INDIA'S FASTEST GROWING $1 BILLION FMCG ENSURES GO-LIVE OF PRODUCTION ASSETS COMPLYING TO BASELINE SECURITY POLICIES WITH SAFE

INDUSTRY

Fast-moving Consumer Goods

RESULTS

- Visibility into technology stack across the organization
- Compliance maintenance with hardening guidelines
- Visibility into newly onboarded asset's security posture
- Visibility into overall security posture

CHALLENGES

- No visibility into the security posture of assets on-cloud for CXOs
- Overall compliance percentage to its own hardening guidelines
- Manual, Human-Intensive exercise
- Ability to deliver business requirement fast with baseline security requirements

THE NEED

The organization keeps onboarding and offboarding assets across the technology vertical. The objective is to ensure the implementation of the security guidelines for all the newly onboarded asset before it goes to the production. The implementation of go-live checklist has been getting exhaustive with the time, and it became difficult for people to drive it manually because its time sensitivity. Measuring and maitaining the security posture of the assets after go-live happens periodically to identify if there is any securiy gaps. It doesn't bring the visibility into the actual security posture and the risk that an organization is exposed to

ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, the organization would perform manual assessment check-list based to identify if the asset meets go-live criteria. Such time-intensive activity has not been allowing them to cater to immediate business requirements as well as ensure the compliance to its own guidelines. Moreover, once an asset is in production, there was no way to identify the security posture of an asset and maintain the constantly changing security requirements

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. Asset grouping as per business requirements
2. Score per asset, per group
3. Monitoring newly added assets in each SAFE Vertical to ensure compliance to security guidelines
4. All the new devices to be onboarded on SAFE before go-live

with minimum SAFE score of 3+

5. Actionable insights to identify most critical vulnerabilities to prioritize patching

1 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

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

2 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 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.

3 MONITORING NEWLY ADDED ASSETS IN EACH SAFE VERTICAL TO ENSURE COMPLIANCE TO SECURITY GUIDELINES

The organization keeps onboarding and offboarding assets to accommodate the business requirements. While onboarding all the new assets, the business objective is to ensure that all the assets comply to the security guidelines defined. With SAFE, an organization can easily identify all the assets that were onboarded between 2 specific dates to visualize compliance.

4 ALL THE NEW DEVICES TO BE ONBOARDED ON SAFE BEFORE GO-LIVE WITH MINIMUM SAFE SCORE OF 3+

The organization uses SAFE to check the security posture of all the new devices before going live. They continuously monitor that the SAFE score of the device be 3+ for it to be secure enough and to be alerted in case ofr score change.

5 ACTIONABLE INSIGHTS TO IDENTIFY MOST CRITICAL VULNERABILITIES TO PRIORITIZE PATCHING

SAFE provides a prioritization matrix, which allows users to get visibility into the high-risk vulnerabilities in their landscape to fix or de-prioritize the gaps. SAFE also takes the Vulnerability based Risk management approach by giving insights on TSAR Vulnerabilities wich are high-risk vulnerabilities that may have a publicly available exploit or determined as such by subject matter experts at Lucideus.

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

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

INDIA'S FASTEST GROWING $1 BILLION FMCG ENSURES GO-LIVE OF PRODUCTION ASSETS COMPLYING TO BASELINE SECURITY POLICIES WITH SAFE

INDUSTRY

Fast-Moving Consumer Goods

RESULTS

- Visibility into technology stack across the organization
- Compliance maintenance with hardening guidelines
- Visibility into newly onboarded asset's security posture
- Visibility into overall security posture

CHALLENGES

- No visibility into the security posture of assets on-cloud for CXOs
- Overall compliance percentage to its own hardening guidelines
- Manual, Human-Intensive exercise
- Ability to deliver business requirement fast with baseline security requirements

THE NEED

The organization regularly on-boards and off-boards assets across the technology vertical. The objective is to ensure the implementation of the security guidelines for newly on-boarded assets before they go into production. With time, this organization's go-live checklist became lengthy and difficult to drive manually. It also became a time-consuming activity. Periodic measurement and maintenance of the assets' security posture after their go-live did not bring visibility into the actual security posture and the risk that the organization was exposed to.

ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, the organization would perform manual checklist-based assessments to identify if the assets met go-live criteria. Such time-intensive activity neither gave them flexibility to cater to immediate business requirements nor ensured the compliance to their own guidelines. Moreover, once an asset was in production, there was no way of identifying its security posture to maintain their constantly changing security requirements.

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. Asset grouping as per business requirements
2. Score per asset, per group
3. Monitoring newly added assets in each SAFE Vertical to ensure compliance to security guidelines
4. All the new devices to be onboarded on SAFE before go-live

with minimum SAFE score of 3+

5. Actionable insights to identify most critical vulnerabilities to prioritize patching

1 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.

2 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.

3 MONITORING NEWLY ADDED ASSETS IN EACH SAFE VERTICAL TO ENSURE COMPLIANCE TO SECURITY GUIDELINES

The organization keeps onboarding and offboarding assets to accommodate the business requirements. While onboarding all the new assets, the business objective is to ensure that all the assets comply to the security guidelines defined. With SAFE, this organization can easily identify all the assets that were onboarded between 2 specific dates to visualize compliance.

4 ALL THE NEW DEVICES TO BE ONBOARDED ON SAFE BEFORE GO-LIVE WITH MINIMUM SAFE SCORE OF 3+

The organization uses SAFE to check the security posture of all the new devices before going live. They continuously monitor that the SAFE score of the device be 3+ for it to be secure enough and to be alerted in case of a change in score.

5 ACTIONABLE INSIGHTS TO IDENTIFY MOST CRITICAL VULNERABILITIES TO PRIORITIZE PATCHING

SAFE provides a prioritization matrix, which allows users to get visibility into the high-risk vulnerabilities in their landscape to fix or de-prioritize the gaps. SAFE also takes the Vulnerability-based Risk management approach by giving insights on high-risk TSAR Vulnerabilities that may have a publicly available exploit or determined as such by subject matter experts at Lucideus.