For an executive stakeholder, the key licensing risk question is:

> **"What could cause my costs to increase unexpectedly over the next three years?"**

Splunk Licensing Risks

1. Log Growth Risk

Splunk's traditional pricing is heavily tied to data ingestion volumes (GB/day). As organisations add new security tools, cloud services, endpoints, retention requirements, or compliance logging, costs can increase significantly.

Risk: High
Typical trigger: M365 expansion, new SaaS applications, increased audit logging, mergers/acquisitions.

2. Multiple Pricing Models

Splunk offers ingest-based, workload-based, activity-based and entity-based pricing models, depending on the product and deployment. This flexibility can make it difficult to determine the most cost-effective approach and forecast future spend.

Risk: Medium to High
Typical trigger: Changes in search behaviour, data volume, or platform usage.

3. Add-On Licensing

Security capabilities may require additional licenses or subscriptions depending on the solution stack, resulting in budget creep over time.

Risk: Medium
Typical trigger: Expanding into SOAR, observability, threat hunting or advanced analytics.

4. Contract Negotiation Dependency

Splunk does not generally publish comprehensive public pricing for enterprise deployments, meaning costs are often determined through negotiated agreements.

Risk: Medium
Typical trigger: Renewals, expansion, vendor consolidation.

Microsoft Sentinel Licensing Risks

1. Data Ingestion Growth

Sentinel is fundamentally consumption-based. If logging volumes increase substantially, Sentinel costs will also rise unless data is filtered, archived, or moved to lower-cost storage tiers.

Risk: Medium

2. Azure Cost Management

Sentinel costs are closely tied to Azure resources, storage and retention. Organisations that lack Azure governance can see unexpected spend growth from data retention and related services.

Risk: Medium

3. Retention and Compliance Requirements

As regulatory requirements increase, organisations may choose to retain more security data for longer periods, increasing storage costs. This is particularly relevant for sectors such as healthcare, defence and financial services.

Risk: Medium

4. Dependence on Microsoft Commercial Framework

Sentinel is integrated into the wider Microsoft ecosystem. Organisations that later decide to move away from Microsoft security services may need to re-evaluate their operational and commercial model. Your own discussions position Sentinel as closely aligned with the Microsoft security stack.

Risk: Low to Medium

Executive Risk Comparison

Risk Area	Splunk	Sentinel
Cost predictability	Medium	Higher
Log volume growth	High	Medium
Licensing complexity	High	Low

Procurement complexity	High	Low
Add-on licence exposure	High	Lower
Budget forecasting	Difficult	Easier
Vendor lock-in concerns	Medium	Medium

CFO Summary

Splunk's biggest licensing risk is commercial complexity. Multiple pricing models, growing ingestion volumes, and add-on products can make budgeting challenging.

Sentinel's biggest licensing risk is uncontrolled data growth within Azure. However, the licensing model is generally easier to understand and forecast because it sits within an existing Azure/Microsoft commercial framework.

> **Splunk presents a licensing management risk, while Sentinel presents a data governance risk.** The former is harder to forecast; the latter is easier to control through good data retention and Azure cost management practices.