InstaSafe
Cloud. Secure. Instant.

REPORT

THE STATE OF ZERO TRUST SECURITY

March 2023

2023

Table of Contents

CONTENTS

EXECUTIVE SUMMARY

The concept of Zero Trust security has gained a lot of attention in recent years as a modern security approach. The Zero Trust security model aims to provide better security by assuming that no user or device can be trusted, even if it is within the corporate network perimeter. This report will provide an overview of the current state of Zero Trust security and the challenges and benefits of implementing this model.

Zero Trust Security is one of the top cybersecurity priorities for cybersecurity leaders, and its adoption has been increasing over the past few years. One of the main reasons for the growing popularity of Zero Trust security is the rise in cyber threats. Traditional security models that rely on network perimeter defenses such as firewalls and antivirus software are no longer sufficient to protect against the advanced threats that exist today. Zero Trust security, on the other hand, takes a more comprehensive approach to security that focuses on protecting assets and data regardless of their location.

SURVEY FINDINGS ON THE CURRENT STATE OF ZERO TRUST

We reached out to various IT leaders who are decision-makers or influencers within their organizations to implement Zero Trust solutions.

Among all the survey respondents, almost 50% belong to CXOs level, 22% belong to Director level, and 10% were product specialists.

We saw a healthy distribution of respondents from different industry verticals. 15% from Software & Internet, 15% from Healthcare & Pharma, 13% from Retail, and 14% from Manufacturing.

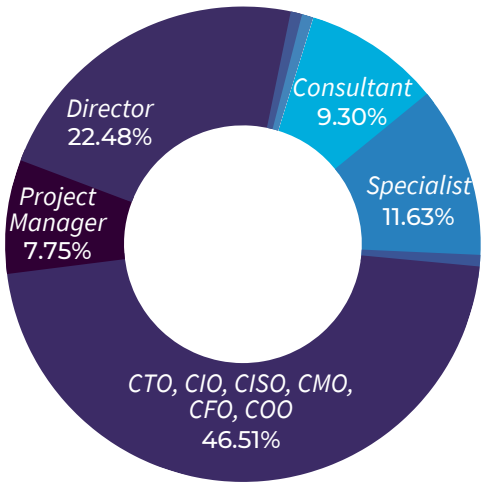


Figure 1: *Distribution of respondents based on Job Title / Seniority*

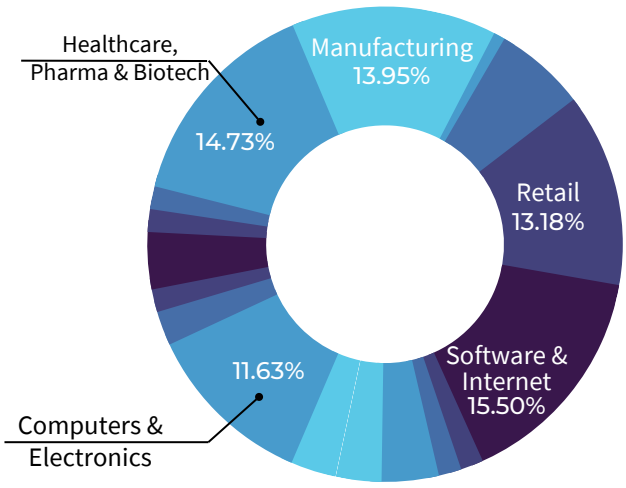


Figure 2: *Distribution of respondents based on their industry*

ORGANIZATION'S CURRENT POSITION ON ZERO TRUST SECURITY ADOPTION

63% of respondents have already implemented some form of Zero Trust solution and their adoption has happened mostly in the last couple of years. 10% of respondents are already in the vendor evaluation phase for the right Zero Trust vendor, and 23% of respondents are planning or thinking to implement in near future. Cumulatively, 99% of respondents are well aware of Zero Trust benefits and have taken some action towards its adoption.

Pre-pandemic, Zero Trust was a buzzword among a lot of IT leaders and there were lot of confusion on the importance of Zero Trust and its inherent benefits. Pandemic became the major accelerator for Zero Trust adoption, as cybersecurity threats also increased manifold.

63% of respondents have already implemented some form of Zero Trust solution and their adoption has happened mostly in the last couple of years.

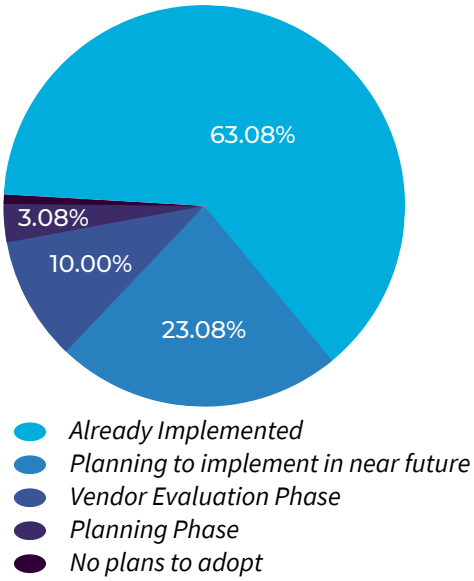


Figure 3: *State of Zero Trust Adoption*

TOP CONCERNS WHILE SECURING ACCESS TO PRIVATE APPLICATIONS

Around 86% of respondents feel unsecured access of private applications by third parties partners or contractors is their top concern, followed by internet-based attacks such as DDoS, Man in the Middle attack, Ransomware is the second most concern. Other concerns include infected systems getting access to applications can affect the entire network and internal users with privileged access can be vulnerable.

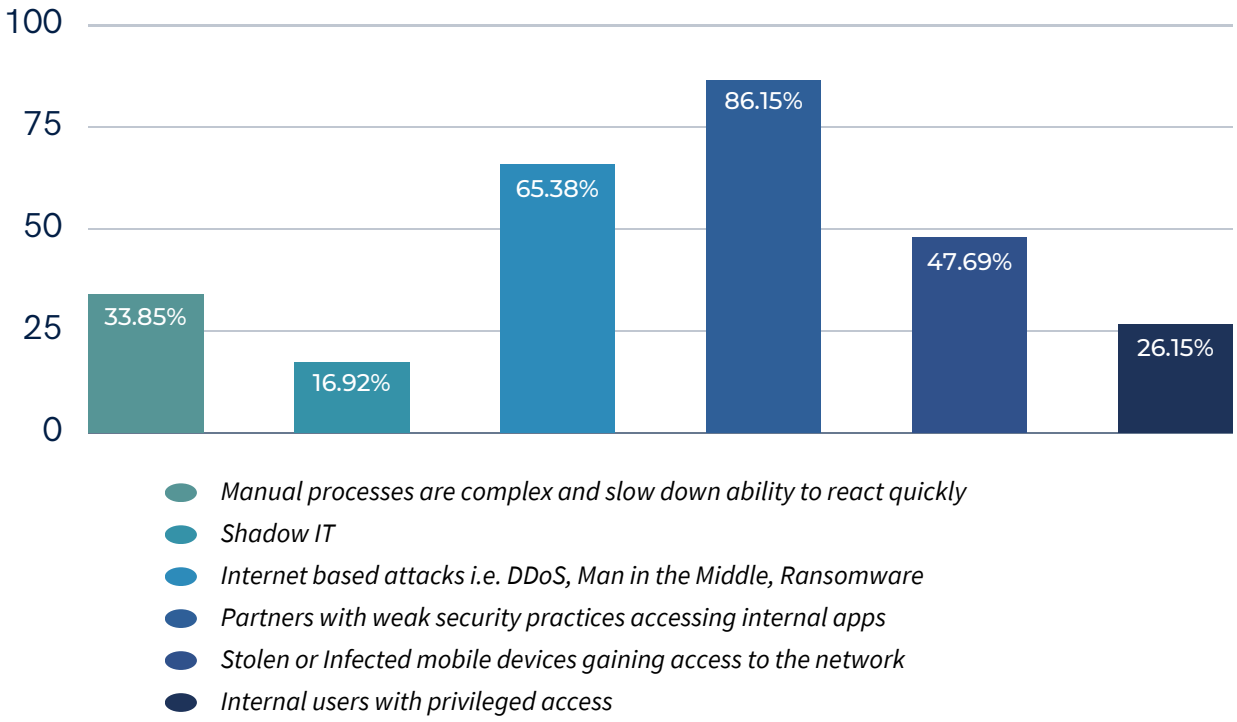


Figure 4: *Distribution of concerns for secure access of private apps*

TOP USE CASES OF ZERO TRUST THAT ORGANIZATIONS ARE LOOKING FOR

Securing access to applications across multi cloud environments is one of the primary use cases that organizations using Zero Trust. Other top use cases includes provisioning third party access to private applications and using Zero Trust as an secure alternative to VPN.

56.15% believe securing access to applications across multi cloud environments is one of the primary use cases that organizations using Zero Trust.

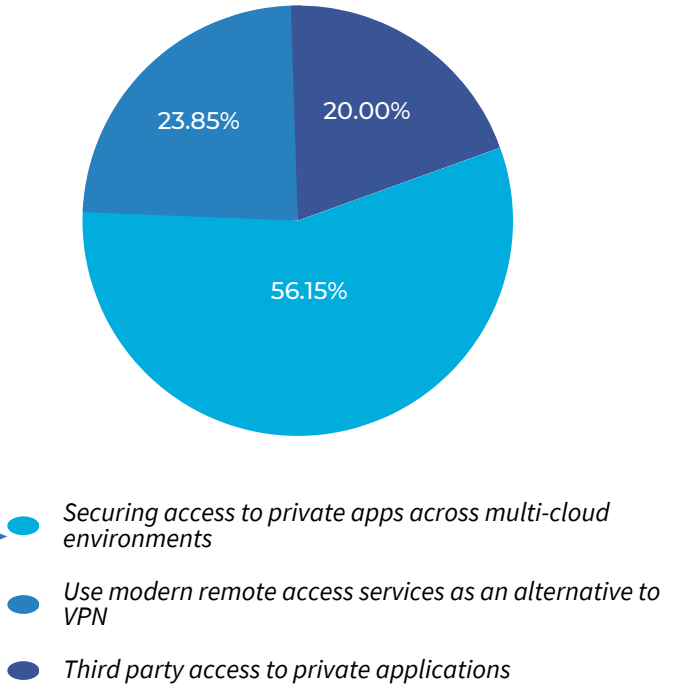


Figure 5: *Distribution of use cases for organizations using Zero Trust*

TOP SECURITY FEATURES OF ZERO TRUST THAT ARE MOST CRITICAL FOR ORGANIZATION

90% of respondents feel the most critical security feature is additional MFA for Identity management and the second most important is granular access controls for users. Other critical security features include Device binding, Device Posture Check, DLP, SSO, and user activity monitoring.

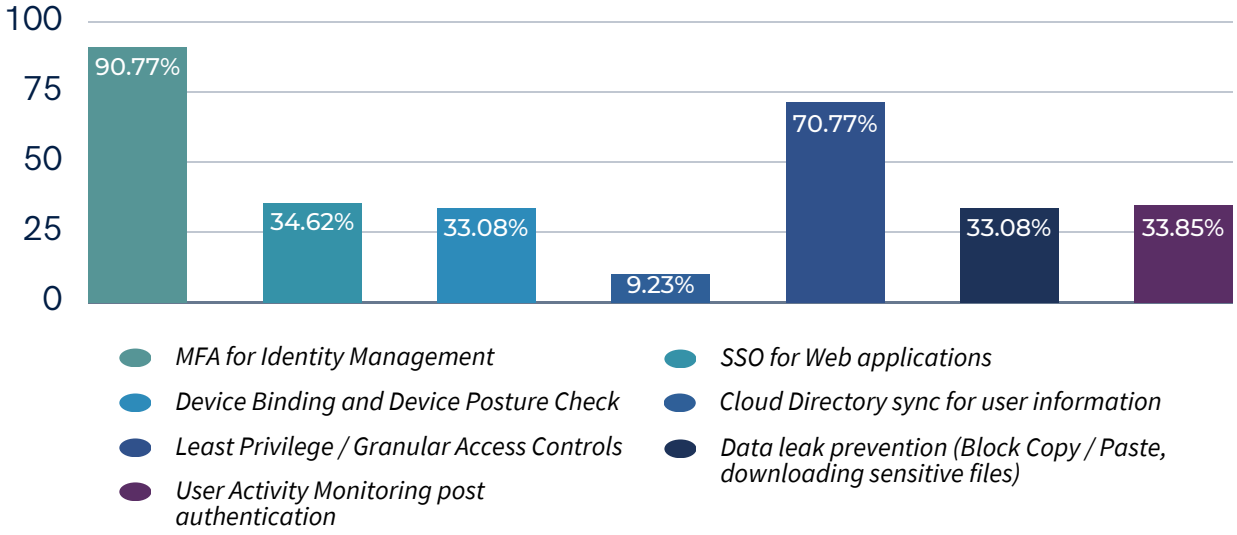


Figure 6: *Distribution of Top Security Features of Zero Trust that are most critical for the organization*

KEY BENEFITS OF ZERO TRUST ORGANIZATIONS ARE LOOKING FOR

Majority of the respondents feel enhanced security and better user experience are the key benefits that organizations are actively looking from the adoption of Zero Trust solution.

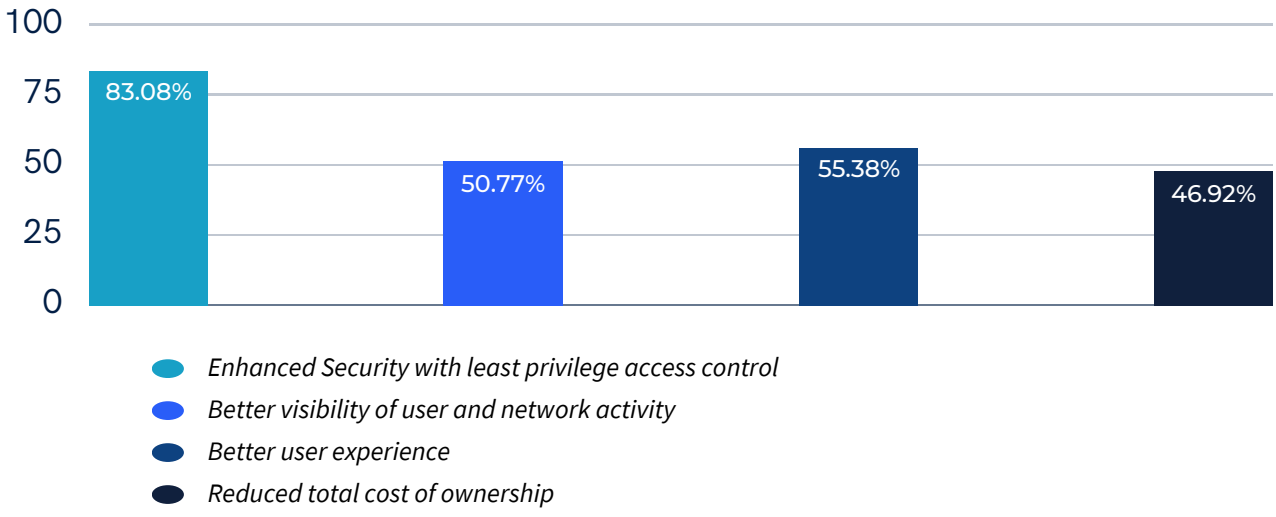


Figure 7: *Distribution of Key Benefits of Zero Trust organizations are actively looking for*

PRIMARY REASON FOR ADOPTING ZERO TRUST SECURITY

A large number of respondents feel Zero Trust is a better and secure alternative solution to Legacy VPN solution and is the primary reason for adoption of Zero Trust security solution. Because of the inherent security benefits of Zero Trust, the second most important reason for adoption is to include Zero Trust as part of cloud transformation initiatives.

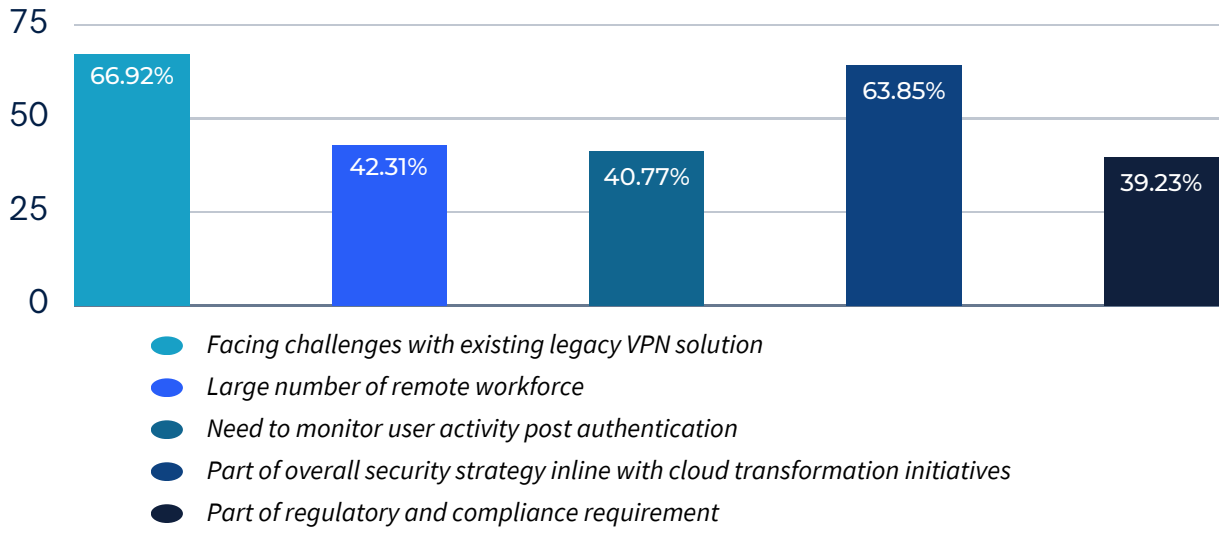


Figure 8: *Distribution of Primary reason for adopting Zero Trust Security*

TYPE OF USERS THAT ORGANIZATION HAS PROVISIONED FOR ZERO TRUST ACCESS

It is interesting to note that majority of organizations are using Zero Trust Access for their third party users which includes suppliers, consultants to connect internal corporate applications. The second most important user types include both internal and external users, which is a great indicator that organizations understand the importance of Zero Trust security. Zero Trust security is effective when it is utilized for both internal and external users. If only internal or external users are used, then security can't be made full proof as we are exposing threats from another set of users.

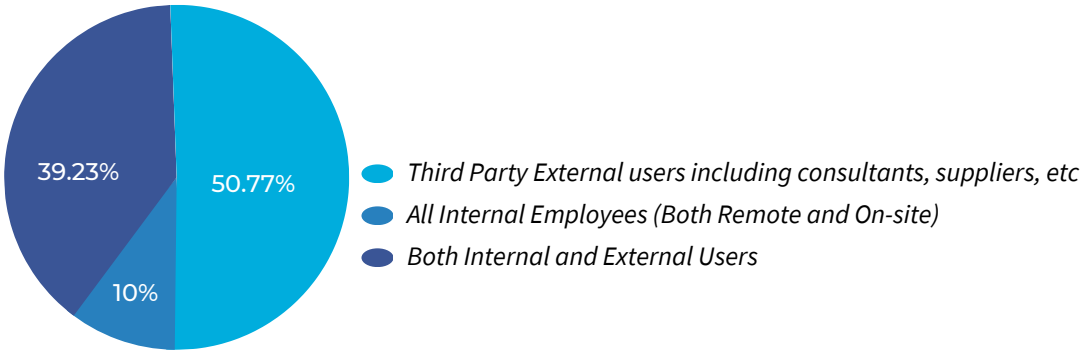


Figure 9: *Distribution of Type of users that organization has provisioned for Zero Trust Access*

TYPES OF APPLICATION AND SYSTEM ACCESS THAT ORGANIZATIONS ARE USING ZERO TRUST ACCESS TO SECURE

Around 74% of respondents use Zero Trust solution to securely access their Cloud services such as AWS, Azure, GCP. More than 50% of respondents use Zero Trust for Server access. Secure access to web applications is also one of the key uses of Zero Trust.

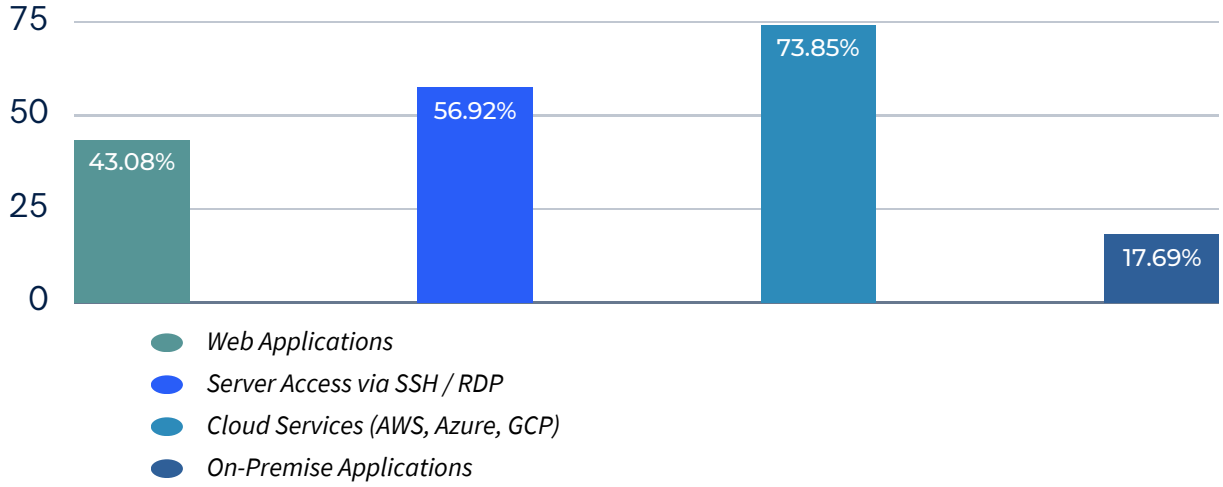


Figure 10: *Distribution of Type of applications and system access that organization is using Zero Trust Access to secure*

CONFIDENCE LEVEL ON ZERO TRUST SOLUTION THAT IT CAN REDUCE SECURITY INCIDENTS

More than 75% of respondents are quite confident of Zero Trust solution that it can significantly reduce security incidents. A meagre 8% respondents don't agree that it could reduce security incidents significantly. The reason may be all respondents are different phase of adoption of the technology. Also, once a solution is adopted, it takes couple of years data points to compare and realise the benefits of a security solution.

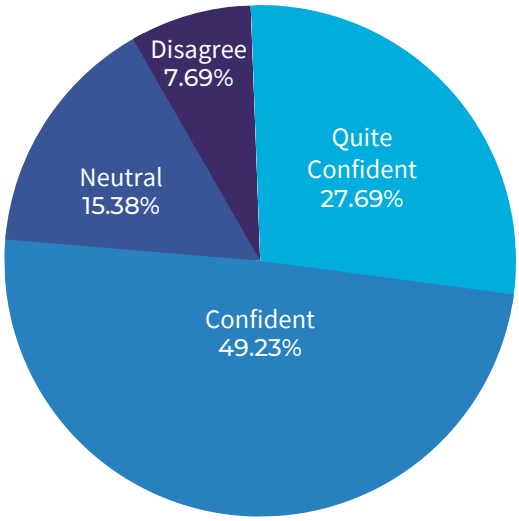
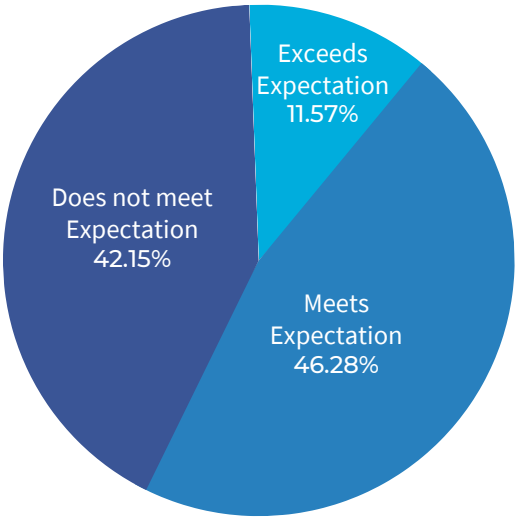


Figure 11: *Confidence Level on Zero Trust solution that it can reduce security incidents*

SATISFACTION LEVEL WITH ZERO TRUST SOLUTION

For organizations who have already implemented Zero Trust Solutions, 58% of respondents feel Zero Trust solution meets or exceeds their expectations. Around 42% of respondents expressed Zero Trust doesn't meet their expectations, however we couldn't capture their initial expectations when they went ahead with the implementation of the solution. It is essential to map initial expectations from the customers and address them suitably with the solution. Zero Trust has several use cases and needs to be addressed accordingly based on customer needs and expectations.



58% of respondents feel Zero Trust solution meets or exceeds their expectations. Around 42% of respondents expressed Zero Trust doesn't meet their expectations.

Figure 12: *Satisfaction Level with Zero Trust Solution*

USE OF VPN AND ZERO TRUST SOLUTIONS INSIDE THE ORGANIZATION

72% of respondents have expressed that their organization is using VPN and Zero Trust simultaneously. A lot of organizations are using VPN for internal users and Zero Trust for external users. Around 26% of respondents' organizations are using Zero Trust solution. Using multiple solutions can create possibility of vulnerability entry points which hackers can exploit. In order to strengthen security, it is advisable to adopt one solution.

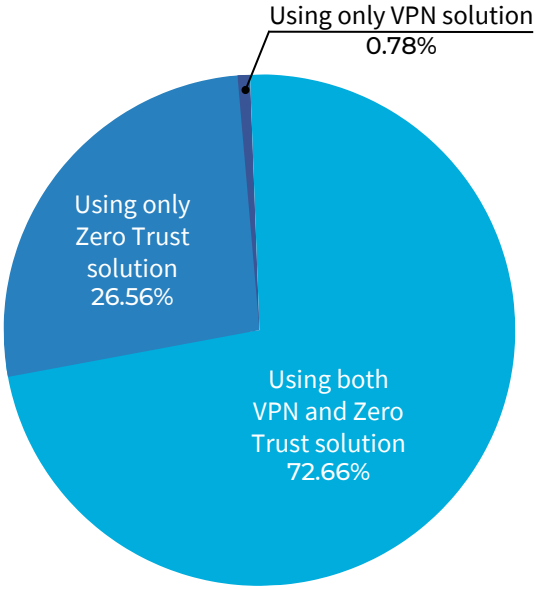


Figure 13: *Confidence Level on Zero Trust solution that it can reduce security incidents*

VENDOR EVALUATION CRITERIA FOR CHOOSING THE RIGHT ZERO TRUST SOLUTION

More than 50% of respondent's organizations rely on their own IT team research based on their requirement to select the right vendor. Around 27% of respondents use the security channel partner in evaluating their vendor. Around 10% of the respondents look for referrals and another 10% of the respondents rely on Analyst report to select top vendors from the category. This tells that organizations are doing their due diligence to select right vendors from this Zero Trust crowded market which has smaller players to big giants. Zero Trust market provides a level playing field to all players and right vendor with right solution has a great opportunity to capture the market.

More than 50% of respondent's organizations rely on their own IT team research based on their requirement to select the right vendor. Around 27% of respondents use the security channel partner in evaluating their vendor.

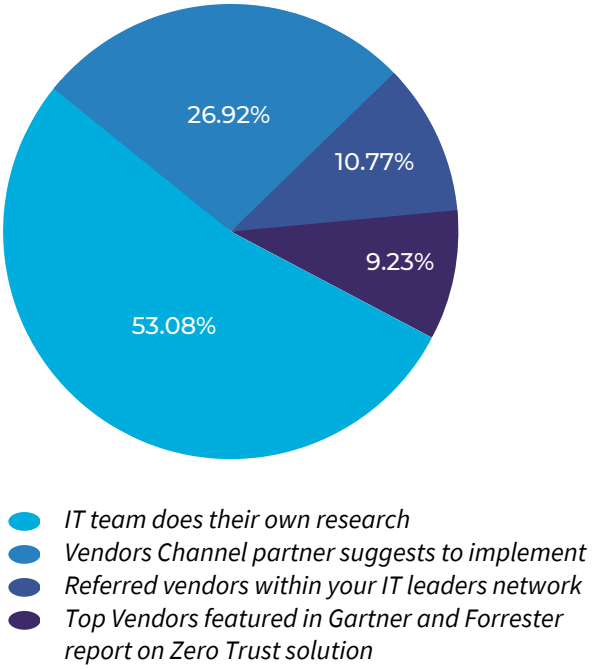


Figure 14: *Vendor Evaluation criteria for choosing the right Zero Trust solution*

SUMMARY

Zero Trust market is highly fragmented with many small, medium, and large players. There is a lot of scope for Zero Trust players to address customer pain points and their expectations. With a distributed workforce, cloud transformation, and the rise of cyber attacks, enterprises are looking for Zero Trust solutions with enhanced security and better user experience. In contrast to the Pre-Covid days, enterprises now very well understand the importance of Zero Trust security and the benefits it can offer to reduce security risks.

With the current pace of adoption, we expect in the next 3 to 5 years, every organization would have adopted a Zero Trust solution for a couple of use cases. Customer expectations from the solution will be more apparent and it will further increase customer satisfaction. Consolidation of the market segment will start happening in another 2 to 3 years.