

# SINGAPORE BASED \$1 BILLION TELCO MEASURES CYBER RISK POSTURE DURING DIGITAL TRANSFORMATION ACROSS HYBRID INFRASTRUCTURE WITH SAFE

## INDUSTRY

Tele Communications

## RESULTS

- Security Monitoring For Digital Assets
- Security Incorporated In Digital Transformation
- Asset Wise Security Score Based On Business Criticality
- Group Of Digital Transformation Stack For Security Posture Monitoring

## CHALLENGES

- No visibility into the security posture of assets on-cloud
- Quantified view of digital transformation stack on hybrid cloud

## THE NEED

The organization has an ambitious vision of transforming their legacy stack of application and underlying IT infrastructure to Hybrid Cloud. The digital transformation journey intends organization to increase people and operations productivity while ensuring customer data security. While organization has practice to perform routine security checks, enabling a central view that provides visibility into the entire migrated digital stack is one of the biggest challenge.

## ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, the organization used to perform regular security checks as a part of their security policy. However, this checks are periodic and doesn't provide visibility into continuous security posture.

## BRING RIGHT VISIBILITY WITH SAFE

SAFE, is an enterprise-class, unified, and real-time Cyber Risk Quantification (CRQ) platform that offers a comprehensive solution, by taking into account both technical and business aspects, to arrive at informed and prioritised decision making. SAFE has a unique assessment approach across five threat vectors concerning organisations, namely People, Policy, Technology, Cybersecurity Products, and Third-parties. SAFE helped the organization with the following unique capabilities:

1. Vulnerability management and prioritization with SAFE
2. Asset grouping as per business requirements
3. Score per asset, per group
4. Continuous assessment and monitoring of IT assets on-cloud and on-prem

1

## VULNERABILITY MANAGEMENT AND PRIORITIZATION WITH SAFE

While running a continuous vulnerability management program, org kept discovering a large number of vulnerabilities on a regular basis. However, in the absence of a common framework to

prioritize and monitor the remediation status these vulnerabilities, the overall program didn't enable in addressing the most business critical issues. It certainly gets difficult to prioritize between hundreds of high vulnerabilities to identify the few that may help an adversary execute a well-crafted attack. Finding a needle in the haystack! SAFE's enables the organization to implement a risk-based vulnerability management program by flagging the most critical vulnerabilities as TSAR. Originally, TSAR refers to the most powerful man-made nuclear weapon to ever be created. In the similar way, SAFE would identify the TSAR vulnerabilities in the cyberspace! SAFE categorises vulnerabilities as TSAR (or non-TSAR) based on the CVE IDs. TSAR vulnerabilities are a combination of vulnerabilities that are being exploited by threat actors (trending vulnerabilities) and remotely exploitable public vulnerabilities. While SAFE has integrations available with multiple VA tools, org built a process to onboard vulnerabilities identified from manual and automated scans it ran so that every time a scan runs, vulnerabilities are managed and prioritized by SAFE. As an output, SAFE provided the organization with a visibility to security posture of each IP Address and each Application on SAFE.

## 2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE can be deployed on-prem or cloud, and can be used as a single and the only platform in your organization to track your cybersecurity posture across all verticals. The organization used SAFE to gain 360 degree view with fully automated configuration assessment performed natively and vulnerability management performed through integrations across their IT stack. SAFE supports more than 80 technology solutions across 11 verticals ranging from endpoints, databases to cloud

services. SAFE further provides an execution plan to reach the desired SAFE score via actionable insights.

## 3 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments performed by SAFE and factoring the inputs received from integrations with other tools. These assets can be further clubbed into an asset group per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This way of risk quantification helps the organization in taking the right decision especially during the mission critical go-lives. The organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

## 4 CONTINUOUS ASSESSMENT AND MONITORING OF IT ASSETS ON-CLOUD AND ON-PREM

SAFE can be deployed on-prem or cloud, and can be used as a single and the only platform in your organization to track your cybersecurity posture across all verticals. The organization used SAFE to gain 360 degree view with fully automated configuration assessment performed natively and vulnerability management performed through integrations across their IT stack. SAFE supports more than 80 technology solutions across 11 verticals ranging from endpoints, databases to cloud services. SAFE further provides an execution plan to reach the desired SAFE score via actionable insights.

**SAFE** helps organizations measure and mitigate enterprise-wide cyber risk in real-time using it's AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

### USA (HQ)

Stanford Research Park  
3260 Hillview Avenue  
Palo Alto, CA 94304

### INDIA

Lucideus House  
Plot No 15, Okhla Phase III  
New Delhi, 110020

# SINGAPORE-BASED \$1B TELCO MEASURES CYBER RISK POSTURE while digitally transforming across their HYBRID INFRASTRUCTURE with SAFE

## INDUSTRY

Tele Communications

## RESULTS

- Security monitoring for digital assets
- Security incorporated in digital transformation
- Asset-wise security score based on business criticality
- Group of digital transformation stack for security posture monitoring

## CHALLENGES

- No visibility into the security posture of assets on-cloud
- Lack of a quantified view of digital transformation stack on hybrid cloud

## THE NEED

An ambitious vision: Transforming their legacy stack of applications & underlying IT infrastructure to Hybrid Cloud while ensuring customer data security. Enabling a central view which provides visibility into the entire migrated digital stack was their most pertinent requirement.

## ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, the organization performed regular security checks as a part of their security policy. However, these checks were periodic and failed to provide continuous visibility.

## BRING RIGHT VISIBILITY WITH SAFE

SAFE is an enterprise-class, unified, and real-time Digital Business Risk Quantification (CRQ) platform which offers a comprehensive solution by taking into account both technical and business aspects and gives informed, prioritised insights. With its unique assessment approach across five threat vectors concerning organisations - People, Policy, Technology, Cybersecurity Products, and Third-parties - SAFE helped this organization with the following:

1. Vulnerability management and prioritization
2. Asset grouping as per business requirements
3. Score per asset & per group
4. Continuous assessment and monitoring of IT assets on-cloud and on-prem

1

## VULNERABILITY MANAGEMENT AND PRIORITIZATION WITH SAFE

On their continuous vulnerability management program, the organization kept discovering a large number of vulnerabilities on a regular basis. However, in the absence of a common framework to prioritize and monitor the remediation status of these vulnerabilities, the overall program could not address the most business critical issues.

It certainly gets difficult to prioritize from hundreds of high-risk vulnerabilities and identify the few that may help an adversary execute a well-crafted attack. It is akin to finding a needle in the haystack!

TSAR is the most powerful man-made nuclear weapon to ever be created. SAFE identifies the TSAR vulnerabilities in cyberspace! It categorises vulnerabilities as TSAR (or non-TSAR) based on their CVE IDs. The TSAR vulnerabilities are a combination of vulnerabilities that are being exploited by threat actors (trending vulnerabilities) and remotely exploitable public vulnerabilities. While SAFE has integrations available with multiple VA tools, this organization automated the process of on-boarding vulnerabilities so that each scan, vulnerabilities were managed and prioritized by SAFE. As an output, SAFE provided the organization with a visibility into the security posture of each IP Address and each Application on SAFE.

## 2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE provides this organization with a consolidated view of SAFE score across departments through a single widget. Any new business unit can be on-boarded easily and be continuously monitored. Each Business Unit has been assigned a priority score and according to the delta change in its value, SAFE sends actionable alerts to the asset group owner and/ or concerned authorities in form of an email or system generated telephonic call.

## 3 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments it has performed and by factoring the inputs received from integrations with other tools. These assets can be further clubbed into an asset group per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This means of business risk quantification helps the organization in taking the correct decision, especially during the mission critical go-lives. This organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

## 4 CONTINUOUS ASSESSMENT AND MONITORING OF IT ASSETS ON-CLOUD AND ON-PREM

SAFE can be deployed on-prem or cloud, and can be used as a single and the only platform in your organization to track your cybersecurity posture across all verticals. The organization used SAFE to gain 360 degree view with fully automated configuration assessment performed natively and vulnerability management performed through integrations across their IT stack. SAFE supports more than 80 technology solutions across 11 verticals ranging from endpoints, databases to cloud services. SAFE further provides an execution plan to reach the desired SAFE score via actionable insights.

**SAFE** helps organizations measure and mitigate enterprise-wide cyber risk in real-time using its AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

### USA (HQ)

Stanford Research Park  
3260 Hillview Avenue  
Palo Alto, CA 94304

### INDIA

Lucideus House  
Plot No 15, Okhla Phase III  
New Delhi, 110020