world, many more users are accessing services remotely. There are not only more sources of data from the expanding infrastructure, but the infrastructure is becoming more heterogeneous. This means more complexity, an expanded and distributed attack surface and more dark security data.

## Slow searches cause security blindspots

As your usage of Splunk correspondingly increases, the on-going performance demands of users' ad hoc searches, scheduled use cases, and more complex dense searches, often overloads the system and causes searches to be skipped, and critical data model acceleration to be delayed. This leads to:

- **Critical alerts and KPIs not firing** in a timely fashion (or at all) - potentially missing real-time security violations
- **Missed reports** - leading to gaps in decision making
- **Incomplete data in dashboards** - giving a misleading 30,000 foot view

In addition, slow search performance limits the scope of historic searches, meaning that longer term patterns may not be visible, meaning unusual patterns are not uncovered and attacks get through.

## “Dialing-up” not “dialing-back” Splunk is the answer

Resolving the issue by enforcing restrictions or quotas frustrates users. Requiring your Splunk experts to vet complex or historic searches consumes valuable resources that should be deployed on more strategic activities. Having to "dial-back" the type of data a Security team can leverage with the tool creates high risk "blindspots". All of these techniques reduce the overall utility of your Splunk investment and are at odds with the business motivation to adopt the tool in the first place.

Instead - “dialing-up” Splunk’s ability to capture and process data and provide real-time insight to your security team by using an accelerated Splunk infrastructure like Sunlight is the answer.



**Having to "dial-back" the type of data a Security team can leverage with the tool creates high risk "blindspots"**

## The Changing Threat Landscape

A rapidly evolving threat landscape, coupled with more security data and a larger attack surface means a high performance security infrastructure that can keep up is now essential to preventing a catastrophic cyberattack.

Top 5 reasons cybersecurity is more difficult today than it was 2 years ago

- 27% Monitoring security across a growing attack surface
- 23% Keeping up with the volume of security alerts
- 22% The cybersecurity team at my organization spends most of its time addressing high priority/emergency issues and not enough time on strategy and process improvement
- 22% Monitoring security across a growing attack surface
- 21% Investigating security incidents

Top 5 challenges in security analytics and operations

- 41% The threat landscape is evolving and changing rapidly
- 35% We collect an process more security data today than we did two years ago
- 34% The volume of security alerts has increased over the past 2 years
- 30% The attack surface has grown over the past 2 years
- 29% It is difficult ot keep up with the operational needs of our cybersecurity analytics and operations technologies

Percentages refer to the number of respondents who chose this (3 responses accepted)



## Getting to real-time business insight

The ultimate goal of businesses using Splunk is to get to real-time threat insight using as broad a sweep of data as possible across the entire application infrastructure - much of that data being dark today. Your dashboards and reports provide a live view of the application infrastructure and KPIs. Security professionals have access to current and historical data and machine-learning backed insights as they need it, and security incident resolution is reduced from hours to minutes & seconds.

## No blindspots = minimum security risk

In order to achieve this, your organisation must monitor as much infrastructure and operational data as possible - from the core datacenter to the edge - at high-fidelity, and in real time. This data must be augmented with intelligence sources to better understand the context and impact of an event. Using advanced detection methods such as machine learning you are able to get beyond the limits of human response and evaluation times. Splunk usage must be opened up to a far broader set of users, to allow all aspects of the business to extract insight from the system.

## A strong foundation for Splunk performance

Underpinning all of this is a robust and high performance Splunk infrastructure, such as Sunlight in AWS or your own datacenter, that doesn't limit Splunk indexing and search capabilities and allows the system to operate as close to real-time as possible without unreasonable infrastructure costs.



## The blockers to Splunk performance

Almost all customers will deploy Splunk in a virtual environment – either on VMware or Nutanix in their own datacenters or in a hyperscaler such as AWS. Given that an Enterprise Splunk deployment will consist of many servers – running these virtualized makes management and scale out considerably simpler.

However legacy virtualisation and storage, both on premises and in the cloud, is not designed for applications like Splunk that drive heavy IO, and a considerable overinvestment in underlying infrastructure is required. Even then, due to the latency and IOPS performance of those stacks, achieving true near real-time performance is prohibitively expensive.

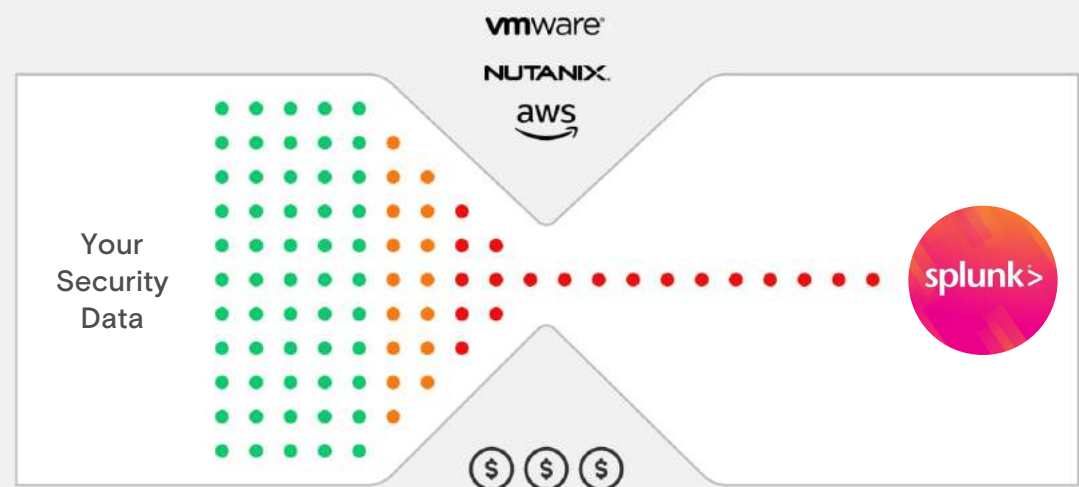
Running ever more scheduled search use cases and complex historic ad hoc searches in Splunk, alongside the basic data acceleration puts a heavy burden on the search and indexing tiers.

Whilst some of these contention problems can be mitigated by fine tuning search scheduling to maximize the search capacity, schedule tuning is a (human capital) intensive process, and often only a stop-gap to defer a more comprehensive solution.

## Are these slowing your Splunk down?

- New sources of data being added from more applications and infrastructure
- Increasing fidelity of data collected and tapping into dark data pools
- Addition of new use cases, including experimental scenarios
- Roll out to more security users
- Drive to real time reports and dashboards
- Adoption of machine learning for advanced detection

- ✓ Throttles Splunk search speed by over **90%** for dense searches
- ✓ Prevents expansion of Splunk monitoring across more dark security data
- ✓ Necessitates massive overinvestment in Splunk infrastructure to achieve required performance



## No more dark data with Sunlight

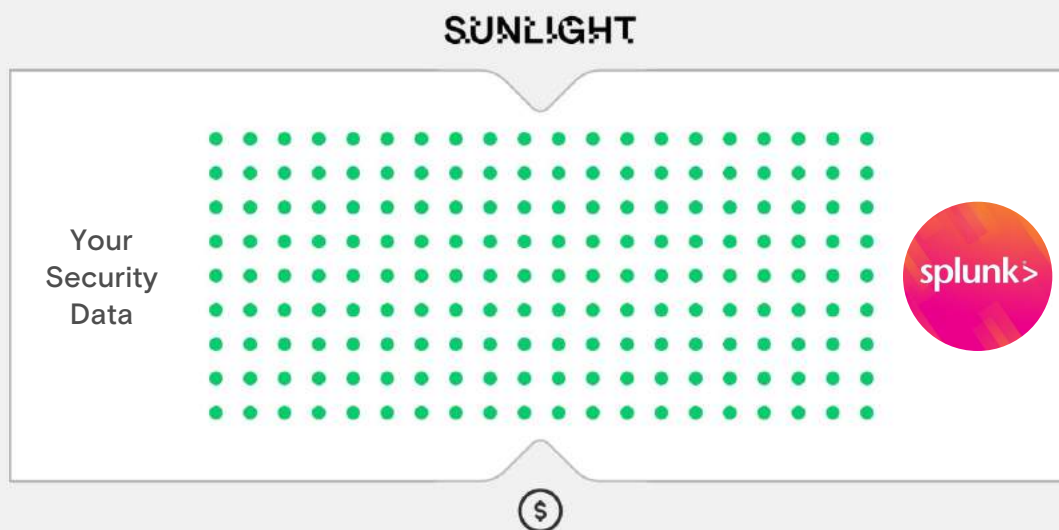
Sunlight NexVisor is a next-gen HCI stack, which has been specifically designed from the ground up to fix the performance gap that exists in the market. Sunlight has architected a complete hyperconverged infrastructure stack that can efficiently handle analytics workloads super-fast with bare metal performance without sacrificing on virtualization flexibility.

Sunlight NexVisor takes full advantage of NVMe flash storage and fast networking, giving you the ability to achieve near-real-time analytics performance at a manageable cost compared to running on legacy virtualisation. This extends to your AWS workloads - which can continue to run in AWS on NexVisor with no changes. Workloads can be scaled elastically and with linear performance - giving you maximum flexibility.

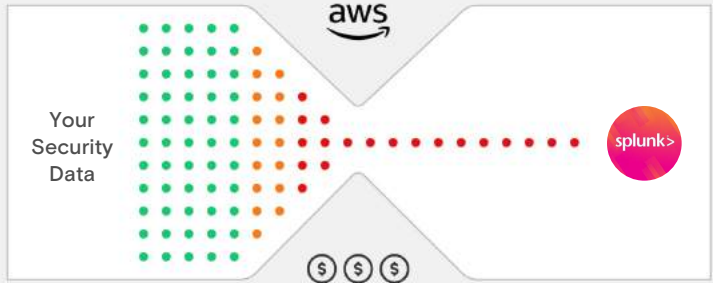
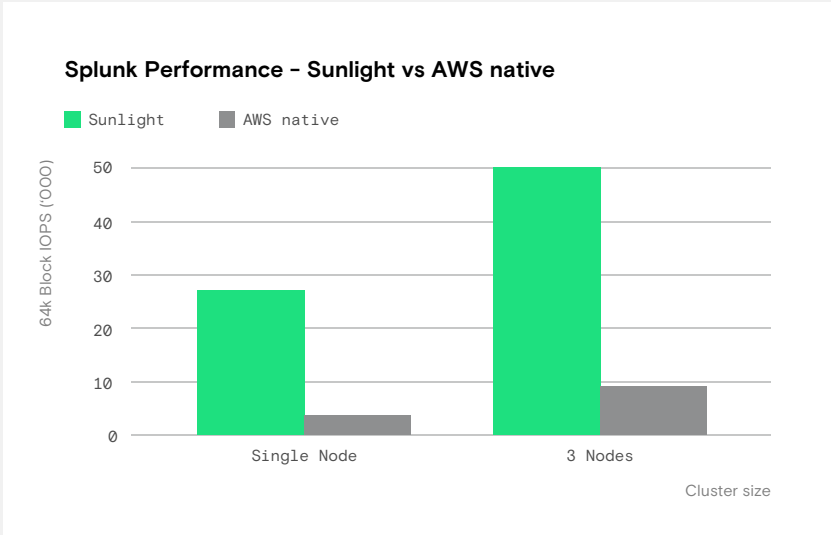
Sunlight NexVisor supports hybrid deployments and can run on-prem, in the cloud (AWS) or at the edge.

## Reduce your Splunk licensing costs

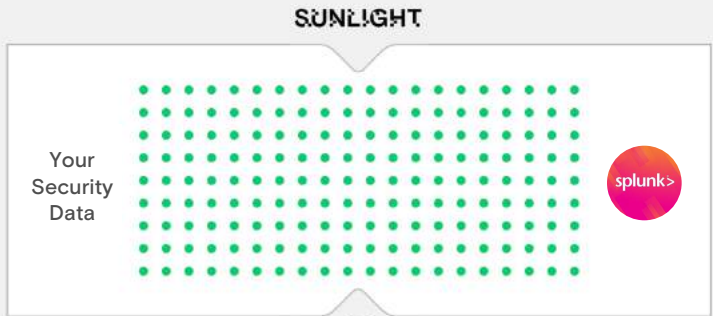
Whereas Splunk licencing is usually ingest-based, large Enterprise Splunk users with multi-terabyte per-day ingest rates may have access to infrastructure-based pricing - which is based on the number of vCPUs in the Splunk infrastructure. This allows large enterprises to ingest and search as much data as their infrastructure will support without having to worry about increases in Splunk licencing costs. Sunlight's performance improvement enables a reduction in vCPUs of over 50% which can lead a corresponding reduction in Splunk licensing costs.



- ✓ Enables Splunk to run at maximum performance - **45-1500%** faster
- ✓ Expand Splunk usage across a broader estate with more users
- ✓ Reduce Splunk infrastructure costs by over **65%**
- ✓ Reduce Splunk licensing costs by over **50%**



Splunk on AWS Native **100% IO Saturation**



Splunk on Sunlight on AWS **50% IO Saturation**

## Maximum Splunk performance, maximum infrastructure efficiency

Sunlight engaged with an independent Splunk partner, to benchmark Splunk running on Sunlight in AWS versus running it in AWS natively. The underlying hardware infrastructure was exactly the same in each case. The partner simulated an ingest rate of 1.6TB a day - typical of a mid-to-large sized enterprise. They measured the search performance of the system in each case.

Sunlight was able to show a huge search performance improvement without even getting close to saturating the storage IO.

Data Ingest Rate	<b>1.6TB per day</b>
Wildcard search time improvement	<b>Up to 45%</b>
Dense search time improvement	<b>Up to 1500%</b>

Get the full benchmark details here:

[performance.sunlight.io/splunk](https://performance.sunlight.io/splunk) ↗





## Case Study – Financial Institution

A mid-sized financial institution wanted to find a way to make their Splunk infrastructure more efficient to support their growing demands without leading to sky-rocking costs. They already ran Splunk in AWS with a 1.5TB per day ingest rate. To support their search burden, migrating their Splunk implementation to Sunlight led to the following infrastructure reduction and corresponding savings. The financial institution now has the ability to scale their usage of Splunk, particularly to support the ITSM product, with only small incremental infrastructure costs.



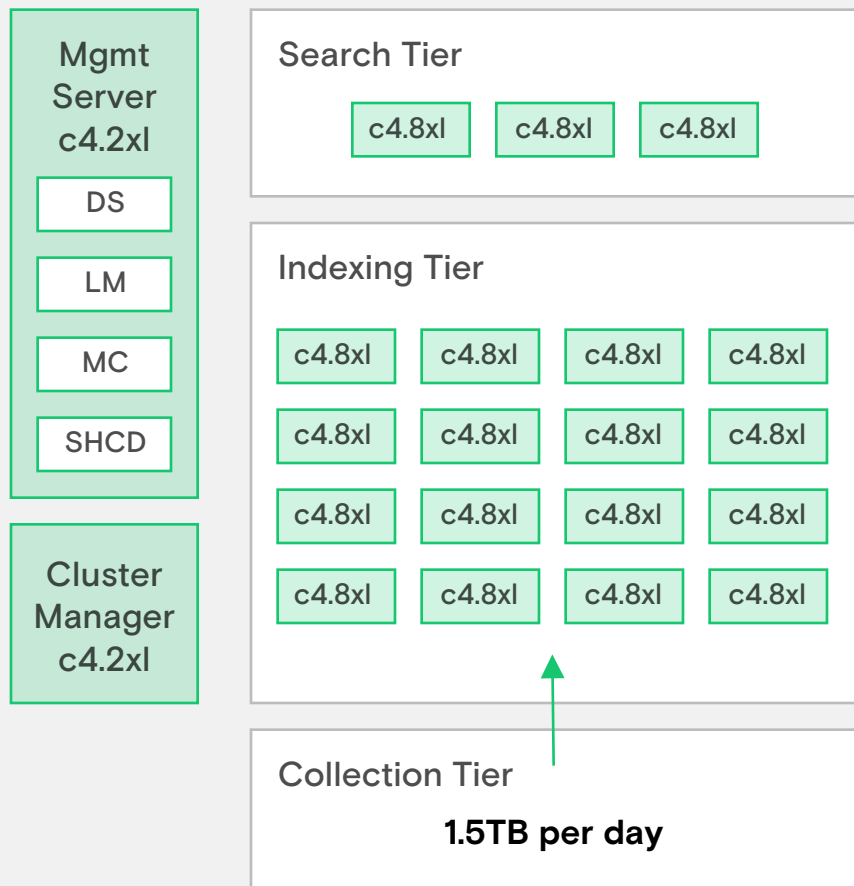
**By using Sunlight for our Splunk implementation, we're able to reduce the TCO by two thirds, meaning we can now expand our Splunk security coverage across more of the IT estate and monitor more security use cases."**

CISO, Financial Institution

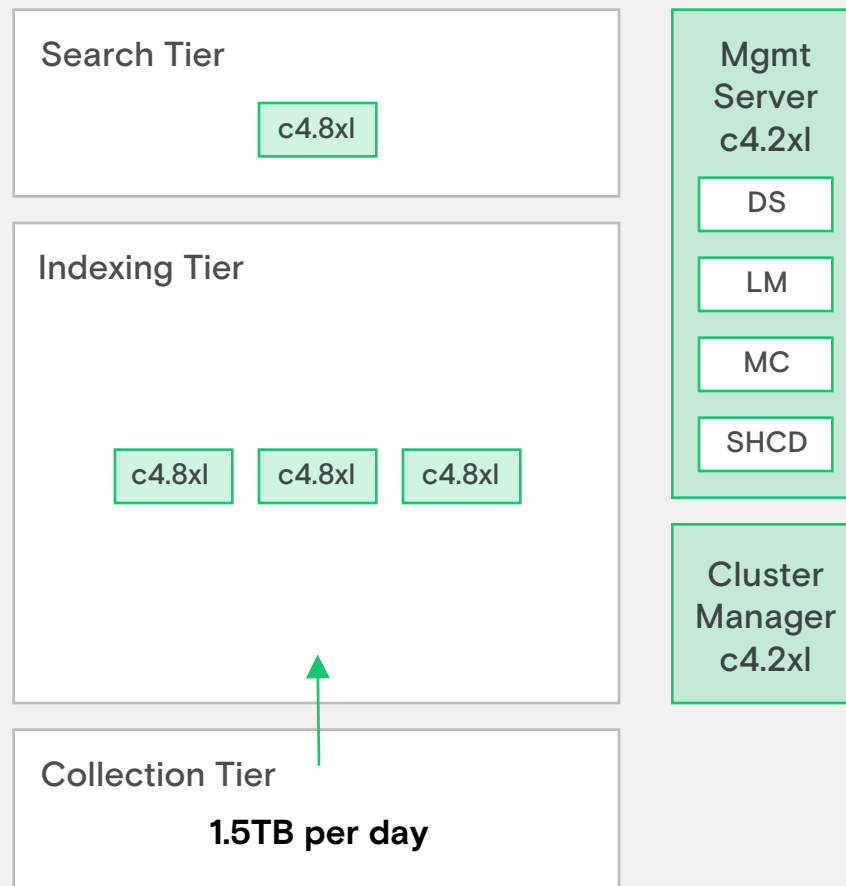
	 Native		 + SUNLIGHT	
	Nodes	Hourly Cost	Nodes	Hourly Cost
<b>Indexer nodes (c4.8xlarge)</b>	16	\$27.20	3	Included in Sunlight servers
<b>Search heads (c4.8xlarge)</b>	3	\$5.10	1	Included in Sunlight servers
<b>Management server (c4.2xlarge)</b>	1	\$0.40	1	Included in Sunlight servers
<b>Cluster manager (c4.2xlarge)</b>	1	\$0.40	1	Included in Sunlight servers
<b>Sunlight servers (z1d.metal)</b>	0	0	2	\$11.16
<b>Total AWS Costs</b>	<b>\$33.10</b>		<b>\$11.16</b>	
<b>Total Annual Cost</b>	<b>\$290k p.a.</b>		<b>\$98k p.a.</b>	

## Case Study – Financial Institution Architecture

### Before – Splunk on AWS



### After – Splunk on Sunlight on AWS



All VMs run on Sunlight on two z1d.metal servers

25%

The number of servers needed to process the same data ingest

## Splunk performance without the headaches

Customer benefits of deploying Splunk on Sunlight NexVisor include:

### Benefits to CISOs



#### Eliminate security dark data

Expand your usage of Splunk across more of your application infrastructure – eliminating blindspots and reducing risk



#### Onboard more Splunk security users

Enable more of your security team to take advantage of Splunk without having to add infrastructure costs or limit usage



#### Run more scheduled use cases

Increase the number of scheduled use cases that can be run to cover more security scenarios and reduce risk

### Benefits to infrastructure managers



#### Minimize Splunk costs

Cut the bloat of traditional virtualization stacks and cloud instances – slashing infrastructure and Splunk licensing costs



#### Easy management

Sunlight's management portal makes it easy to manage your entire Splunk infrastructure from a single pane of glass



#### Easy to get started

You'll be up-and-running with a Splunk-on-Sunlight trial fast and for free – and our technical team will walk you through every step of the process

# Get started Try Sunlight

If you would like to see how Sunlight can solve your Splunk performance problems without sacrificing flexibility and saving you 65%+ on infrastructure costs, then try our Splunk savings calculator and get in touch for a free trial.

[www.sunlight.io/free-trial](http://www.sunlight.io/free-trial) ↗

[www.sunlight.io/splunk-calculator](http://www.sunlight.io/splunk-calculator) ↗

✉ [sales@sunlight.io](mailto:sales@sunlight.io)

🌐 [www.sunlight.io](http://www.sunlight.io)

📍 Castle Park, Cambridge, United Kingdom

## SUNLIGHT

V1.0 - 7 APR 2021

Sunlight makes performance possible anywhere - from the cloud to the edge. Demanding applications like AI, Big Data, Analytics and Rendering run 3x faster on Sunlight compared to legacy virtualisation, and because Sunlight has a tiny footprint - it's perfect for the edge. Enterprises and MSPs use Sunlight to cut the costs of delivering high performance IT by 70%. Sunlight is a complete HCI stack that can be deployed on-premise on standard data center hardware, in AWS and on resource-constrained far-edge devices.

in

🐦

[www.sunlight.io](http://www.sunlight.io)

Copyright © 2021 Sunlight.io and respective copyright owners. All rights reserved.