Betting the business

Search for a Safe and Scalable Environment

Thousands of companies make decisions every day on where and how to deploy new features of their operations and even totally new ventures. Solitaire Interglobal Ltd. (SIL) is normally involved in that decision-making process by modeling the risk and cost-benefit for a large customer base that stretches around the globe. Our expertise is centered around complex modeling that incorporates holistic views of an organization, but for others rather than for ourselves.

In 2018, SIL found itself in a somewhat unique position. Intellectual capital that had been developed over the years came up in a general data mining analysis as being highly applicable to a changing trend in the overall marketplace. A quick review, followed by an extensive discussion led SIL to make the decision to move forward on this new business opportunity ourselves, rather than handing it off to one of our business partners.

The demands of a commercial, customer-facing business unit were totally new territory for SIL, and our analysis group jumped in enthusiastically to drill down on the ramifications of this strategic direction. Over 7 million models later, an approach had been developed and criteria defined to empower effective selection of platform and business partner.

The window for selection was less than three months, and critical pathway tasks depended on that timing.

APPROACH

The general approach that SIL took was to analyze multiple petabytes of data to define the weaknesses of deployments for new ventures. This was inclusive of other disruptive technologies that demonstrated the same growth pattern produced by the initial data mining.

Since SIL has been modeling predictive performance for over 40 years, as well as monitoring aspects of business and security for more than 23 years, a substantial repository of real-life data was available for the analysis. By drawing on the information of the Global Security Watch (GSW), cost and risk factors that were very current in the existing shape of cyberspace could be factored in.

Additionally, SIL supports more than 6500 worldwide customers with a spectrum of modeling services that deliver millions of analyses per year in support of critical decision-making. The information from that activity was also mined for supporting experiential reference.

Security, financial impact, longevity, and broadscale risk information allowed SIL to evaluate the opportunity and distill a clear set of decision criteria. Only by taking a

holistic view, could SIL provide itself with what millions of executed analyses had delivered for customers.

The criteria included evaluation points around the increasing connection of people and organizations within the Internet. Knowing that this was a market-driven initiative, SIL factored in security and exposure based on the virtualized interconnected and cloud-oriented world that businesses have to exist within today.

CRITERIA

The areas of criteria identified were those that have shown themselves to be critical for our customers and other businesses worldwide over the last two years. With the rapidly changing face of cyberspace, understanding the current environment is crucial since the market's volatility alters from minute to minute.

A general list of the criteria looks like a summary of the majority of articles written today about doing business over the web. The number one area is that of security, driving the safeguard of uninterrupted business operations, and keeping control of proprietary digital assets. Other areas of concern highlighted feasibility, finances, and risk.

The category list for SIL's criteria can be summarized as:

- Security
- Platform Feasibility
- Financial Costs
- Risk

In each of these categories, specific areas of concern were evaluated in the findings used as input to the decisions that needed to be made.

SECURITY

The first and foremost consideration for the proposed new service was the safeguard of customer data and the intellectual capital of both the new venture and the contributing content providers. Without these assets being protected, there simply would be no possible way that the business will succeed.

It is well understood today that cyberspace is extremely difficult to secure. The increasing integration between cyberspace and the physical world has exponentially expanded the opportunities for theft, damage, and corruption. The proposed venture was one that would rely totally on operating in the digital market, and hence electronic protection of its assets and operations was deemed the most critical criterion of all.

With a high level of experience that SIL has in analyzing the impact of security on business, the evaluation team was extremely sensitive to the fact that not only are threat levels are higher today than they ever have been, but the trend continues to accelerate. If the requirements to protect the new venture's operation was substantiative in terms of cost and personnel requirements, there would be myriad impacts on financial feasibility and customer reach.

Therefore, SIL exhaustively examined data from the Global Security Watch (GSW). This is a member service that has tracked the detailed evolution of security threats and the

associated effect on business on a worldwide basis and currently collects reported information from more than 10.1 million organizations.

The data from the GSW provides an unmatched source of threat intel from a business perspective that provided input to the analysis and is built on a foundation of real-world production information. Although threat footprints and other detailed mechanisms are collected in the GSW, the main focus relates to the impact on the business operation, organizational assets, and prevention and remediation costs. This meant that the data source was ideal as input to the evaluation.

A broad-scale analysis of the findings for the last five years showed an increasing trend in both the number of security incursions and the financial scope of those for media-handling organizations similar to the deployment that SIL was investigating. A large number of thefts of creative content have occurred over the last several years in video, entertainment, and publishing organizations.

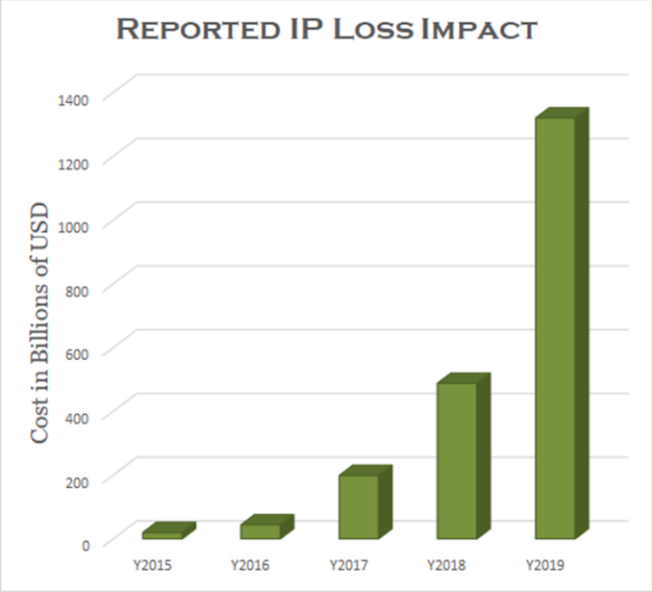
These customer-reported incursion details showed an exponential rise in both frequencies and associated damage costs. This included not only the immediate cost to address the security breach, but the cost of modification to procedures and the long-term loss of benefit from exclusive IP ownership.

Knowing that this was a pivotal point for a venture that will be streaming unique intellectual property, the ability of the selected solution to unilaterally encrypt all data was tagged is crucial.

An organization's client and corporate data is a crucial resource. It is literally priceless since it forms the core market advantage and intellectual capital of any business. Encryption has been one way of protecting this asset since once encrypted, its availability and vulnerability to hackers is eliminated. Many of those assets are currently unprotected, and that was made evident by the GSW customer reports.

Within the data that SIL had available, the reported financial loss based on damaged or stolen IP showed a grim picture. It was evident that unless addressed, any exposure of the new venture's IP would be unacceptable.

A summary showing the trend of IP asset security impact can be seen in the chart below. This includes only customer-reported data, rather than any extrapolation or projection. The information results from the aggregation of more than 6 ½ billion individual reports to the Global Security Watch, covering worldwide commercial and public sector organizations. Over 85% of the initial estimates have been substantiated by the tracked actual costs within the reporting entity.



Security deployed in the most efficient and effective manner was the most crucial requirement in the evaluation and selection of platform on which to launch the new streaming service.

PLATFORM FEASIBILITY

Although it was difficult to see past the urgent need for security, including data protection and privacy, there were other high priority requirements for the new venture to become a reality. That area of platform feasibility included the capability of the selected platform to scale since the demand for capacity would have significant peaks.

Additionally, the entire area of quality of service would need to be considered since the end customer response would be driven by consistent delivery and meeting expectations of speed.

Existing streaming services have significant issues with erratic delivery, broken links, and spotty coverage. Although the proposed new venture does not share many of the characteristics of current video streaming, its reception would be adversely affected by any of those problems.

With a significant growth potential and a worldwide launch planned, the nature of an active cyber market indicated a need to balance the risk of exploding demand against an infrastructure that could quickly and easily scale to address any level of capacity demand.

Realizing that the criteria in this area addressed the raw ability to scale, financial considerations were not addressed at this point. Instead, the ability of the platforms under consideration to handle peak workload without infrastructure modification and the load thresholds that could be maintained on an ongoing basis were examined.

Additional factors that played into the evaluation in this area included any delay in supplemental capacity availability and the degree of automation that was possible to remove the human element from the execution timeline.

FINANCIAL COSTS

Of course, there was a financial component to the evaluation. After all, just because it's possible to provide a service doesn't mean that there is a commercial justification for doing so.

There were several areas of financial metrics that were identified as critical to the decision. They can be summarized as:

- Cost to deploy the initial application in terms of weighted time expense
- Cost of security, both initial and ongoing
- Cost of scalability, both core and associated with growth

As with most things, the analysis showed that it is not the initial cost that is the most substantial, but the upkeep and ongoing operations financial impact. Therefore, the total cost of ownership (TCO) was the primary metric used.

RISK

The perspective that SIL takes when viewing risk is that it is an accumulation of not only the possibility of shortfalls in protection, deployment, and operations, but the metric must include the scope of the impact of that failure. Given that, the risk evaluation was structured to build an accumulated risk metric that would provide the decision-making team with a consistent and useful criterion.

Since SIL risk analysis is built on an actuarial basis, the extensive data reported by SIL customers and participants in GSW was used to create that complex probability matrix. With an excess of 164 million discrete data points, each of the possible platform solutions received intense scrutiny.

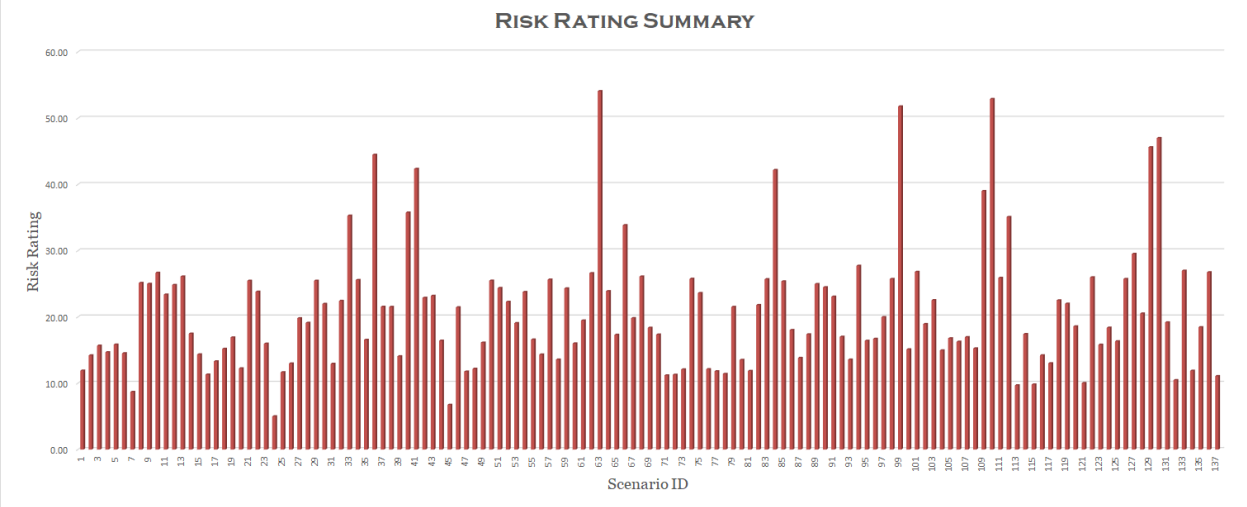
RISK-BASED SOLUTION FILTERING

SIL works with millions of model requests every year. One of its strengths is the massive database the covers the aspects of risk and behavior. Any time that a SIL model is requested, that ocean of data is mined for possibilities. Over 50% of these predictive models start out with more than 500 options.

Depending on the parameters set by SIL customers, the field is narrowed down to a more comprehensible number of scenarios before being further culled. This is a process that is executed hundreds of times per day in the SIL analytic labs.

This standard SIL process produced an initial field of 712 possible scenarios for internal SIL consideration. After the first round reduction, 137 were left. These included on-premise infrastructures, public cloud solutions, MSP offerings, and hybrid cloud infrastructures. All of these options were modeled to build comparison points. The consolidated risk rating was used to do the first level cut.

Any scenario with a risk rating of over 15 was deemed unacceptable, and anything rated more than 10 discarded as significantly high risk. The general risk metric for the solutions can be seen in the chart below.



All of the solutions that exceeded the threshold for high risk were eliminated, and only those that were medium to low risk were considered.

This group of shortlisted platform solutions included only five scenarios. Each of these was reviewed in more detail.

None of the solutions presented a low-risk profile. This was not unexpected since the venture being considered was a significant paradigm shift in both the streaming and entertainment environment. In any new creative endeavor, there is a considerable element of risk, and that was not ignored when building the evaluation profile.

However, the platform contribution obviously needed to be minimized, so that the overall feasibility of the project was not additionally burdened.

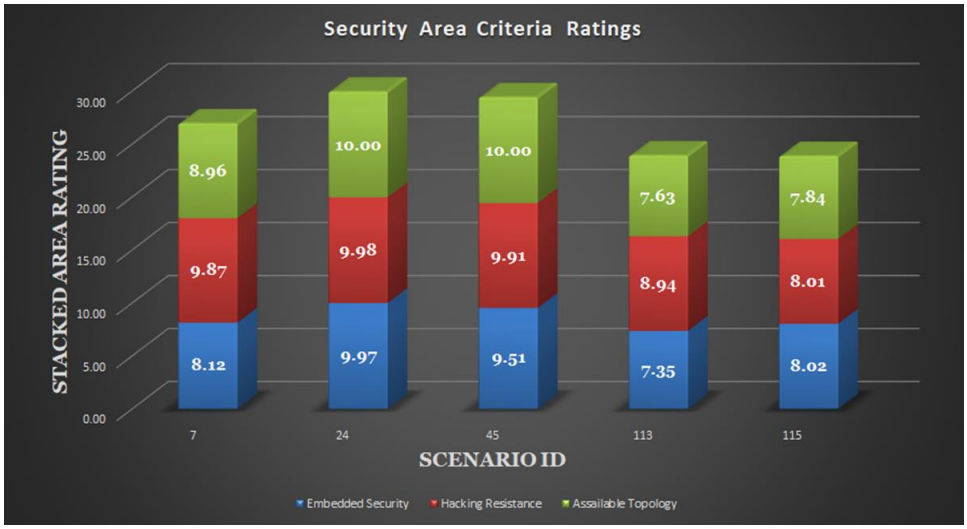
The evaluation committee found it extremely interesting that all of the shortlisted scenarios shared key components that addressed security and scalability. To differentiate among the options in this group, the secondary criteria would have to be factored in, but first, verification of operational abilities was required for the first two areas.

SECURITY PLATFORM COMPARISON

The evaluation criteria within the security area involve the level of encryption of data and operations, the ability of the platform to set up automatic encryption so that the chance of anything slipping through the system lifecycle without encryption was minimized, and the robustness of the system resistance to cyber incursions.

The factors that had to be considered included the embedded security components of the underlying operating system, the demonstrated track record of historical hacking resistance, and the modeled assailable topology of deployment on each of the five solutions.

In these areas, each of the options was rated on a scale of 1 to 10, with 10 being the best. The chart below shows the findings of the evaluation group.



The shared architectural components among some of the solutions were evident in their similarities in the three focus security considerations. While each of the solutions would have differing details for deployment, the preponderance of data indicated that any one of these would be acceptable from the perspective of IP protection.

PLATFORM FEASIBILITY COMPARISON

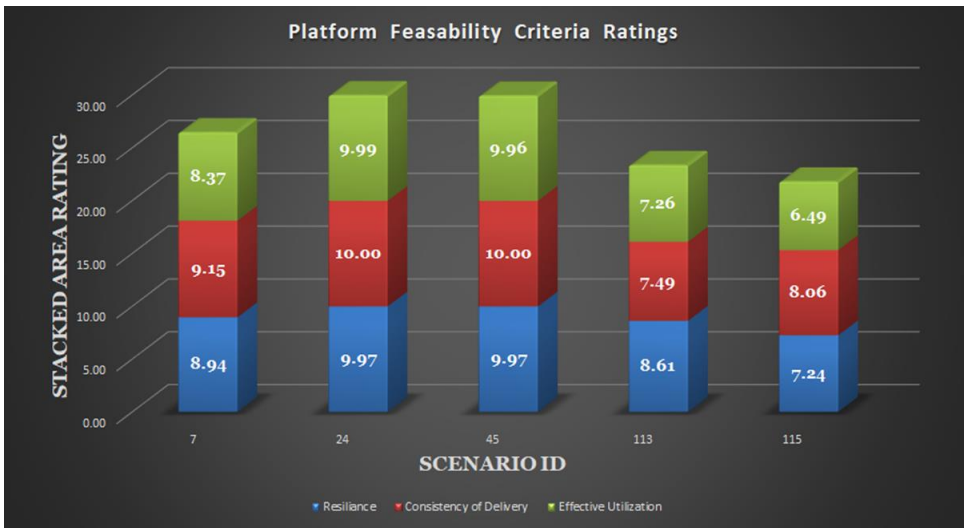
The next area to undergo a detailed examination was platform feasibility. The specific evaluated criteria within this area looked at demonstrated deployments combined with a modeled application for the new venture.

Since ultimately, the IT infrastructure is designed to support business functions, the ability for the selected scenario to host and deliver the services was paramount. Having a highly secure platform would be relatively useless if the proposed products and services could not be made available to the end customer in a professional manner.

The criteria in this portion of the evaluation matrix quantified the ability of the platform to handle the necessary load of operations, as well as its resilience and handling spike workload. Since SIL wanted the best possible quality of service, the consistency of demonstrated service delivery needed to be outstanding.

The third aspect under examination was the solution's effective use of the platform. This area relied on the demonstrated ability to load the capacity of each platform in an operational environment without significant outages or system failures. Although this is a combined synergy among operating system, hardware architecture, and database, since the solution presented in each scenario is a package, only a single metric was considered.

Once again, relying on a rating metric that ranges from 1 to 10, the five scenarios with their associated ratings can be seen in the table below.



The variations in the parameters in this area widened the difference between the proposed scenarios substantially. With stated goals of the offered service citing quality as a pivotal differentiator, the evaluation group was now able to articulate the impact of each option against that goal.

FINANCIAL COMPARISON

The total cost of ownership (TCO) provides one of the central business-side metrics for a business case evaluation. This high-level metric aggregates all of the expenses within the organization that contribute to any aspect of the deployment and operation.

TCO is comprised of the expenses necessary to run a continuing operation. The categories of expense in this metric include IT operations staff, break and fix application support, outside services to supplement operational staff or problem solve, power and cooling expenditures, hardware and software maintenance and licensing, and floor space.

The costs for both staffing and the infrastructure are auditable, while the price for incursion effects is a combination of both objective and customer-projected subjective amounts. In all cases, the numbers are obtained from customer reports and have not been altered, but instead, have been simply aggregated and averaged across the analysis base.

The specific criteria that were examined in more detail within this comparison area included a relative rating for per user delivery of the media streaming service. This cost rating was more of a total cost of information or TCI. A broad model was done by SIL to

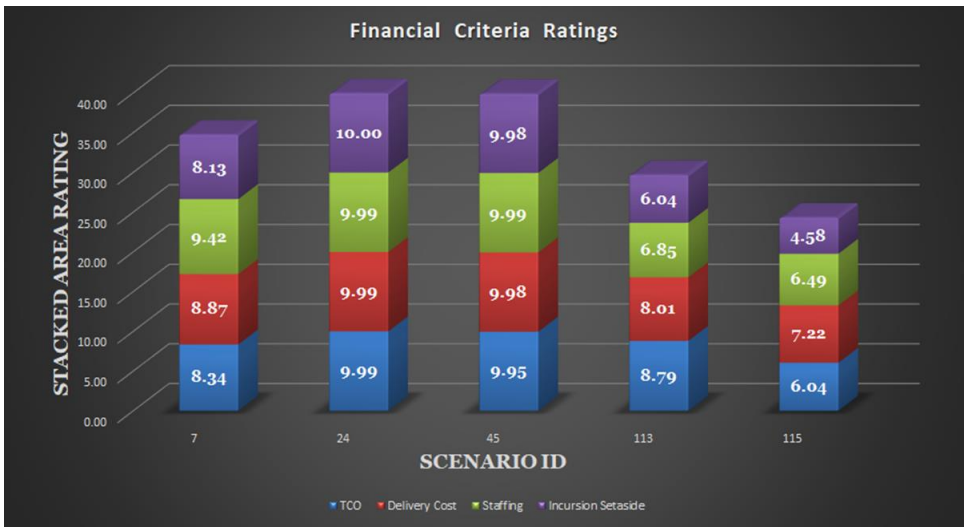
create a capacity demand profile for the same customer demand on each platform solution.

The third detailed area that was examined in the cost arena was that of staffing. The aspects of staffing include both the overall expense of staff hours and the availability of the needed skill sets demanded by the particular scenario. Since some of the options had extremely divergent staffing profiles, this specific criterion was included in the detailed analysis.

Finally, the impact of incursion costs and set-asides had to be considered. In today's market, the insurance industry is starting to define financial set-asides for different cyber profiles. This allows a better articulation of the financial risk that conducting business in cyberspace brings to an organization.

Generally speaking, this metric looks at things like remediation costs and impact on the customer base when an incursion occurs. However, this is not from the perspective of specific incidents, but instead the view of the deployment as a whole. As such, it was a vital consideration.

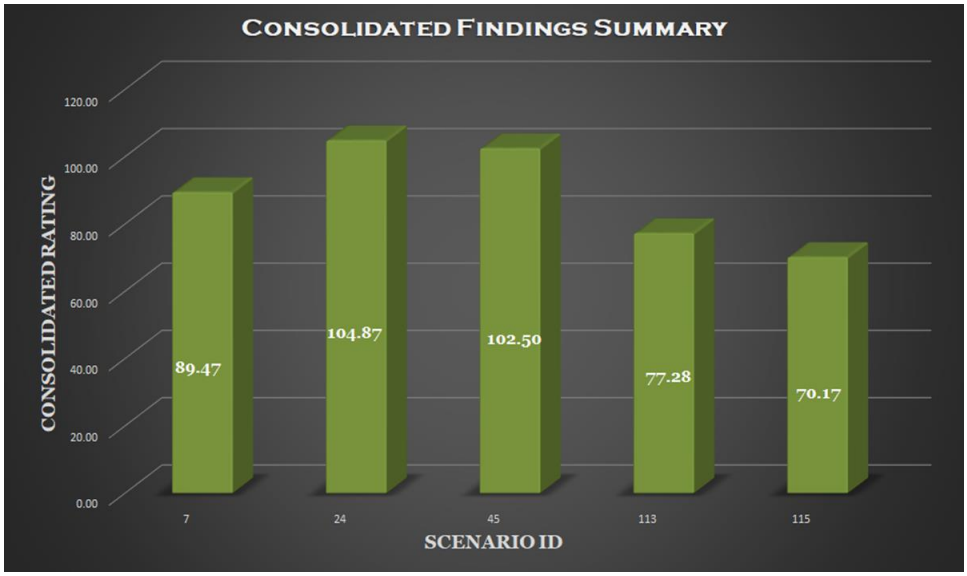
In this final area, there are four contributing measurements. The metric remains based on a 1 to 10 rating and can be seen in the chart below.



Once again, shared underlying similarities are apparent in similar scenarios that have a slightly different composition. However, the escalating differentiation was extremely evident in this sector of the evaluation.

FINDINGS SUMMARY

The evaluation findings were complete, and the final aggregation was done. It was the executive management team's hope that the extensive analysis would identify any substantial area of differentiation. When all of the findings were aggregated, the summarized rating that was submitted to the organization's decision-makers can be seen below.



The decision between scenario 24 and scenario 45 came down to finer points of comparison that were driven by decisions at the executive management level. The discussion at that level took far longer than it did for the initial modeling and evaluation. Only after the decision was made was the evaluation committee told what the different scenarios were.

SELECTED SCENARIO

The selected solution was IBM's Hyper Protect Services Cloud. Its embedded protocols for encryption and demonstrated excellence in security provisioning moved it to the shortlist. The quality of service delivered to and reported by customers made it one of the front runners. Finally, the efficient leveraging of the deployment platform and the ability to tie reasonable costs to actual utilization moved it to the lead.

The most compelling comparison points that the evaluation group found and that were articulated by the executive decision-makers can be seen in the table below.

Quick Summary

Category	Key Evaluation Comparison Point	Executive Take-Away
Risk	In a field of 137 different proposed solutions, the IBM Z-based Cloud Hyper Protect Service solution	The overall danger in deploying on the highly secure, scalable platform is lower by an order of magnitude.
Security Effectiveness	Out of hundreds of millions of reported incursions, there are none that resulted from failures in IBM Z platform shortfalls or failures during the last five years.	IBM Z provides the most secure data protection and privacy environments for application.
Platform Feasibility	While all five of the shortlisted scenarios showed excellent deployment feasibility, the IBM Z Cloud Hyper Protect Service contained the best solution for worldwide deployment, including scalability and reliability.	IBM Cloud Hyper Protect Services will allow an immediate deployment worldwide and will scale as needed without limitation.

Category	Key Evaluation Comparison Point	Executive Take-Away
Financial Impact	With a minimal requirement for additional training or staffing, coupled with an improved cyber insurance profile and premium, the IBM Z based Cloud Hyper Protect Services reduce the financial load by close to one-third of overall planned expenses.	IBM Cloud Hyper Protect Services mean that we can make better use of our capital.

In the situation that SIL found themselves, the ability to identify and articulate the metrics necessary to make an informed decision was critical. For the business, the shifting nature of cyber business was a significant danger. More rapid changes, active attacks, and a challenging risk management role, all combined to present substantial hazards to the proposed deployment.

The exhaustive selection analysis performed found a clear winner in the IBM Z-based Cloud Hyper Protect Services solution. Its clear differentiation in the areas of security, including IP protection and customer privacy, platform feasibility, cost, and overall risk made the selection of the IBM Z-based Cloud Hyper Protect Services solution the obvious choice for the new venture.