If you're speaking to a CFO, CIO or CISO, **licensing complexity is often a bigger differentiator than feature parity**.

Based on Splunk's published pricing models and your own discussions around Sentinel positioning, Sentinel is generally easier to forecast and govern, while Splunk offers more licensing flexibility but introduces more variables. [splunk.com], [splunk.com]

Executive Summary

Area	Splunk	Microsoft Sentinel
Licensing models	Multiple	Primarily consumption-based
Quoting complexity	High	Low to Medium
Cost prediction	Medium	High
Add-on licensing	Common	Often included in Microsoft ecosystem
Procurement effort	Higher	Lower
CFO friendliness	Moderate	High
Risk of overspend	Higher	Lower

Splunk Licensing Complexity

Splunk currently offers multiple pricing approaches:

- Ingest pricing (GB/day)
- Workload pricing (SVCs/vCPU consumption)
- Activity-based pricing
- Entity-based pricing (certain offerings)
- Separate add-on licensing for products such as Enterprise Security, SOAR and other modules. [splunk.com], [splunk.com], [sp6.io]

Challenges

1. Multiple Pricing Models

A customer must first determine:

- How much data they will ingest
- How much search activity they will perform
- Whether workload pricing is preferable
- Which add-ons are required

The "right" licence is dependent on usage patterns rather than simply the number of users or devices. [splunk.com], [sp6.io]

2. Difficult Budget Forecasting

Costs may be affected by:

- Log volume growth

- New integrations
- Increased search activity
- Additional security use cases

Consequently, budgeting often requires a detailed discovery exercise with Splunk or a partner. [splunk.com], [motadata.com]

3. Add-On Dependencies

A security team may discover that:

- Enterprise Security
- SOAR
- Observability
- IT Service Intelligence

all have separate commercial considerations. [sp6.io], [motadata.com]

CFO Perspective

A CFO often asks:

> "What will this cost if my log volume doubles?"

With Splunk, that answer can be more complicated because it depends on the pricing model selected and the workload being consumed. [splunk.com], [splunk.com]

Microsoft Sentinel Licensing Complexity

Sentinel is generally simpler because it is built around Azure consumption.

The primary cost drivers are:

- Log ingestion
- Retention
- Data lake/storage choices
- Optional Microsoft security products

Sentinel itself is fundamentally an Azure service.

Advantages

1. Single Commercial Framework

Most customers already have:

- Azure
- Microsoft 365
- Entra ID

- Defender

Sentinel simply extends existing Microsoft commercial agreements rather than introducing an entirely separate vendor framework.

2. Easier Cost Modelling

A finance team can normally estimate:

```
Daily log volume
×
Retention period
=
Approximate Sentinel cost
```

This makes budget discussions easier than modelling search activity, compute units and multiple licensing methods. (This is a practical simplification rather than a Microsoft licensing rule.)

3. Leverages Existing Investments

Many Microsoft data sources integrate naturally into Sentinel, reducing the number of separate products that need to be purchased and managed. Your own SecQube materials position Sentinel as part of the wider Microsoft security ecosystem.

What Customers Usually Find Confusing

Splunk

Customers often ask:

- Which pricing model should we choose?
- What happens if we ingest more data?
- Do we need Enterprise Security?
- How many SVCs do we need?
- What happens during growth or acquisitions?

Sentinel

Customers typically ask:

- How much data will we ingest?
- What retention period do we need?
- Do we already own Microsoft licences that reduce costs?

These are generally easier questions to answer during pre-sales.

Strong SecQube Sales Message

For a 250-3,000 seat customer, a compelling message is:

> Splunk licensing is highly flexible but often difficult to forecast because costs can depend on ingest volume, compute consumption, activity levels and add-on products. Microsoft Sentinel is generally easier to procure because it sits within the broader Microsoft commercial model, allowing organisations to align SIEM spending with existing Azure and Microsoft security investments. [splunk.com], [splunk.com]

For executive buyers, the conversation often becomes:

"Do I want maximum commercial flexibility, or maximum cost predictability?"

That framing tends to resonate strongly with CFOs and procurement teams.