SECONIZE

ISO 27001:2013 IAS BQSR CERTIFIED

De-Risking Cyber

Cyber risk and compliance management

Supported by:

CySecK Cyber Security Karnataka

CyRise

Hewlett Packard Enterprise

CYBER SECURITY GRAND CHALLENGE INNOVATE TO SECURE

INCUBATED BY 10000 START-UPS

Microsoft

Microsoft for Startups

DSCI PROMOTING DATA PROTECTION

De-Risking the Cyber Space

1. CISOs must go thorough their compliance with cybersecurity frameworks

2. Companies need to re-align frameworks with business strategies and risk profiles

3. Adaptation to robust cybersecurity is needed to enable business growth

Traditional Risk Management

- ☑ Checkbox Drive
- Point in Time
- Technical
- Arcane

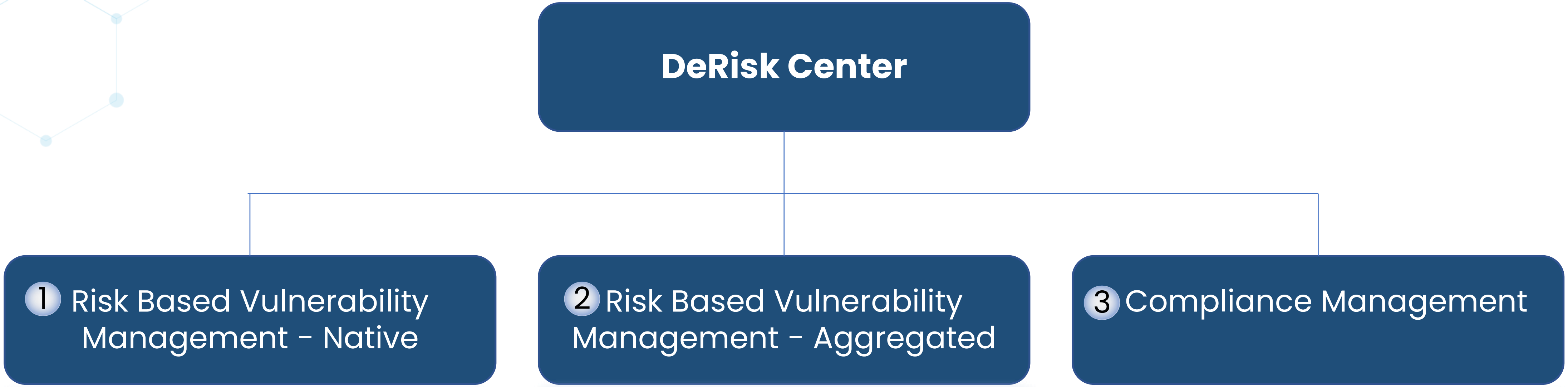
Seconize – DeRisk Center Cloud Oriented | Automated | Holistic | ***Continuous*** | ***Contextual***

- Impact Based
- Near Real Time
- Unified
- Automated

IT Risk Management with data driven approach

- Evaluating business risks from IT infra & applications
- To achieve manageable risk level by prioritizing remediation

Primary Use Cases



DeRisk Center

1 Risk Based Vulnerability Management - Native

2 Risk Based Vulnerability Management - Aggregated

3 Compliance Management

Automated VA + PT
Cloud: AWS, Azure, GCP
Workloads: VM (Linux, Windows), Kubernetes
Applications: Website, WebApp, Mobile App
Network Devices: Firewalls, Routers

Target customer profile:
Interested in scanning (VA+PT) and risk modelling

- Integrate with Third Party scanners
- Aggregate, Normalize and De-Duplicate the Data
- Risk modeling and prioritization
- Remediation Tracking

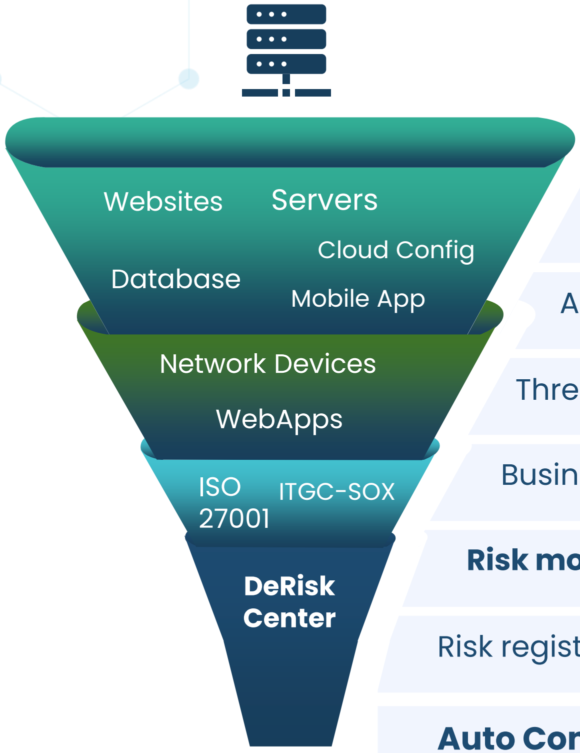
Target customer profile:
Invested in scanners, want to consolidate

- Automated compliance gap assessment
- Evidence Gathering
- Support for International ITGC SOX and Regional compliances RBI SEBI IRDAI

Target customer profile:
Want to automate compliance internal audit

De-Risk Center – Risk Mgmt

Our assessments are based on industry-wide standards like SANS Top 25, OWASP Top 10, CIS, OWASP MSTG, Open SCAP, CSM, CCM

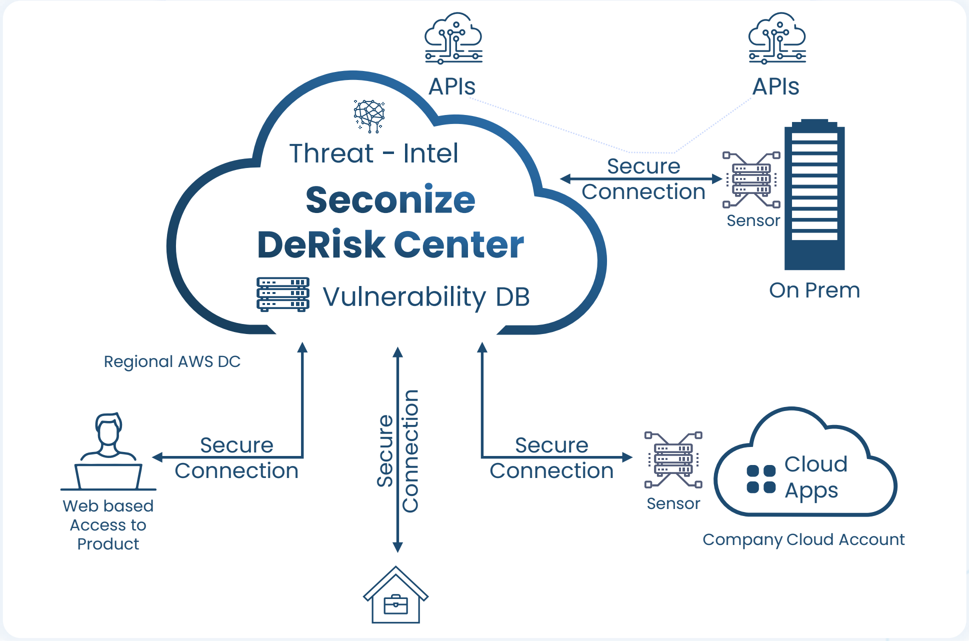


De-Risk flow:

- Assets: Discovery
- Access inside-out view: Scan by type
- Threat Intel outside-in view: Leaked & active Info
- Business context : **Contextual** assessment
- **Risk modeling** : Elements of risk
- Risk register : **Prioritization** & **auto -remediation**
- **Auto Compliance** : Gap Assessments

Security Assessment, Prioritized Risk View Compliance gap assessment;

Across On-Prem, Cloud, Home



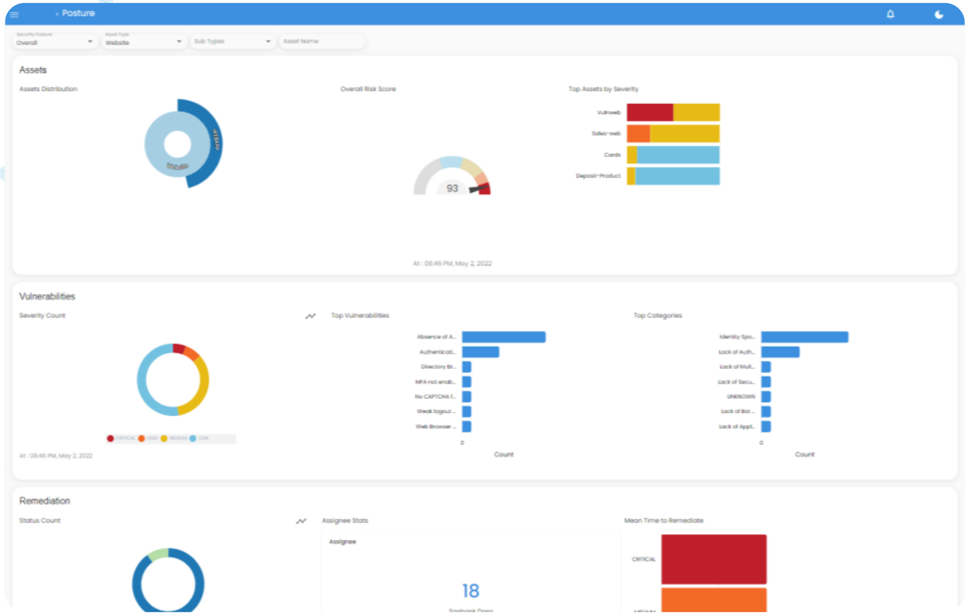
Top use cases

- Security Assessment cloud, infra and applications. Identify the issues and the associated risks.
- Unifying the VA results from multiple sources to give a unified view to the CISO to better manage the cyber risks
- Automating the compliances
  - Integrating with the multiple systems to gather the evidence and mapping to the controls
  - Reducing the time taken for an audit from months to days

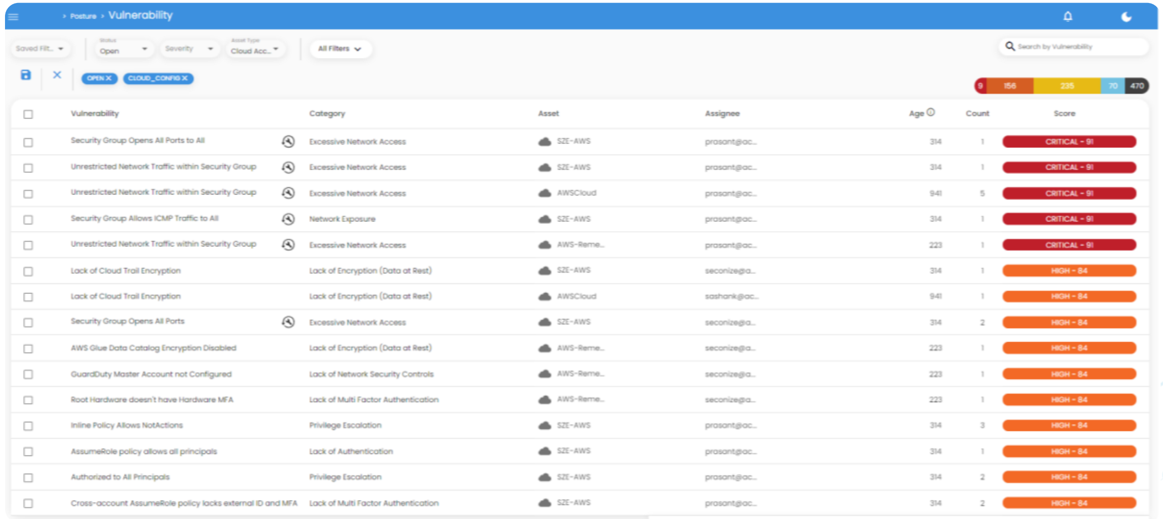
Salient Points: Deployed in customer region, Security and privacy, Best practices, Hybrid deployment, Cloud Management, Sensors on premises

Product Visualisation

Risk Dashboards

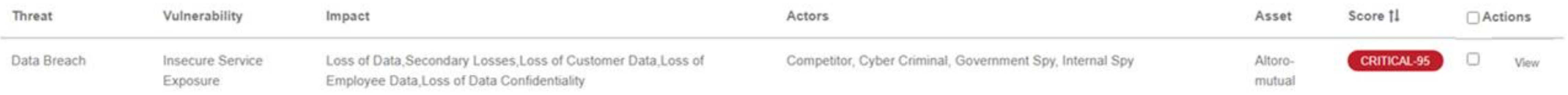


Automated Risk Register



□	Vulnerability	Category	Asset	Assignee	Age	Count	Score
□	Security Group Opens All Ports to All	Excessive Network Access	SZE-AWS	prasant@ac...	314	1	CRITICAL - 91
□	Unrestricted Network Traffic within Security Group	Excessive Network Access	SZE-AWS	prasant@ac...	314	1	CRITICAL - 91
□	Unrestricted Network Traffic within Security Group	Excessive Network Access	AWSCloud	prasant@ac...	941	5	CRITICAL - 91
□	Security Group Allows ICMP Traffic to All	Network Exposure	SZE-AWS	prasant@ac...	314	1	CRITICAL - 91
□	Unrestricted Network Traffic within Security Group	Excessive Network Access	AWS-Reme...	prasant@ac...	223	1	CRITICAL - 91
□	Lack of Cloud Trail Encryption	Lack of Encryption (Data at Rest)	SZE-AWS	seconize@a...	314	1	HIGH - 84
□	Lack of Cloud Trail Encryption	Lack of Encryption (Data at Rest)	AWSCloud	sashank@ac...	941	1	HIGH - 84
□	Security Group Opens All Ports	Excessive Network Access	SZE-AWS	seconize@a...	314	2	HIGH - 84
□	AWS Glue Data Catalog Encryption Disabled	Lack of Encryption (Data at Rest)	AWS-Reme...	seconize@a...	223	1	HIGH - 84
□	GuardDuty Master Account not Configured	Lack of Network Security Controls	AWS-Reme...	seconize@a...	223	1	HIGH - 84
□	Root Hardware doesn't have Hardware MFA	Lack of Multi Factor Authentication	AWS-Reme...	seconize@a...	223	1	HIGH - 84
□	Inline Policy Allows NotActions	Privilege Escalation	SZE-AWS	prasant@ac...	314	3	HIGH - 84
□	AssumeRole policy allows all principals	Lack of Authentication	SZE-AWS	prasant@ac...	314	1	HIGH - 84
□	Authorized to All Principals	Privilege Escalation	SZE-AWS	prasant@ac...	314	2	HIGH - 84
□	Cross-account AssumeRole policy lacks external ID and MFA	Lack of Multi Factor Authentication	SZE-AWS	prasant@ac...	314	2	HIGH - 84

Risk Object



Threat	Vulnerability	Impact	Actors	Asset	Score ⇅	□ Actions	
Data Breach	Insecure Service Exposure	Loss of Data,Secondary Losses,Loss of Customer Data,Loss of Employee Data,Loss of Data Confidentiality	Competitor, Cyber Criminal, Government Spy, Internal Spy	Altoro-mutual	CRITICAL-95	□	View

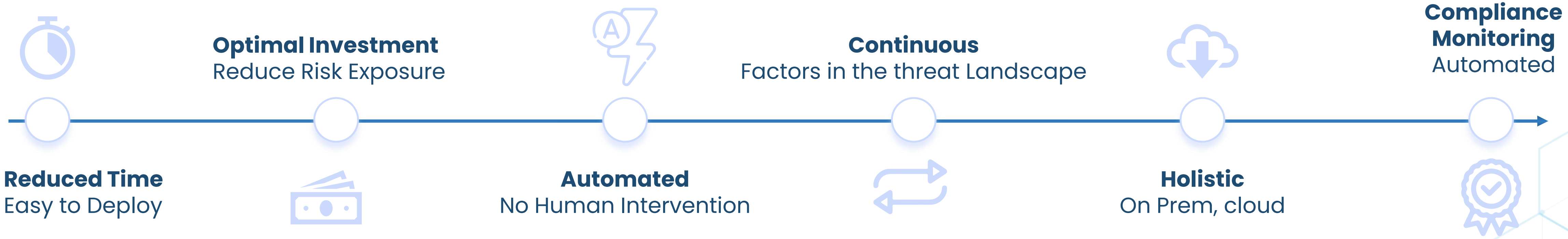
Advantages of DeRisk Center

First report within days

Protect existing investments

80% fewer breaches

40% effort reduction



Reduced Time
Easy to Deploy

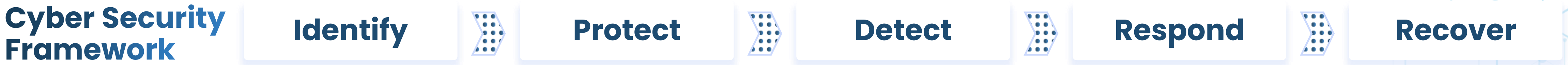
Optimal Investment
Reduce Risk Exposure

Automated
No Human Intervention

Continuous
Factors in the threat Landscape

Holistic
On Prem, cloud

Compliance Monitoring
Automated



Cyber Security Framework

Identify → Protect → Detect → Respond → Recover

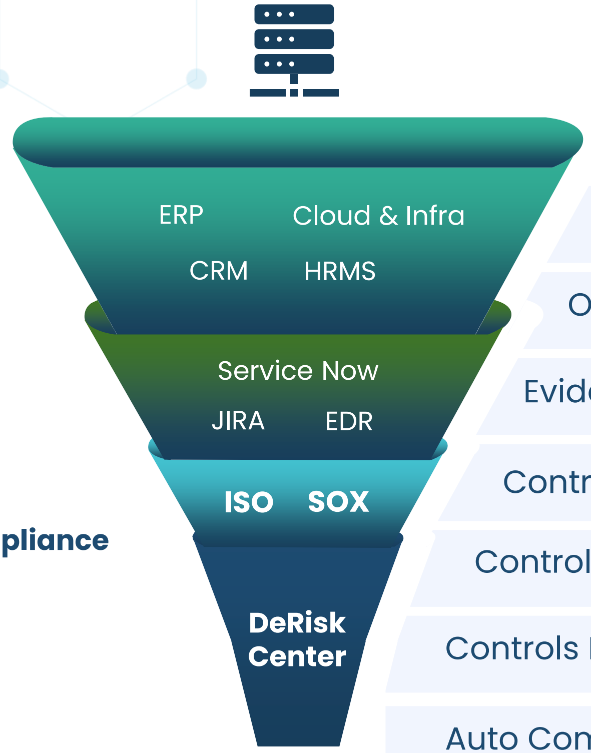
- ○ Identify early and often
- ○ Mitigate top risks – optimize spend

- ○ RoI justified
- ○ Automate compliance - Effort reduction

- ○ Virtual CISO

Seconize DeRisk Center – Compliance Mgmt

Assessments are based on industry-wide standards like
ISO 27001-2013, SOX, NIST CSF , PCI DSS , CCM

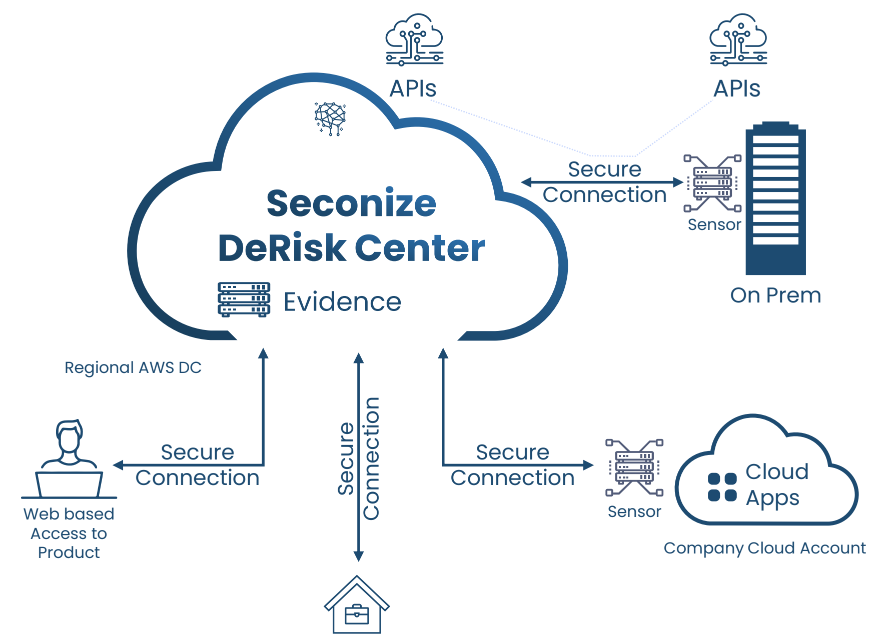


Auto Compliance

De-Risk flow:

- Onboarding Business Applications
- Onboarding of IT Solutions
- Evidence Collection through APIs
- Controls to Evidence Mapping
- Control Gap Assessment
- Controls Monitoring & Risk Assessments
- Auto Compliance : ISO, **SOX**

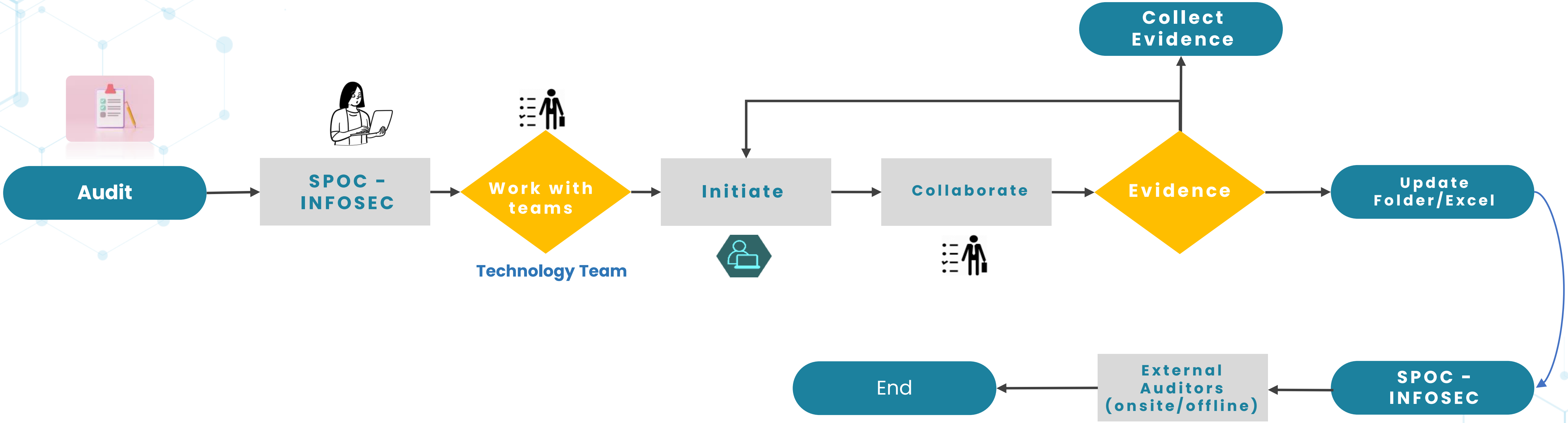
Serving Across On-Prem, Cloud,



Compliance gap assessment; Automated technology gaps; Workflows for manual inputs; Internal audit report

Salient Points: Deployed in customer region, Security and privacy best practices, Hybrid deployment, Cloud Management, Sensors on premises

Before



Audit

SPOC - INFOSEC

Work with teams

Technology Team

Initiate

Collaborate

Evidence

Collect Evidence

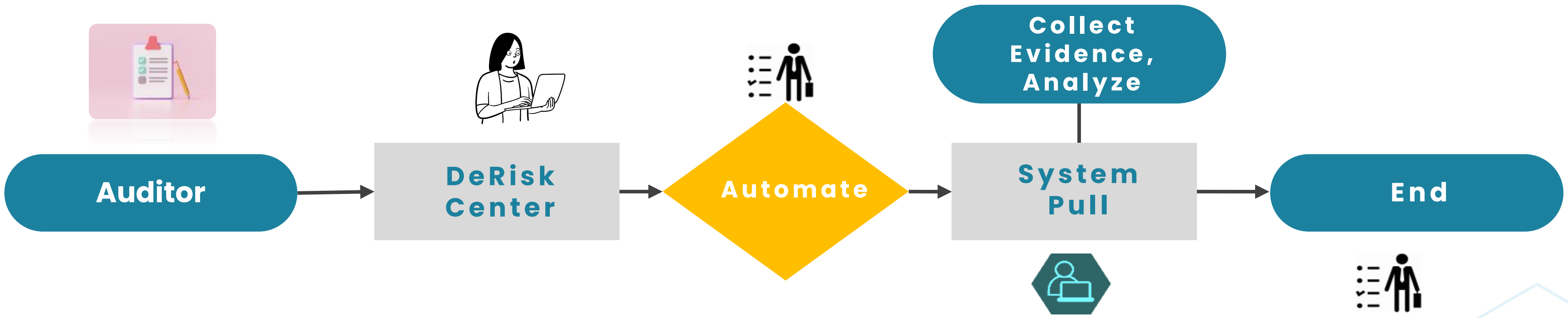
Update Folder/Excel

SPOC - INFOSEC

External Auditors (onsite/offline)

End

After



Auditor

DeRisk Center

Automate

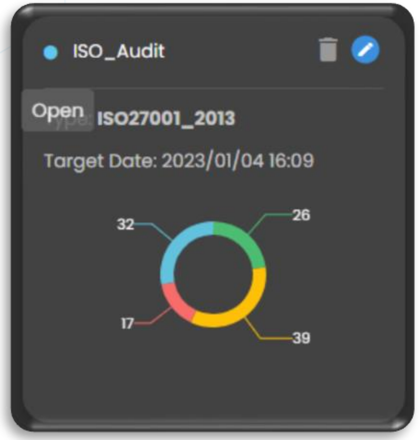
System Pull

Collect Evidence, Analyze

End

Product Visualization – Compliance Mgmt

Compliance Dashboard

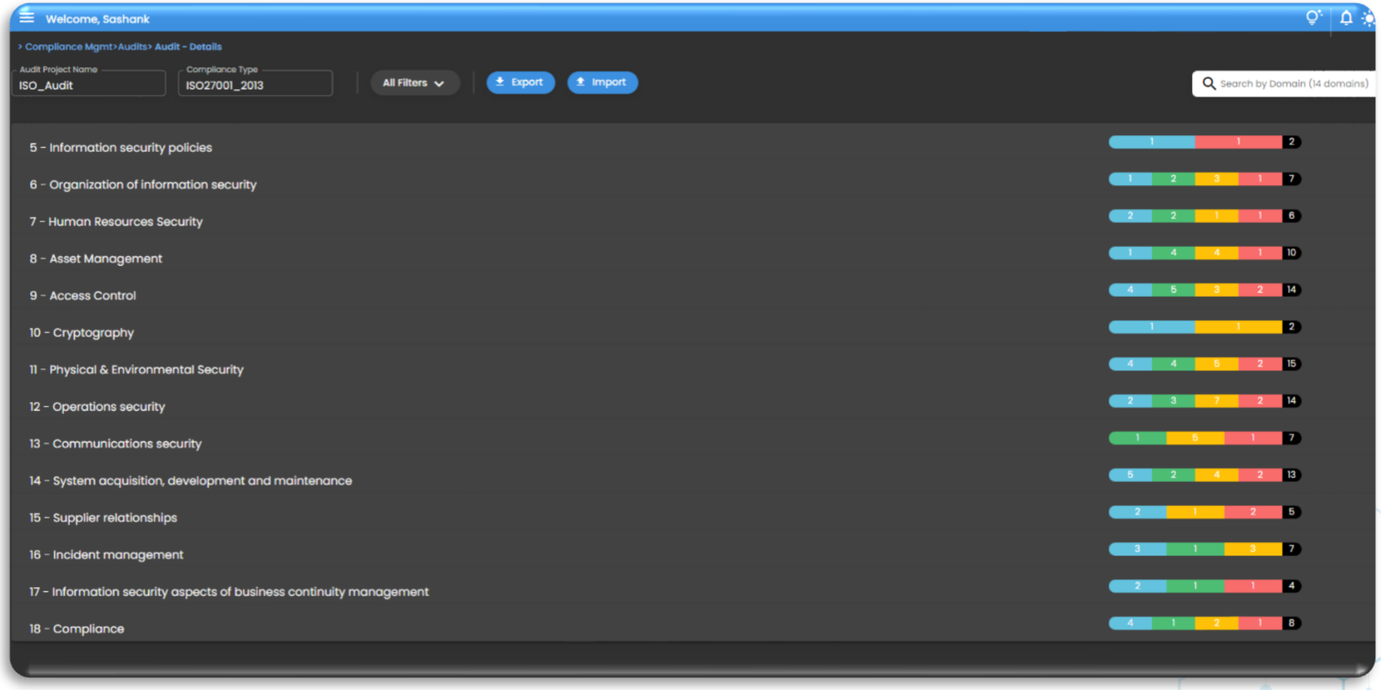


ISO_Audit

Open ISO27001_2013

Target Date: 2023/01/04 16:09

Compliance Details



Welcome, Sashank

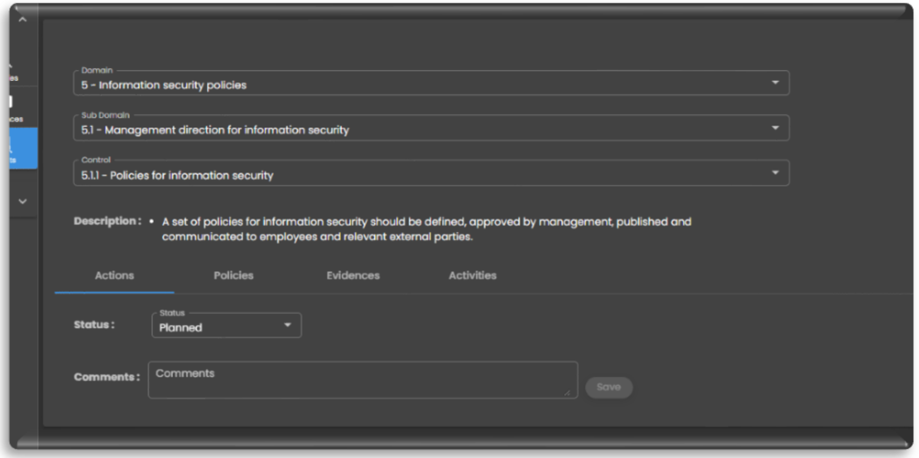
› Compliance Mgmt›Audits› Audit - Details

Audit Project Name: ISO_Audit

Compliance Type: ISO27001_2013

5 - Information security policies	🟦 1 🟥 1	2
6 - Organization of information security	🟦 1 🟩 2 🟨 3 🟥 1	7
7 - Human Resources Security	🟦 2 🟩 2 🟨 1 🟥 1	6
8 - Asset Management	🟦 1 🟩 4 🟨 4 🟥 1	10
9 - Access Control	🟦 4 🟩 5 🟨 3 🟥 2	14
10 - Cryptography	🟦 1 🟨 1	2
11 - Physical & Environmental Security	🟦 4 🟩 4 🟨 5 🟥 2	15
12 - Operations security	🟦 2 🟩 3 🟨 7 🟥 2	14
13 - Communications security	🟩 1 🟨 5 🟥 1	7
14 - System acquisition, development and maintenance	🟦 5 🟩 2 🟨 4 🟥 2	13
15 - Supplier relationships	🟦 2 🟨 1 🟥 2	5
16 - Incident management	🟦 3 🟩 1 🟨 3	7
17 - Information security aspects of business continuity management	🟦 2 🟩 1 🟥 1	4
18 - Compliance	🟦 4 🟩 1 🟨 2 🟥 1	8

Control Details



Domain: 5 - Information security policies

Sub Domain: 5.1 - Management direction for information security

Control: 5.1.1 - Policies for information security

Description : • A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Status : Planned

Comments : Comments

De-risk Center Covers All Your Security Needs

Vulnerability Assessment

- ✓ Cloud config
- ✓ Cloud workloads
- ✓ Database
- ✓ Network devices

Application Assessment

- ✓ Website
- ✓ Webapp
- ✓ Mobile App
- ✓ Vulnerability Assessment
- ✓ Penetration testing

Risk Management

- ✓ Risk model
- ✓ Contextual risk scoring
- ✓ Threat Intel
- ✓ Prioritized risk register
- ✓ Fix recommendations
- ✓ Advisories
- ✓ Auto-Remediation

Compliance Monitoring

- ✓ APIs Integration
- ✓ Automated Controls Assessment
- ✓ Automated Mapping
- ✓ Simplified Workflows
- ✓ Evidence Management

Annual Continuous Monitoring

- ✓ API Integration with IT Solutions
- ✓ Initial Onboarding & hand-holding
- ✓ Ongoing product support, Ongoing product enhancements
- ✓ 2 hrs consultancy each month

Specific to Compliance Management

Get Started with a Trial Account

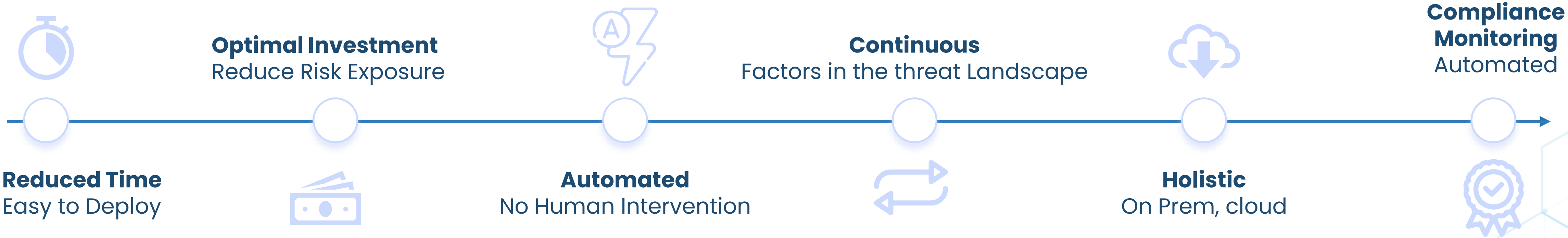
Advantages of De-Risking

First report within days

Protect existing investments

80% fewer breaches

40% effort reduction



Optimal Investment
Reduce Risk Exposure

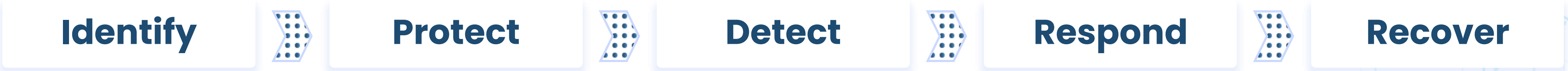
Continuous
Factors in the threat Landscape

Compliance Monitoring
Automated

Reduced Time
Easy to Deploy

Automated
No Human Intervention

Holistic
On Prem, cloud



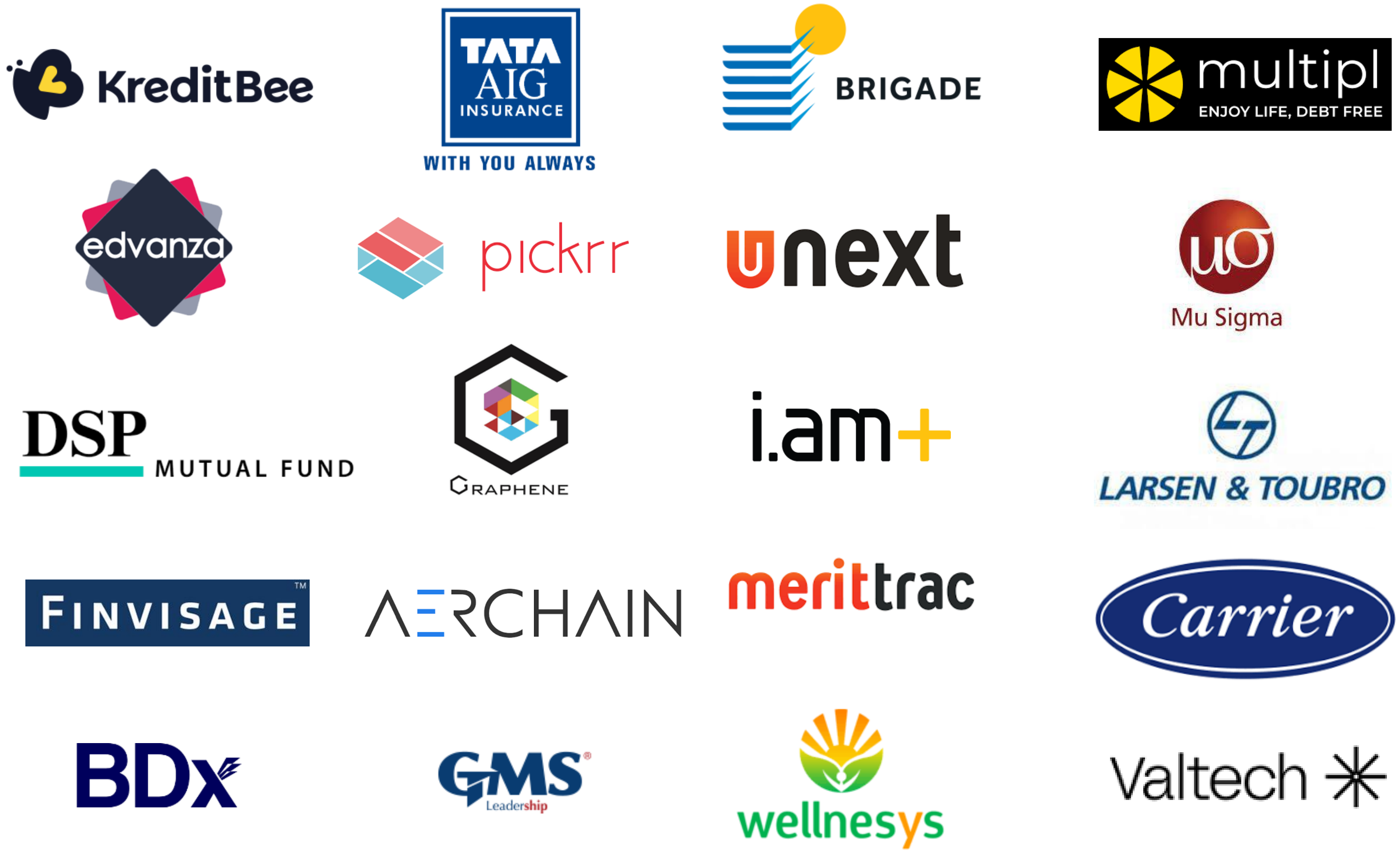
Cyber Security Framework

- ○ Identify early and often
- ○ Mitigate top risks – optimize spend

- ○ RoI justified
- ○ Automate compliance - Effort reduction

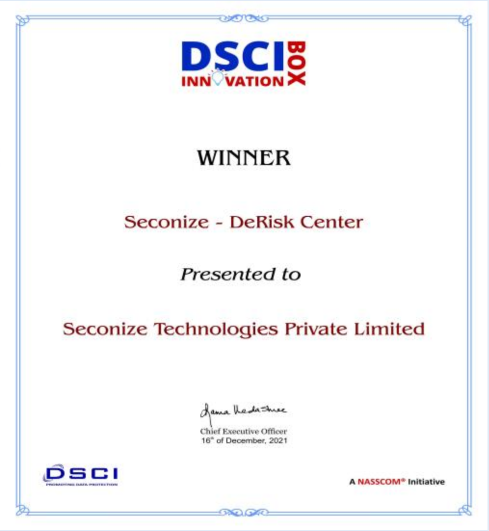
- ○ Virtual CISO

Customers


KreditBee
TATA AIG INSURANCE
WITH YOU ALWAYS
BRIGADE
multipl
ENJOY LIFE, DEBT FREE
edvanza
pickrr
unext
Mu Sigma
DSP MUTUAL FUND
GRAPHENE
i.am+
LARSEN & TOUBRO
FINVISAGE
AERCHAIN
merittrac
Carrier
BDx
GMS Leadership
wellnesys
Valtech

Recognition

DSCI – India
Cybersecurity Product
Of the year 2021



DSCI INNOVATION BOX

WINNER

Seconize - DeRisk Center

Presented to

Seconize Technologies Private Limited

Chief Executive Officer
16th of December, 2021

DSCI

A NASSCOM® Initiative

DSCI
SECONIZE
Supervisory Technologies
[SupervisoryTech]
For
Government
(Central, State, Cyber Authorities)
Regulators
(Sectoral)
Compliance Automation
Malware, TI, & Sandbox
Honeypot
Identity, Authentication, & Verification
SIEM and SOC Technologies
Fraud Management
Risk Quantification
Attack Surface Management
Observability & Synthetic Monitoring

DSCI Product Companies

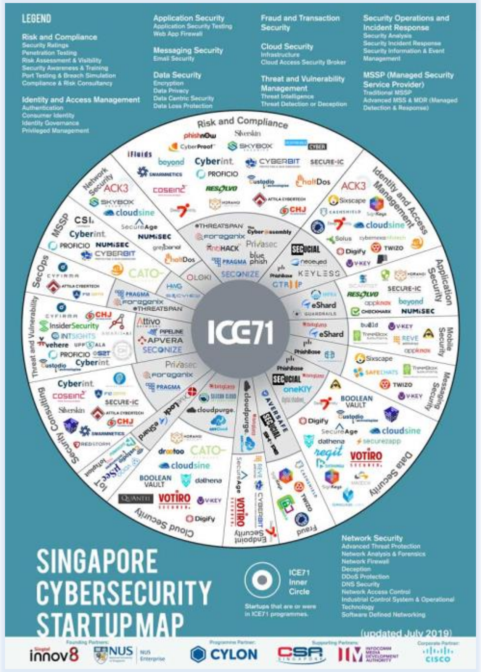
Globe – 100 Startups to look out for in 2021

MVP Stage – Winner

Emerge 50 – Top 50 Deep Tech startups

Top 5 Startups to watch out for in 2020

How Indian Cyber Security Startups Are Growing - List Of Startups You Can Look Out For In 2020



Singapore – Cybersecurity map
Top 5 cybersecurity

iDEX Defence Award Winner, 2023

Thank You

SECONIZE

De-Risking
Cyber

hello@seconize.co

+91-9845054920

in https://www.linkedin.com/company/seconize/

@seconize_co

www.seconize.co

Case Study – Cloud Infra and App security for a growing Startup

Customer Profile

Customer is a large startup with HQ in Bangalore. Customer has dynamic IT environment with employees, partners, vendors connecting to corporate network.

Customer Situation

- ➢ Has 16+ AWS Cloud accounts
- ➢ B2C, so has Web and mobile applications used by millions of users
- ➢ Finds it challenging to manage security across the cloud and applications

Seconize Solution

- ➢ Seconize DeRisk center is a comprehensive risk assessment product that leverages analytics, business context, and automation to proactively identify risks, ahead of a security breach.
- ➢ The core value proposition of Seconize DeRisk Centre (DRC) is in identifying the different vulnerabilities in the Cloud infrastructure and applications, translating them into potential risks based on the Organization's context.
- ➢ Provides remediations, auto-remediation and validates the fixes to derisk the organization
- ➢ Simple and intuitive workflows identify and manage the risks and vulnerabilities
- ➢ Comprehensive and exhaustive dashboards for efficient operation

Cloud / Business – Benefits & Key Outcomes

- ➢ Reduced cyber risks from supply chain
- ➢ Improved productivity by streamlining the risk assessments of vendors

Top Risks

- Loss of reputation
- Regulations
- Confidential Customer data

IT Infrastructure

- Cloud First
- Multi Cloud
- Web and Mobile Apps

Key Outcomes

- Cloud security posture management
- Application assessment
- Quick remediation

Case Study – Compliance Automation for SEBI regulated firm

Customer Profile

Customer is a large Mutual Fund house HQ in Mumbai. Regulated by SEBI, they have to report on a regular basis and are externally audited by several agencies.

Customer Situation

- Need to comply to SEBI system and SEBI Cyber
- Reporting happens on a quarterly basis
- Finds it challenging to audit across many technologies and teams. Usually takes months of effort.

Seconize Solution

- Seconize DeRisk center is a comprehensive compliance management product that automatically collects evidence and maps to the specific controls, essentially internal audit automation.
- Multiple compliances like ISO27001:2013 can be mapped too, leading to enormous time saving for the organization.
- It's a complete data driven compliance management.
- Simple and intuitive workflows to manage the compliance
- Auditor login and views supported
- The confidentiality of the data is maintained by not letting users download data.

Benefits & Key Outcomes

- Reduced time taken drastically from months to days
- Improved efficacy as it is completely data driven and not only sample evidence collection

Top Risks

- Non compliance
- Regulations
- Confidential data

IT Infrastructure

- Multiple IT systems
- Multi Teams
- Audited by 3 top firms

Key Outcomes

- Compliance mgmt. automated
- Do 9 audits per year, with little effort from internal audit team