TRUSTELEMENTS

Dynamic Cyber Risk Management

Our Clients

"TrustElements helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. Over 3,500 users continued to collaborate and run critical business functions seamlessly during the process."
Robert Florescu, CISO, CityMD

"Switching to TrustElements has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity."
Bruce Lucarelli, CTO, DermOne

"TrustElements has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency"
Alexey Gololobov, CFO, Columbus Hospital LTACH

"TrustElements has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security."
Kevin Hannigan, President, ACC Inc.

ACC Automated Control Concepts INC. Smart solutions.

CITYMD URGENT CARE

WORLD INSURANCE

ETS®

COLUMBUS HOSPITAL LTACH NEW WORLD MEDICINE℠

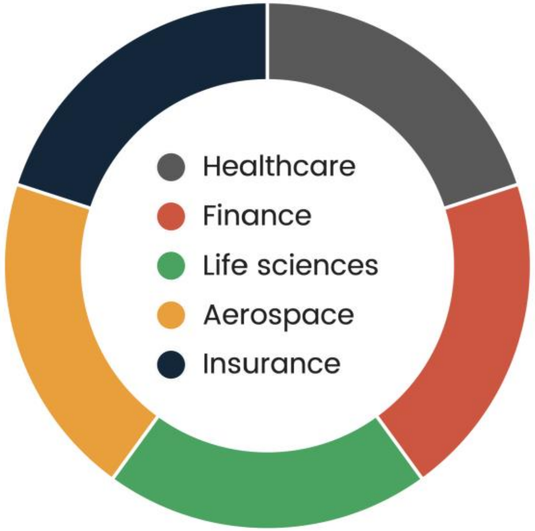
SENTRY management.

In-Phase Technologies, Inc.

OCEANFIRST BANK

Summit Health

PRISM Vision Group®



Problem Statement

- **Breaches are reaching an all-time high**
  - The frequency and sophistication of cyber attacks have increased exponentially in recent years.
- **Companies spend $200B/year for cyber**
  - **Cyber Security Breaches are inevitable**
  - Cybersecurity breaches disrupt business operations, damage company's reputation and erode customer confidence.
- **SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets**

Business executives need to be actively involved in understanding and managing cybersecurity risks to safeguard the organization's interests.

We’re empowering cybersecurity teams to make the right choices in the age of cyber risk uncertainty

TrustElements Features

Proactively handle cybersecurity risks in real-time.

Continuously Audit and Comply with Regulatory Requirements

Invest into your Cybersecurity based on Quantified Dollar Risk

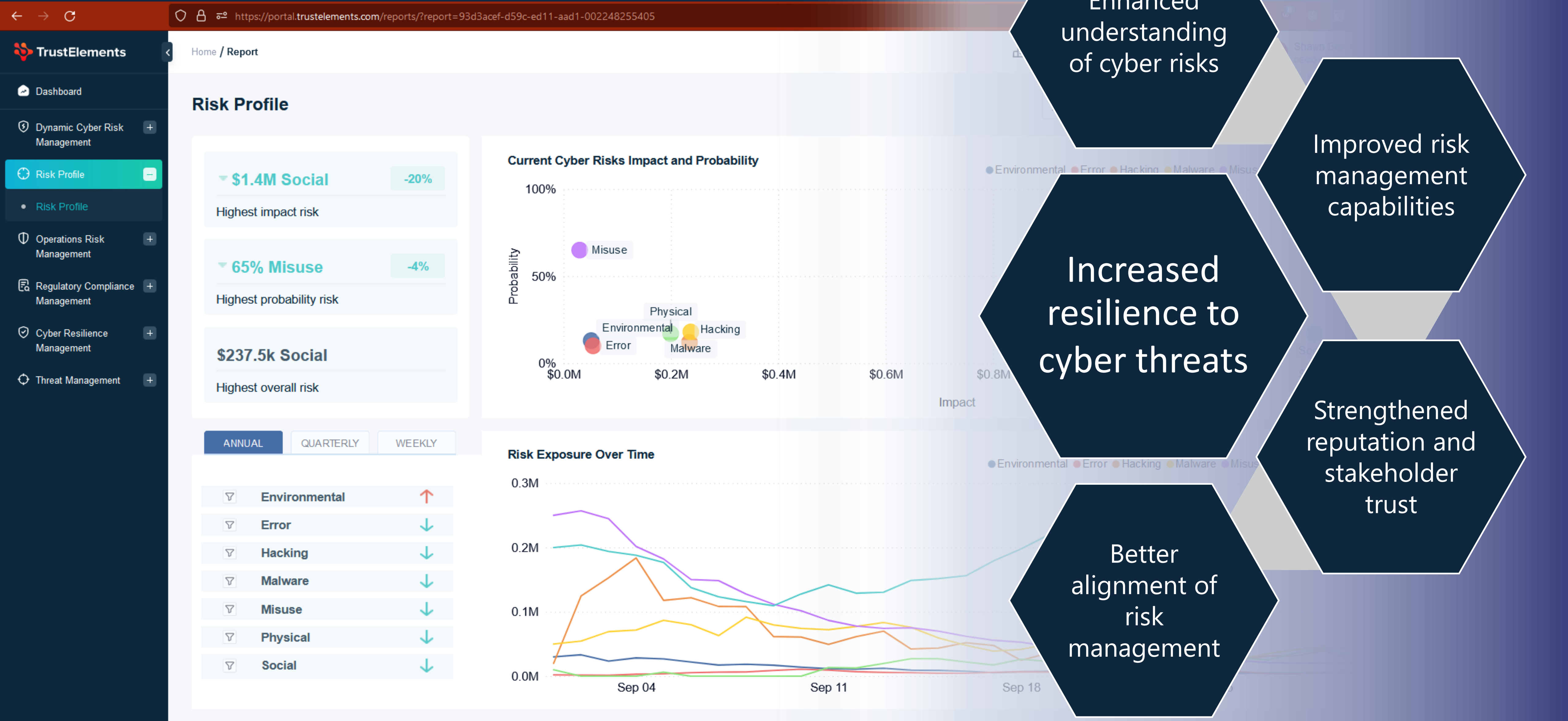
Simple Reporting to Business Stakeholders

Trusted by

"In today's environment of increasingly sophisticated criminal attacks, our mutual customers rely on proactive solutions such as TrustElements to help protect their organizations from cyberthreats…".

Ryan McGee,
Director of Product Marketing for Security

TrustElements Benefits



https://portal.trustelements.com/reports/?report=93d3acef-d59c-ed11-aad1-002248255405

TrustElements

- Dashboard
- Dynamic Cyber Risk Management +
- Risk Profile −
  - Risk Profile
- Operations Risk Management +
- Regulatory Compliance Management +
- Cyber Resilience Management +
- Threat Management +

Home / Report

Risk Profile

$1.4M Social -20%
Highest impact risk

65% Misuse -4%
Highest probability risk

$237.5k Social
Highest overall risk

ANNUAL | QUARTERLY | WEEKLY

Environmental	↑
Error	↓
Hacking	↓
Malware	↓
Misuse	↓
Physical	↓
Social	↓

Current Cyber Risks Impact and Probability

Risk Exposure Over Time

Enhanced understanding of cyber risks

Improved risk management capabilities

Increased resilience to cyber threats

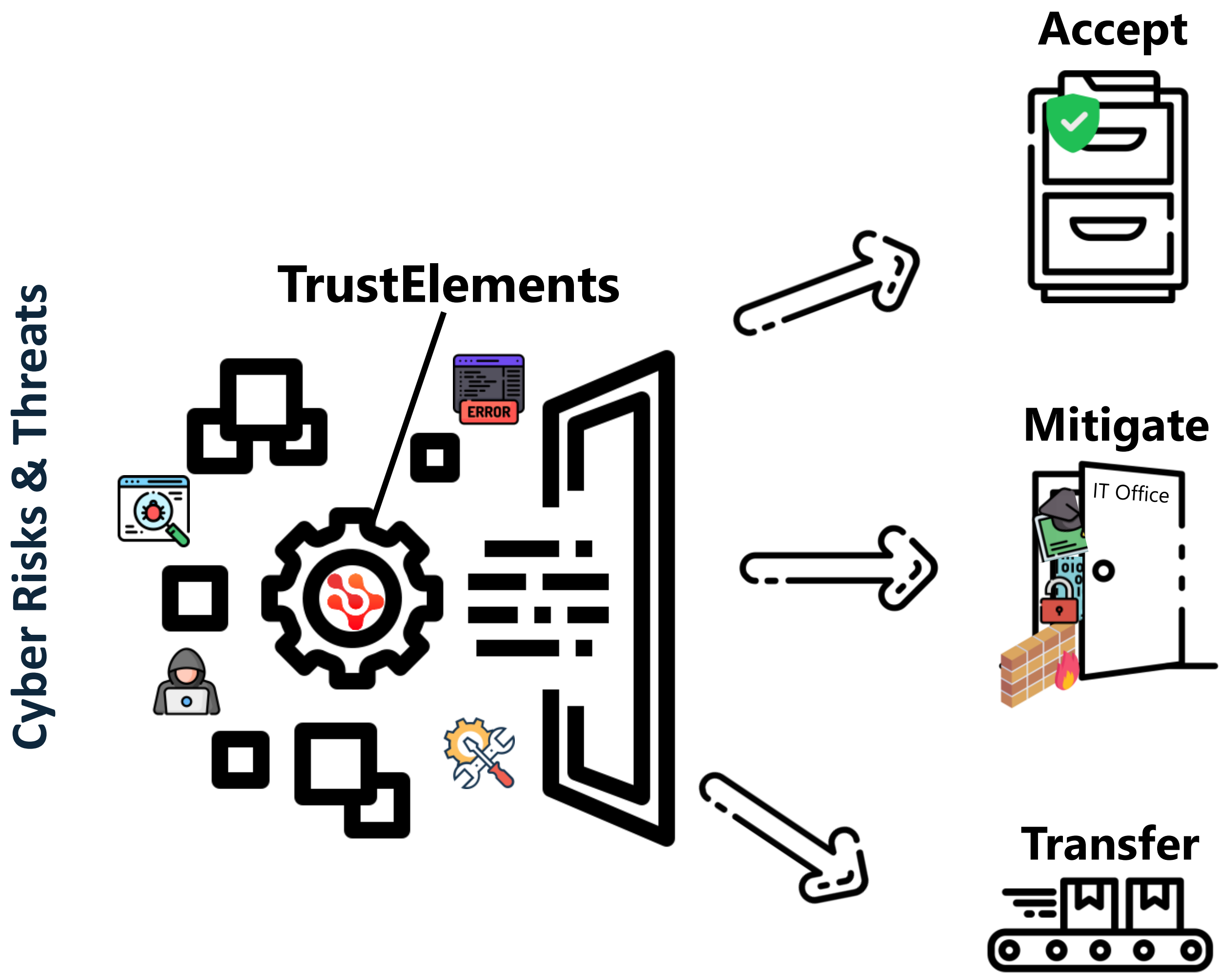
Strengthened reputation and stakeholder trust

Better alignment of risk management

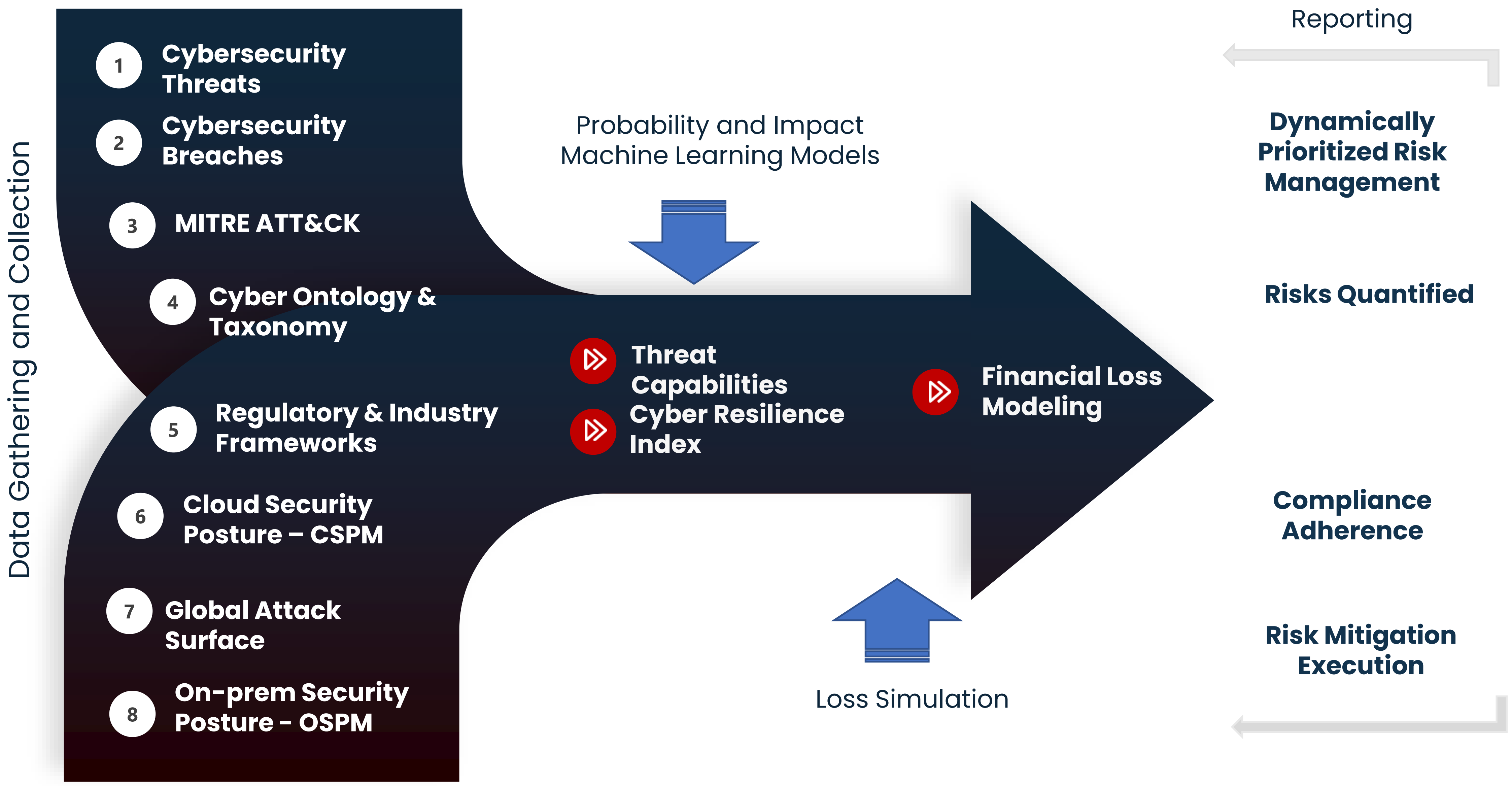
- TrustElements provides **dynamic cyber risk monitoring** and **assessment** and utilizes advanced **risk models** to accurately **quantify losses** to **manage enterprise risks**

- We are uniquely qualified to identify, mitigate and transfer cyber risks based on your risk appetite

- We serve as independent audit platform that aligns IT cyber efforts with board of directors' strategy



TRUSTELEMENTS APPROACH



Data Gathering and Collection

1. Cybersecurity Threats
2. Cybersecurity Breaches
3. MITRE ATT&CK
4. Cyber Ontology & Taxonomy
5. Regulatory & Industry Frameworks
6. Cloud Security Posture – CSPM
7. Global Attack Surface
8. On-prem Security Posture - OSPM

Probability and Impact Machine Learning Models

Threat Capabilities

Cyber Resilience Index

Financial Loss Modeling

Loss Simulation

Reporting

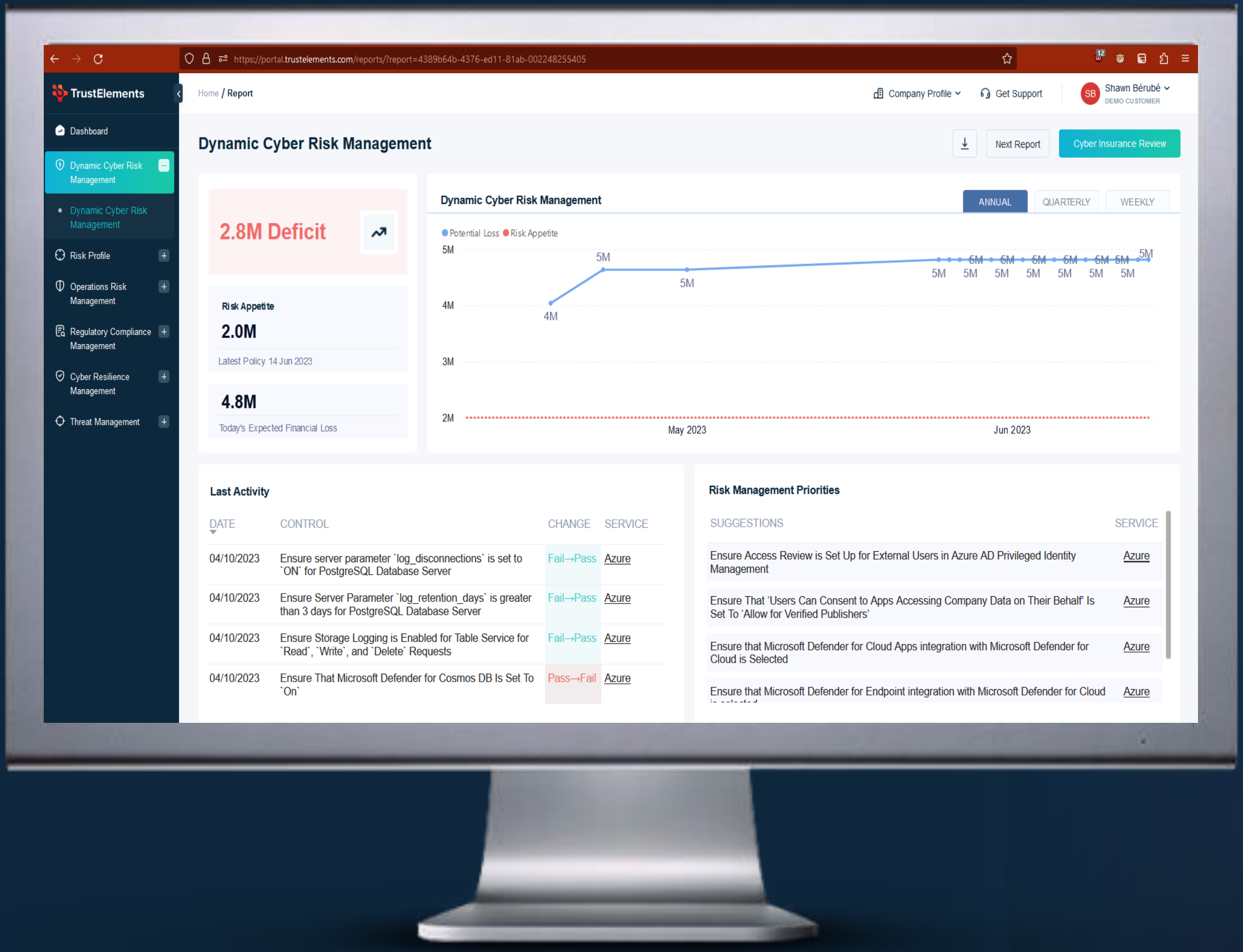
Dynamically Prioritized Risk Management

Risks Quantified

Compliance Adherence

Risk Mitigation Execution

TrustElements’ Dynamic Cyber Risk Management (DCRM)


https://portal.trustelements.com/reports/?report=4389b64b-4376-ed11-81ab-002248255405
TrustElements
Home / Report
Company Profile
Get Support
SB
Shawn Bérubé
DEMO CUSTOMER
Dashboard
Dynamic Cyber Risk Management
Dynamic Cyber Risk Management
Risk Profile
Operations Risk Management
Regulatory Compliance Management
Cyber Resilience Management
Threat Management
Next Report
Cyber Insurance Review
ANNUAL
QUARTERLY
WEEKLY
● Potential Loss ● Risk Appetite
5M
4M
3M
2M
May 2023
Jun 2023

Dynamic Cyber Risk Management

2.8M Deficit

Risk Appetite
2.0M
Latest Policy 14 Jun 2023

4.8M
Today's Expected Financial Loss

Dynamic Cyber Risk Management

Last Activity

DATE	CONTROL	CHANGE	SERVICE
04/10/2023	Ensure server parameter `log_disconnections` is set to `ON` for PostgreSQL Database Server	Fail→Pass	Azure
04/10/2023	Ensure Server Parameter `log_retention_days` is greater than 3 days for PostgreSQL Database Server	Fail→Pass	Azure
04/10/2023	Ensure Storage Logging is Enabled for Table Service for `Read`, `Write`, and `Delete` Requests	Fail→Pass	Azure
04/10/2023	Ensure That Microsoft Defender for Cosmos DB Is Set To `On`	Pass→Fail	Azure

Risk Management Priorities

SUGGESTIONS	SERVICE
Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management	Azure
Ensure That ‘Users Can Consent to Apps Accessing Company Data on Their Behalf’ Is Set To ‘Allow for Verified Publishers’	Azure
Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	Azure
Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected	Azure

Real-time data with adaptive cyber risk prioritization

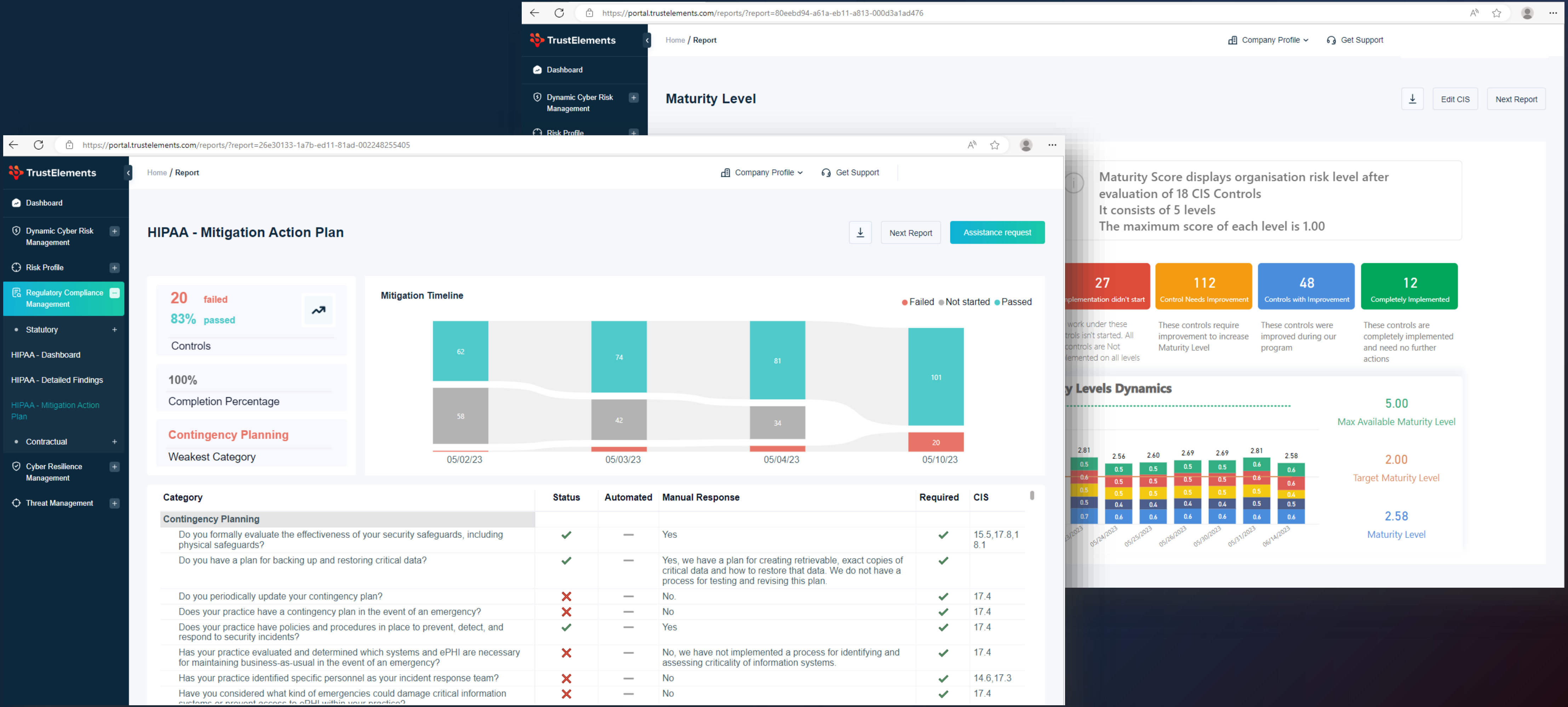
Manage risks via a quantified dollar value

Automate mitigation, acceptance, or transference of risks based on your risk appetite

Automated Regulatory Compliance

TrustElements

Compliance tracking functionalities to ensure adherence to industry regulations and best practices.



Maturity Level

Maturity Score displays organisation risk level after evaluation of 18 CIS Controls
It consists of 5 levels
The maximum score of each level is 1.00

27 — nplementation didn't start: work under these trols isn't started. All controls are Not lemented on all levels

112 — Control Needs Improvement: These controls require improvement to increase Maturity Level

48 — Controls with Improvement: These controls were improved during our program

12 — Completely Implemented: These controls are completely implemented and need no further actions

y Levels Dynamics

5.00 Max Available Maturity Level

2.00 Target Maturity Level

2.58 Maturity Level

HIPAA - Mitigation Action Plan

20 failed
83% passed
Controls

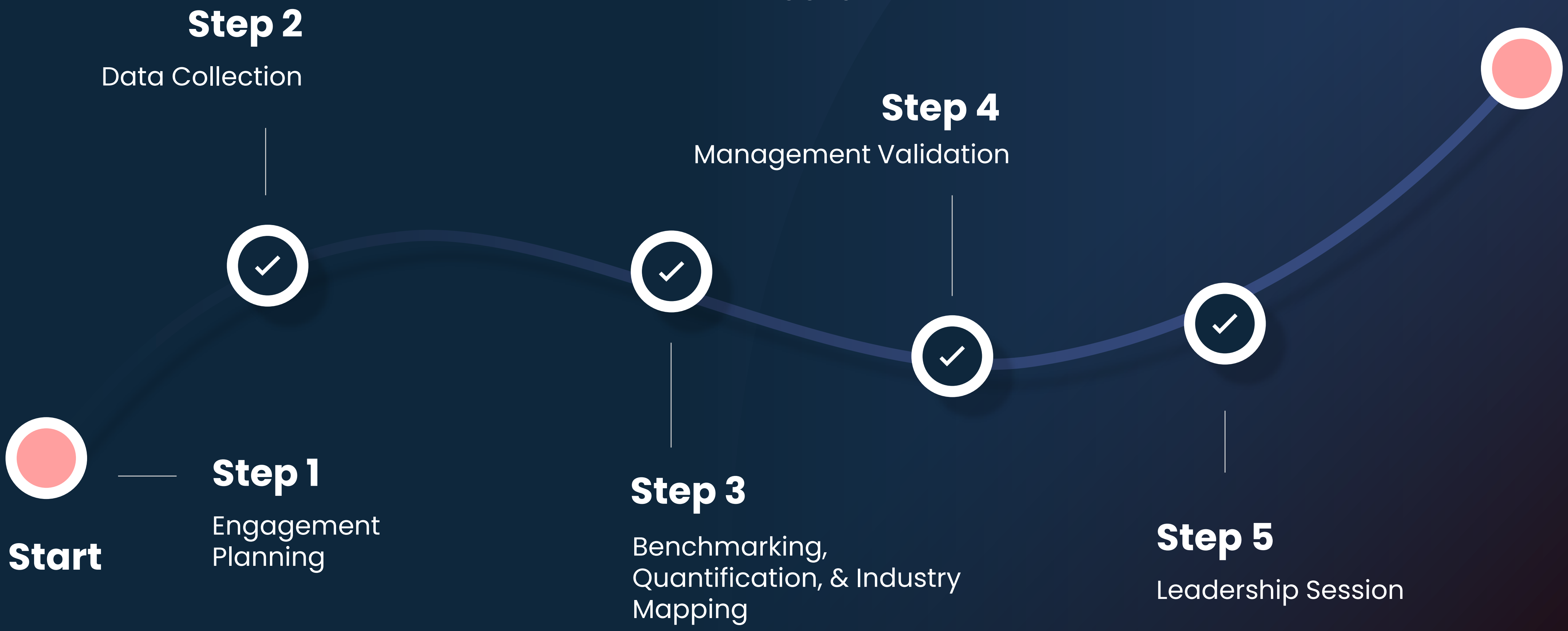
100%
Completion Percentage

Contingency Planning
Weakest Category

Category	Status	Automated	Manual Response	Required	CIS
Contingency Planning					
Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?	✓	—	Yes	✓	15.5,17.8,18.1
Do you have a plan for backing up and restoring critical data?	✓	—	Yes, we have a plan for creating retrievable, exact copies of critical data and how to restore that data. We do not have a process for testing and revising this plan.	✓	
Do you periodically update your contingency plan?	✗	—	No.	✓	17.4
Does your practice have a contingency plan in the event of an emergency?	✗	—	No	✓	17.4
Does your practice have policies and procedures in place to prevent, detect, and respond to security incidents?	✓	—	Yes	✓	17.4
Has your practice evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?	✗	—	No, we have not implemented a process for identifying and assessing criticality of information systems.	✓	17.4
Has your practice identified specific personnel as your incident response team?	✗	—	No	✓	14.6,17.3
Have you considered what kind of emergencies could damage critical information systems or prevent access to ePHI within your practice?	✗	—	No	✓	17.4

Onboarding Process

Gain valuable insights within 1-2 weeks



Start

Step 1

Engagement Planning

Step 2

Data Collection

Step 3

Benchmarking, Quantification, & Industry Mapping

Step 4

Management Validation

Step 5

Leadership Session

Ongoing Mitigation

THANK YOU

Schedule a demo

TrustElements

Inquiries: contact@trustelements.com
Call us: 862-240-1404