



# **White paper on the SaaS & Cybersecurity Landscape in New Zealand: Importance of SaaS Cost Optimisation and Cybersecurity Posture Management for NZX listed Companies.**

## **Introduction**

In today's digital age, businesses increasingly rely on Software as a Service (SaaS) solutions and robust cybersecurity measures to remain competitive and secure. This white paper explores the significance of SaaS cost optimisation and cybersecurity posture management, using market data from top companies listed on the New Zealand Stock Exchange (NZX). These insights aim to guide businesses in maximising their IT investments and strengthening their cyber defences.

## **SaaS Market Overview for NZX Companies: Market Size and Growth**

The SaaS market in New Zealand is projected to grow significantly, with an estimated market size of approximately USD 1.2 billion by 2024. This growth is driven by the increasing adoption of cloud services, digital transformation initiatives, and the need for scalable and cost-effective IT solutions across various sectors. Leading NZX companies are investing heavily in SaaS solutions to enhance their operational efficiency and agility.

## **SaaS Market Share Distribution**

The SaaS market share is distributed among several key players, with the top vendor holding approximately 18% of the market. The second largest vendor commands about 15%, followed by the third with 12%. Other significant vendors hold market shares of 10%, 8%, 7%, 6%, 5%, 4%, and 3%, respectively. These vendors provide comprehensive cloud service offerings that are widely adopted by enterprises across New Zealand due to their scalability, accessibility, and cost-effectiveness.

## **IT Budgets and SaaS Spend**

Collectively, top NZX-listed companies allocate significant portions of their IT budgets to SaaS applications. On average, approximately 20% of the total IT budgets are dedicated to SaaS solutions. This substantial investment underscores the importance of SaaS applications in enhancing operational efficiency and supporting digital transformation initiatives.

## **Cybersecurity Market Overview for NZX Companies: Market Size and Growth**

The cybersecurity market in New Zealand is projected to reach USD 507.60 million by 2024, with an expected growth to USD 1.03 billion by 2029. This growth underscores



the critical need for robust cybersecurity measures to protect digital assets from increasingly sophisticated cyber threats.

### **Cybersecurity Market Share Distribution**

The cybersecurity market is dominated by several key players. The leading vendor in this space holds a significant market share, followed by others who also have substantial presence. The distribution of market share among these vendors reflects the competitive landscape and the importance of comprehensive cybersecurity solutions.

### **IT Budgets and Cybersecurity Spend**

Top NZX-listed companies allocate significant portions of their IT budgets to cybersecurity. On average, approximately 15% of the total IT budgets are dedicated to cybersecurity measures. This allocation reflects the critical need to protect digital assets and ensure business continuity amidst a rising number of cyber threats.

### **Importance of SaaS Cost Optimisation:**

#### **Financial Efficiency**

SaaS cost optimisation is crucial for enhancing financial efficiency. By managing SaaS expenditures effectively, businesses can avoid overspending and ensure their investments yield maximum returns. This is particularly important for NZX companies with large-scale operations and significant IT budgets.

#### **Operational Flexibility**

Optimising SaaS costs enables businesses to remain agile and responsive to changing market conditions. Continuous evaluation and adjustment of SaaS expenditures allow companies to align their IT investments with strategic goals, maintaining operational flexibility.

#### **Enhanced Decision-Making**

Data-driven insights from cost optimisation efforts provide businesses with a clearer understanding of their SaaS usage patterns. This facilitates better decision-making, enabling companies to identify underutilised resources, eliminate redundancies, and prioritise essential applications.

### **Importance of Cybersecurity Posture Management:**

#### **Risk Mitigation**

Cybersecurity posture management is vital for mitigating risks associated with cyber threats. A strong cybersecurity posture ensures businesses can detect, respond to, and recover from cyber incidents effectively, minimising potential damage to their operations and reputation.

#### **Compliance and Regulatory Adherence**

Adhering to cybersecurity best practices helps businesses comply with industry regulations and standards. This not only protects them from legal repercussions but also builds trust with customers and stakeholders concerned about data privacy and security.



## **Business Continuity**

A robust cybersecurity posture is critical for ensuring business continuity. By proactively managing their cybersecurity posture, businesses can safeguard their operations against disruptions caused by cyber-attacks, maintaining uninterrupted service delivery.

## **Integrating Cost Optimisation and Posture Management**

Combining SaaS cost optimisation with cybersecurity posture management provides a comprehensive approach to IT governance. This integration ensures businesses manage their expenditures efficiently while maintaining a strong defence against cyber threats. By adopting solutions that offer both cost optimisation and robust security features, companies can achieve a balanced and sustainable growth trajectory.

## **Conclusion**

The SaaS and cybersecurity landscapes are rapidly evolving, presenting both opportunities and challenges for businesses. Cost optimisation and cybersecurity posture management are critical components of a successful IT strategy, enabling companies to maximise their investments while protecting their digital assets. As the market continues to grow, businesses must prioritise these aspects to remain competitive and resilient in an increasingly digital world.

## **Sources**

1. FMI Market Insights
2. Cognitive Market Research
3. Mordor Intelligence
4. Astute Analytica
5. Market.us
6. Flexera's 2024 State of the Cloud Report
7. Gartner's IT spending forecasts
8. Splunk
9. Malwarebytes
10. VentureBeat