AFRIKO CYBER

CYBER SECURITY SERVICES

SOMANSA DLP

OFFERINGS

Privacy-i is Sure, the image you sent is a brochure about Privacy-i, a software that monitors and scans for confidential data on desktops and laptops. The software works by using pre-defined and customizable content-aware detection methods and policies.

The features are:

- Data Leakage Prevention: Privacy-i can help prevent data leaks by controlling and recording endpoint (PC) events where information can be leaked to printers, removable storage media, messenger, WebMail, and cloud.

- Minimizes the risk of data breaches: By scanning, destroying, or encrypting unattended personal data on PCs, and deleting unnecessary personal information files, Privacy-i can help minimize the risk of data breaches.

Privacy-i

Endpoint DLP Privacy-i

SOMANSA DLP

OFFERINGS

Mail-i is for a network data loss prevention (DLP) solution. It helps organizations protect sensitive data by monitoring data in motion. It can do this by monitoring traffic from web-hosted mail, webhard, social networking, instant messengers, P2P, and shared folders.

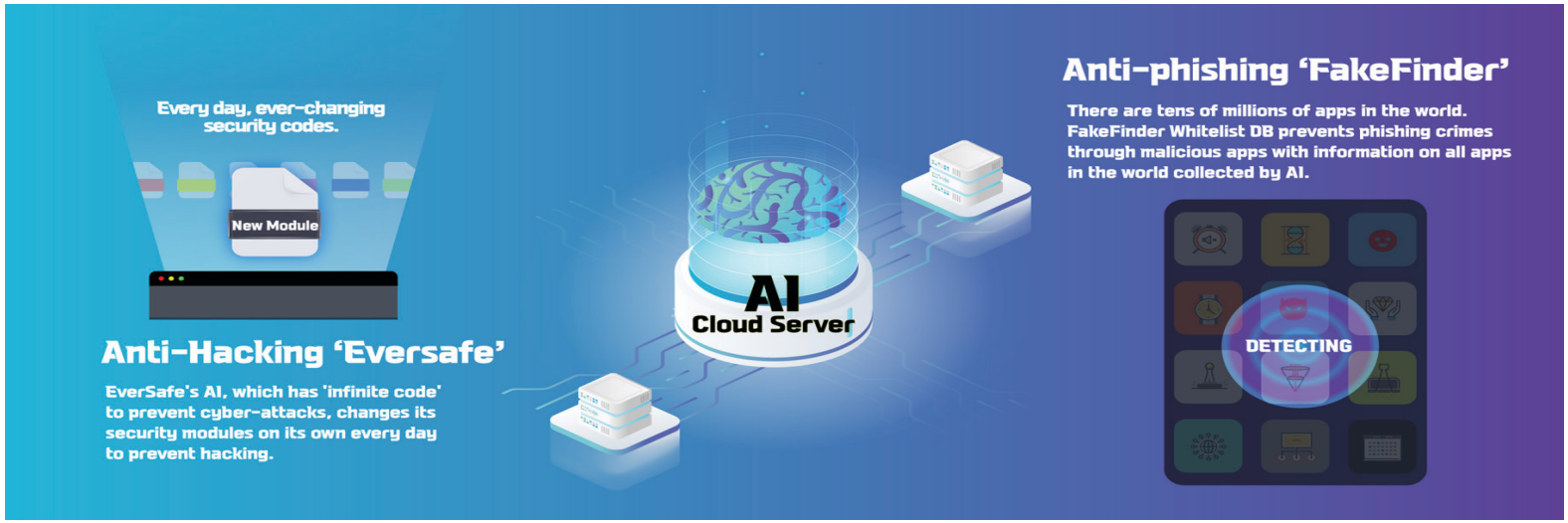
The features are:

- It can decrypt SSL/TLS traffic, which means it can monitor data that is encrypted in transit.
- It can control SSL/TLS-based web services such as Google Drive, Apple iCloud, Microsoft Office 365, and Dropbox.
- It can control and block data leaks from individual PCs, even if the Privacy-i agent is not installed, disabled, or out of date.

Privacy-i
Endpoint DLP Privacy-i

Moving Target Defence (MTD)

We provide anti-hacking & anti-phishing solutions based on AI(artificial intelligence)



Moving Target Defence (MTD)

There are 3 solutions - Mobile

There is no unsolved maze in this World. But we only need ***sufficient time*** to analyze the maze. ***If the hacker who understands the programming language of developers, has sufficient time, everything will be finally analyzed and bypassed.***

[Problem] Is the hacker able to analyze the following code?

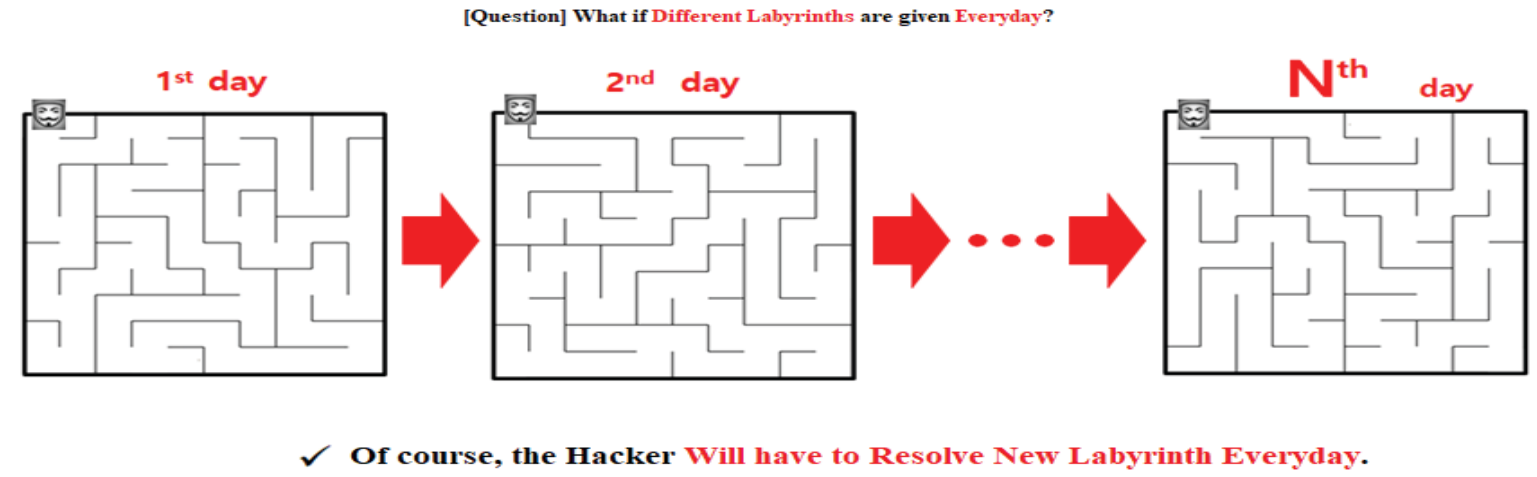
```
.line 57
iget-object v0, p0, Lcom/isaku/app/RegisterPinActivity;->account:Lcom/isaku/app/model/UserAccount;

iget-object v1, p0, Lcom/isaku/app/RegisterPinActivity;->newpin:Landroid/widget/EditText;

invoke-virtual {v1}, Landroid/widget/EditText;->getText()Landroid/text/Editable;

move-result-object v1

invoke-virtual {v1}, Ljava/lang/Object;->toString()Ljava/lang/String;

move-result-object v1

invoke-virtual {v0, v1}, Lcom/isaku/app/model/UserAccount;->setPin(Ljava/lang/String;)V

.line 59
new-instance v0, Lcom/isaku/app/RegisterPinActivity$RequestActivationCodeTask;

iget-object v1, p0, Lcom/isaku/app/RegisterPinActivity;->account:Lcom/isaku/app/model/UserAccount;
```

[Answer] The code is analyzed as following labyrinth with only sufficient time

Moving Target Defence (MTD)

There are 3 solutions - Mobile

TBut if New Mazes are given Everyday to the Hacker as the following image, the Time of the Hacker could be controlled as the Hacker needs to resolve Different Mazes Everyday.



Moving Target Defence (MTD) - Anti-Hacking Solution

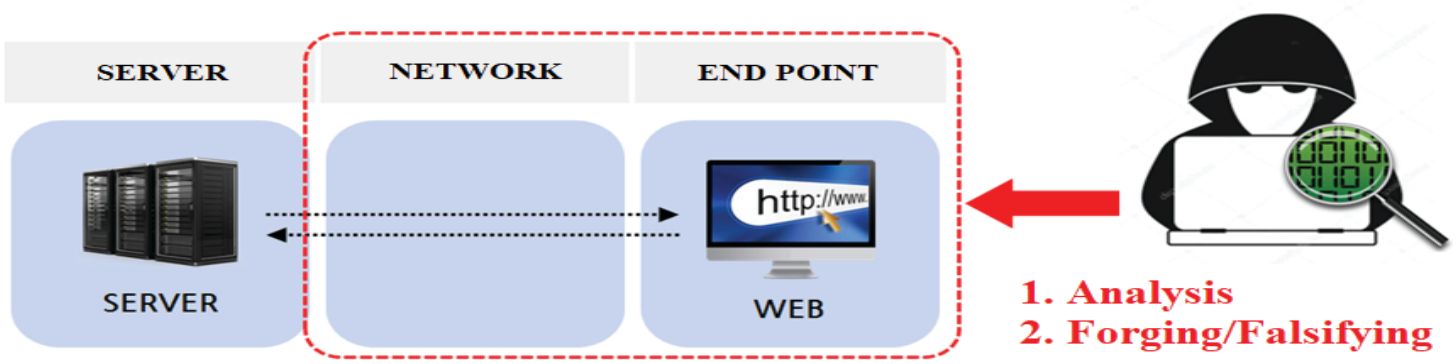
(1) anti-hacking solution) : AI based MTD Security Module Generator

- Security module can be generated infinitely.
- Every security module has different source code.

Moving Target Defence (MTD) - Web

- Everspin extended to ***WEB Area (PC & Mobile)*** in addition to mobile area, through endless R&D on the Moving Target Defense Technology (released in January 2021)
- Woori Credit Card hosted a competitive technological BMT between EverSafe and Arxan of U.S.A., EverSafe WON OVERWHELMINGLY.
- Korea Investment & Securities Co., Ltd. hosted a competitive technological BMT between Eversafe and Imperva(*) of U.S.A., again, Eversafe WON OVERWHELMINGLY.

(*)Highest Class in the World of Web Security: https://en.wikipedia.org/wiki/Imperva)



We have Extended the Dynamic (Moving Target Defense) Security Technology even to the WEB area
to Completely Block the Analyzing and Forging Act of the Hacker in the WEB, where hacking attack is very frequent.

Moving Target Defence (MTD) - Web

- Moving Target Defense-based Anti-Hacking Technology performs protection by changing the security code that detects hacker's analysis and forgery by daily or weekly basis.
- ***EverSafe WEB' is an Anti-Hacking Solution which does not give enough time to the attempt of hacker of analyzing and hacking the Web.***

Actual security script provided to Client A (part of source code)

Dynamic Change Factors(*)

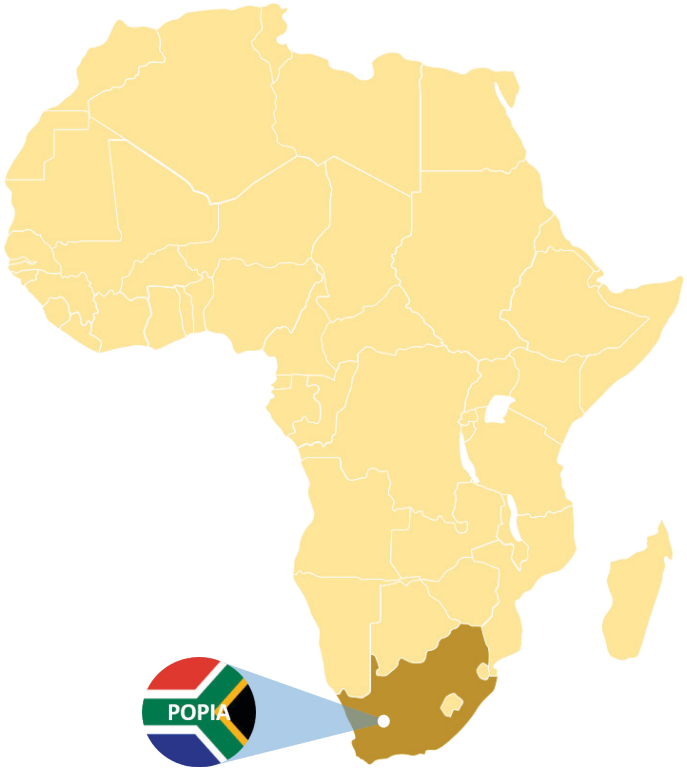
- Automatized tool detection code
- Integrity detection code
- Identifier
- Function location
- Factor sequence, return value use method
- Encryption algorithm
- Inter-function forgery detection code
- Hash algorithm
- String encryption
- Constant encryption
- Dummy code

Key Functions (Functions provided by the script with Dynamic Change Factor applied).

- HTML forgery prevention and obfuscation.
- URL de-identification.
- JavaScript obfuscation.
- Developer tool detection.
- Operation data encryption (E2E)
- Scrapping prevention
- Session forgery

(*) Dynamic Change Factors : Security script is running by changing the factors indicated in the table everyday or by certain cycle.

POPIA at A Glance



Purpose
POPIA aims to promote the protection of personal information processed by public and private bodies and to establish minimum standards for the lawful processing.

Scope
The Act applies to the processing of personal information by any responsible party (individual or organization) in South Africa, regardless of whether the processing occurs electronically or manually.

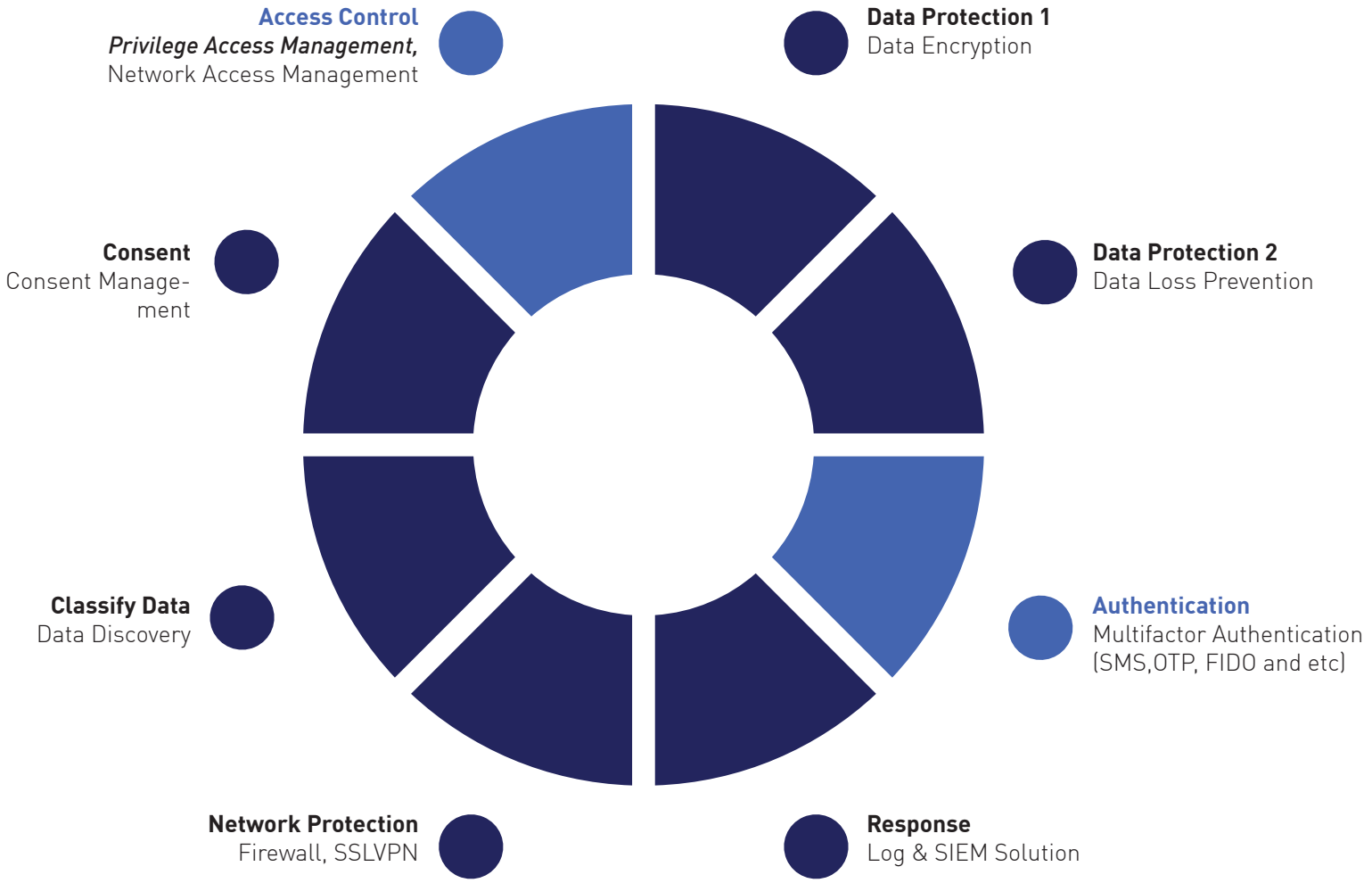
Personal Information
POPIA defines personal information broadly to include any information relating to an identifiable, living natural person, and includes factors such as race, gender, age, identity numbers, email addresses, physical addresses, and more.

Conditions and Lawful Processing
The Act sets out conditions for the lawful processing of personal information, including obtaining the data subject's consent, processing necessary for the performance of a contract, compliance with legal obligations, and legitimate interests pursued by the responsible party.

Security Measures
Responsible parties are required to implement appropriate technical and organizational measures to secure personal information against unauthorized access, loss, or destruction.

Compliance and Enforcement
POPIA establishes the Information Regulator, an independent body responsible for monitoring and enforcing compliance with the Act. Non-compliance can result in significant penalties, including fines and imprisonment.

POPIA at A Glance



PAM MARKET OVERVIEW

Why **PAM?**

PAM HIGHLIGHTS :
The need for Privileged Access Management **(PAM) arises from regulatory and compliance requirements,** coupled with concerns about cybersecurity, particularly in the context of laws such as the General Data Protection Regulation (GDPR). The GDPR has made information security, including access to various systems containing sensitive information, a significant concern for many organizations.

Regarding the selling points versus pain points, it is quite clear that many organizations require security controls to oversee users with assigned high permissions, especially when accessing systems with high sensitivity. However, the implementation of PAM or security controls within the IT system structure must address various aspects beyond just functional usage.

It is evident that certain sub-features may not be of paramount importance to users, but the **primary features play a crucial role in addressing various critical pain points.**

Supervision and Management of High-Privileged Users

2. **Cyber Threat**
3. **Data Protection Laws (GDPR/POPIA)**
4. **Regulation and Compliance Issues**
5. **Security Vulnerabilities**

Why **PAM?**

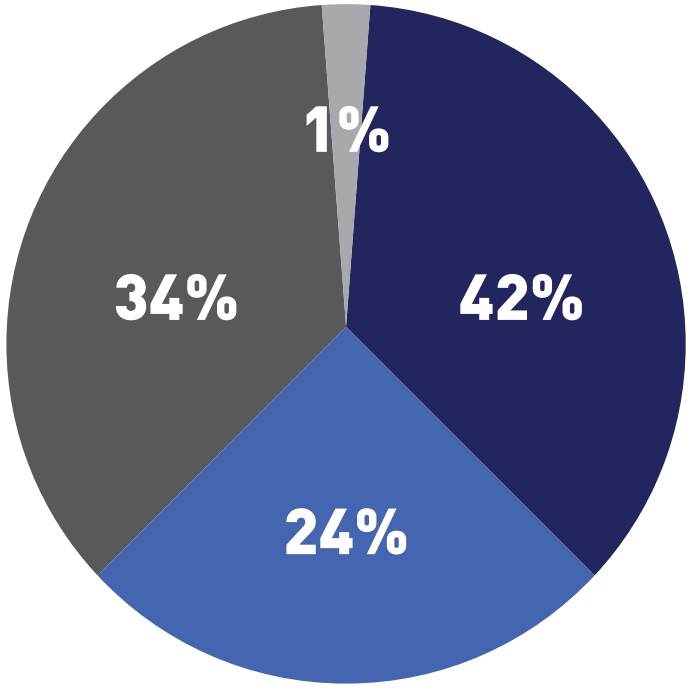
Majority of organizations express concern when granting excessively high privileges or dealing with users possessing elevated privileges. It is commonplace for information providers to communicate such apprehensions with the team.

The rationale behind each organization's apprehension, after adopting Privileged Access Management (PAM), revolves around whether the system can effectively address these concerns or not.

These concerns typically include:

- Security and Vulnerabilities
- Compliance Issues
- Rights and Access Permissions
- Integration with existing systems

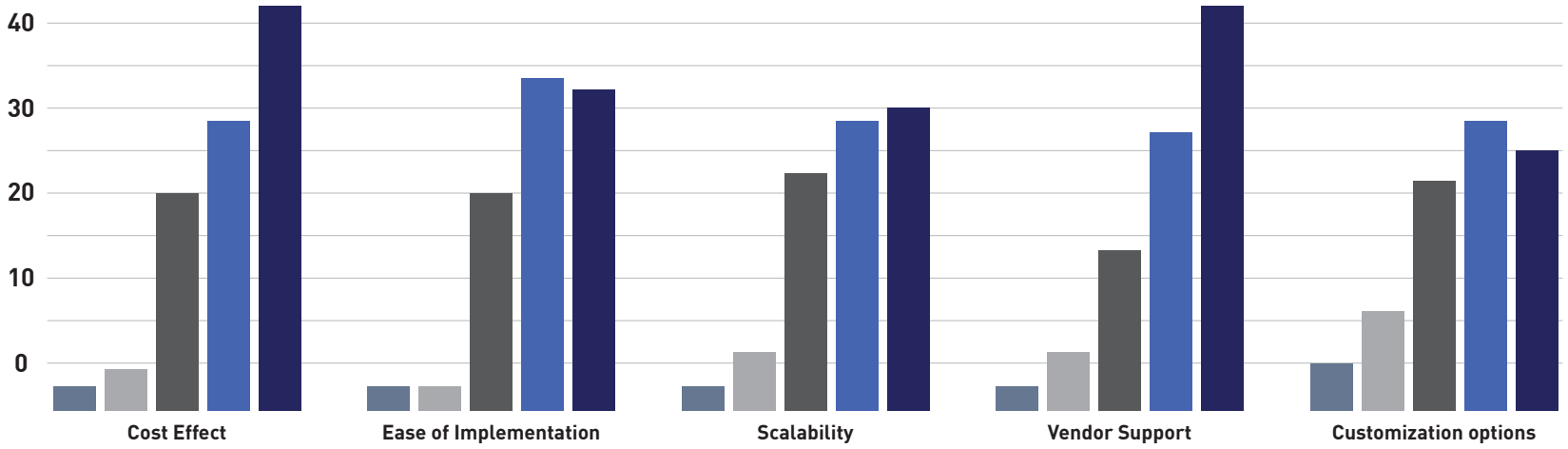
Beyond addressing issues for IT departments and organizations, these fundamental requirements mentioned above should be given top priority.



Which **PAM?**

IMPORTANT NOTE :
The importance of each factor depends on the organization's priorities, existing infrastructure, and long-term goals. Organizations may weigh these factors differently based on their specific context, industry, and risk profile.

A thorough assessment of their own requirements and a careful evaluation of how each factor aligns with their goals will help organizations make an informed decision when selecting a PAM solution.



Organizations in Thailand may prioritize solutions that offer a good balance between affordability and the value provided.

The ease implemented is crucial, particularly for organizations with limited IT resources or tight timelines.

A PAM solution that can easily **scale to accommodate an expanding infrastructure**

The level of support offered by the PAM vendor is significant.

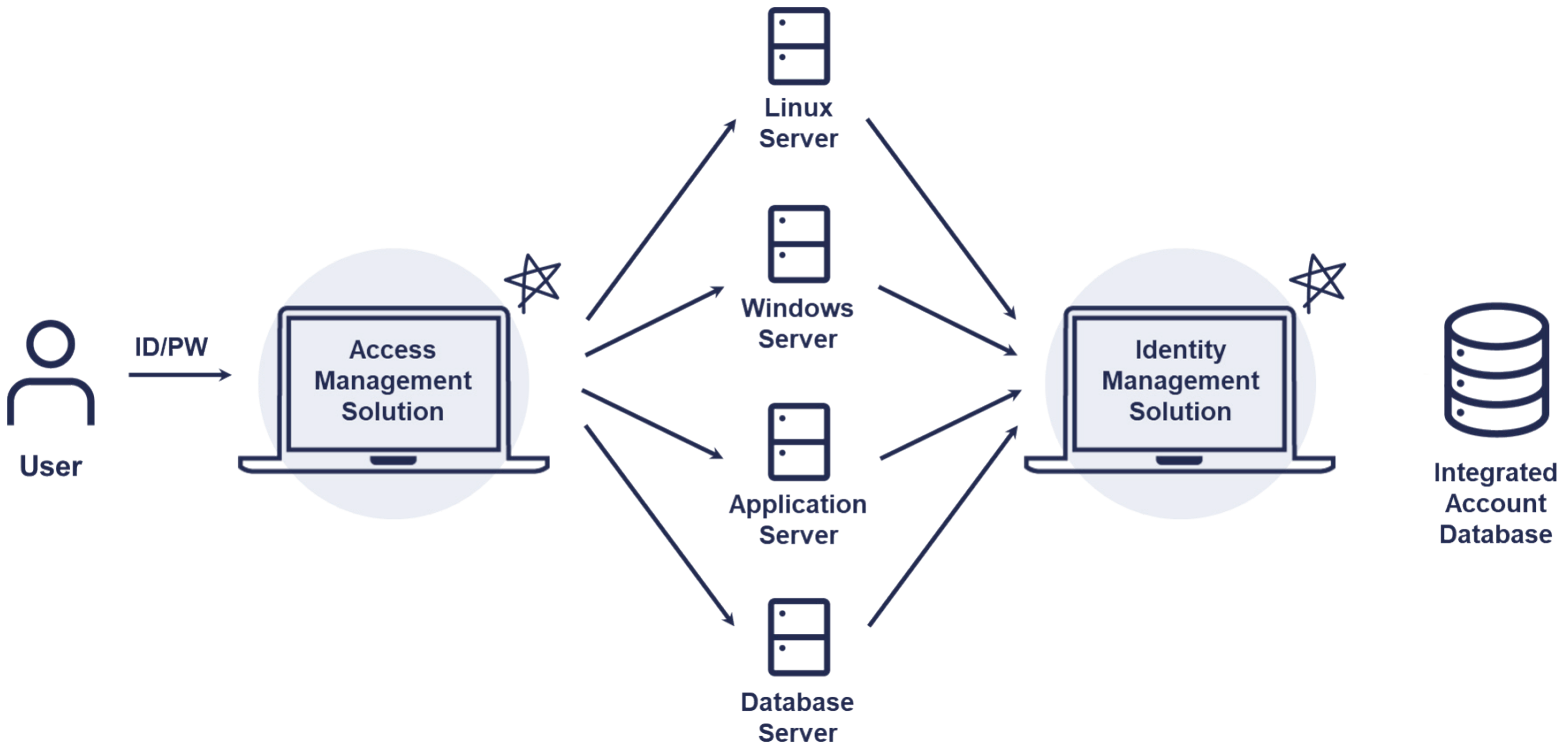
Organizations with unique security needs or specific compliance requirements may prioritize solutions that offer a high degree of customization.

Scoring 1-5

1 (less important)
2
3
4
5 (very important)

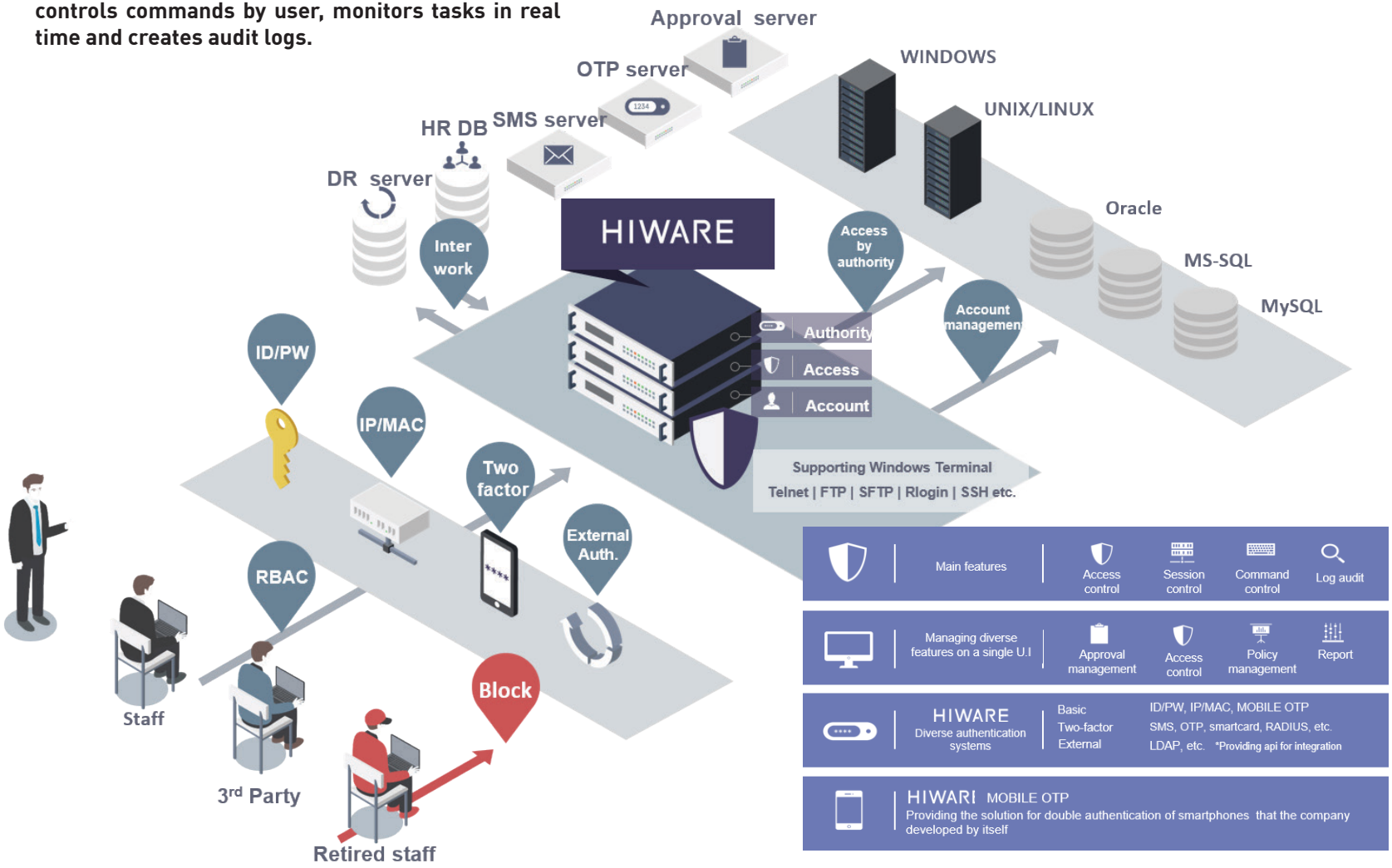
NETAND & HIWARE

Identity & Access Management



HIWARE PAM for System and DBMS

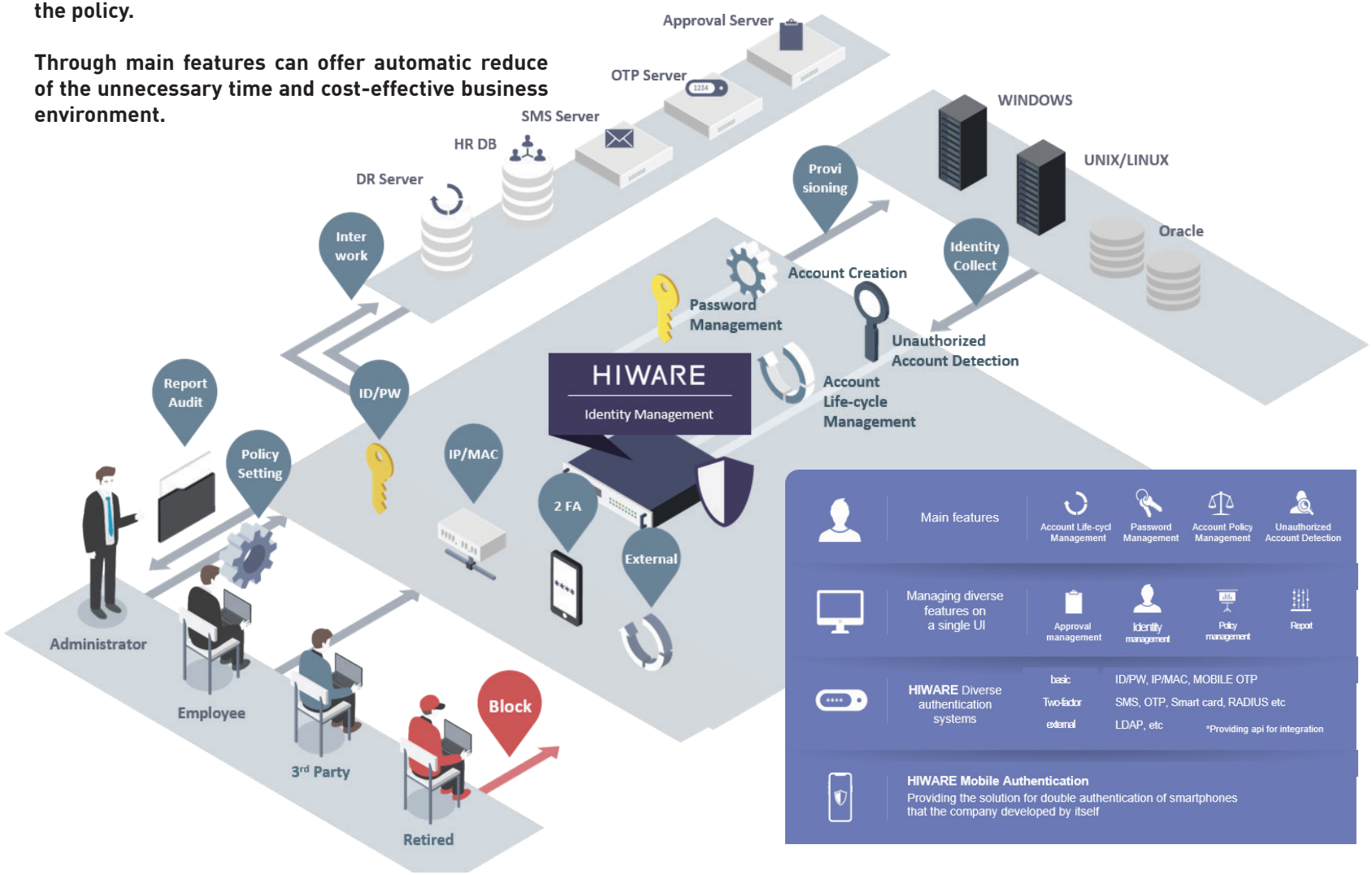
HI-PAM is an access control solution which controls and manages remote access of infrastructure and operation systems such as networks and servers, controls commands by user, monitors tasks in real time and creates audit logs.



HIWARE PAM for System and DBMS

HI-IM collects identities from heterogenous devices and manages the life-cycle and passwords through the policy.

Through main features can offer automatic reduce of the unnecessary time and cost-effective business environment.



HIWARE PAM for System and DBMS

1. Cyber Breach Testing
2. Information Security Audits and Assessments
3. Digital Forensic Investigations
4. Managed Security Services
5. Client Protection
6. Information Security Awareness and Training
7. Password Assurance
8. Predictive Analysis
9. 3rd Party Risk Management

01. Cyber Breach Testing:

Cyber Breach Testing involves the use of a variety of manual and automated techniques to simulate an attack– either from malicious outsiders or internal staff. The discipline of breach testing is employed within organisations to undertake an offensive approach to ensuring the protection of key assets. This form of testing underlines the security weaknesses within computer systems, networks, web applications and access controls that an attacker could potentially exploit.

Breach testing provides an overview of the organisation's cyber resilience and an evaluation of the incident and response capability, the effectiveness of policies and procedures, its adherence to compliance requirements, and its employees' security awareness and training levels. The outcome of a cyber breach test is a detailed report on the vulnerabilities of the tested infrastructure and how these can be exploited by an attacker. Services included are:

- Penetration Testing
- Firewall Rule Testing
- Application Security Testing
- Wifi Security Testing
- Network Security Testing

02. Information Security Audits and Assessments:

Organisations are increasingly required to demonstrate their compliance to data protection legislation and security standards. Improved compliance reduces the risks that threaten the confidentiality, availability, and integrity of customer information.

The Information security audit is an overall assessment of the Client's information security practices, both physical and digital, that can potentially lead to its compromise, if exploited by cybercriminals. The information security audits follow a risk-based approach, which means that the audit will seek to identify risks with the greatest potential impact to the organisation.

We offer a bespoke and independent review and examination of system records, activities, and related documents and deliver assessment results in a detailed report, supported with a roadmap for remediation. Services included are:

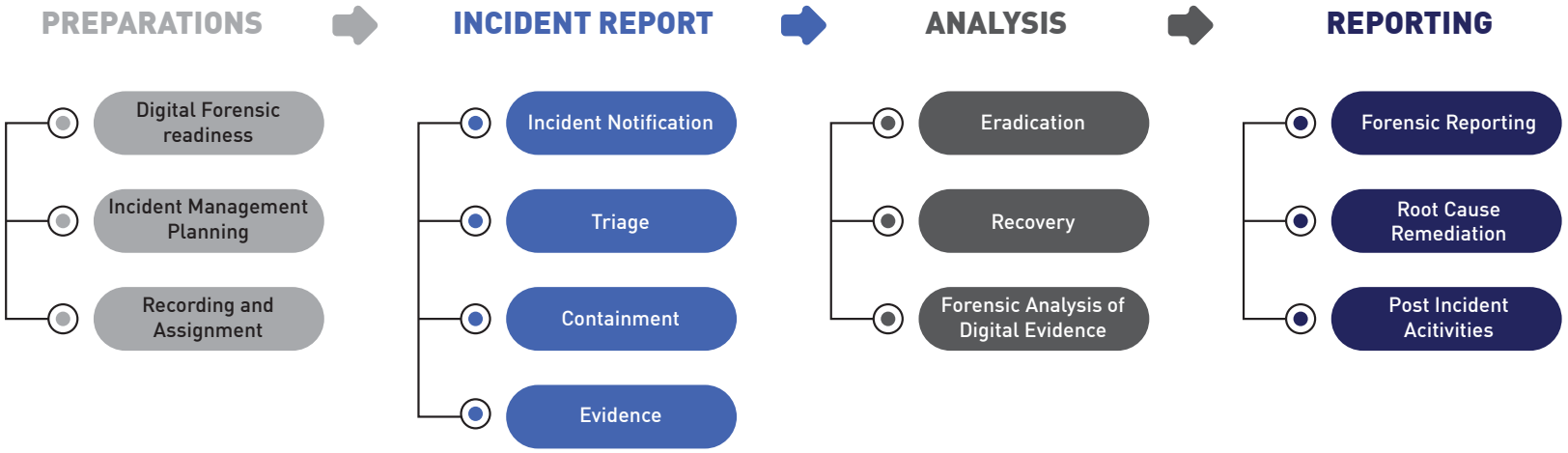
- Baseline Information Security Risk Assessments
- OT Security Assessments
- Vulnerability Assessments
- Privacy Compliance Assessments (PoPIA and GDPR)
- Information Security Maturity Assessment
- Third-Party Information Risk Assessment
- Digital Footprint Assessment

03. Digital Forensic Investigations:

Digital forensics is a form of forensic science that assists organisations with the recovery and investigation of incidents in the digital environment. Digital Forensic investigations are a source of truth.

The digital forensic investigator uses innovative techniques and procedures to investigate the root cause of any data breach with the purpose of recovering lost or stolen data, discovering the origins of a specific attack, tracing it back to its source, and produce a detailed investigative report with recommendations on how to restore the device. Services included are:

- Mobile device forensics (Smart Devices)
- Server Forensics



04. Managed Security Services:

FSI offers our clients the opportunity to outsource all security functions to a highly skilled and experienced team of cyber security experts. FSI assists in the identification and deployment of complex security infrastructure, managing platforms and tools, providing continuous 24/7/365 monitoring, and offer incident response services.

Our MSS tam ensures that our client's systems are safe and compliant with cyber security standards. Our MSS include:

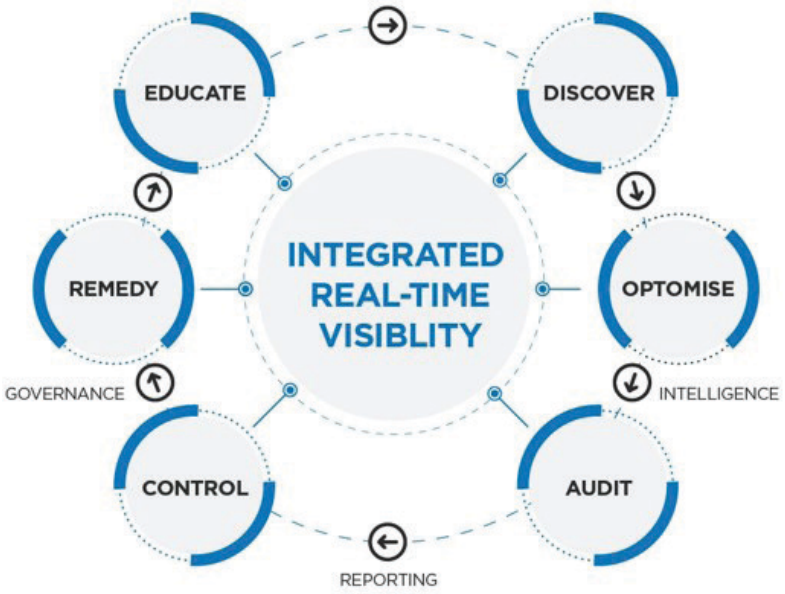
- Firewall Management
- EDR / Antivirus Management
- Vulnerability / Patch Management
- SIEM/ SOAR Capability
- Cyber Threat Intelligence/ Dark web scraping
- Third-Party Risk Monitoring
- Threat Hunting
- Access Management (OneSpan Token System)

Principle 1: Govern Proactively

Principle 2: Protect Intelligently

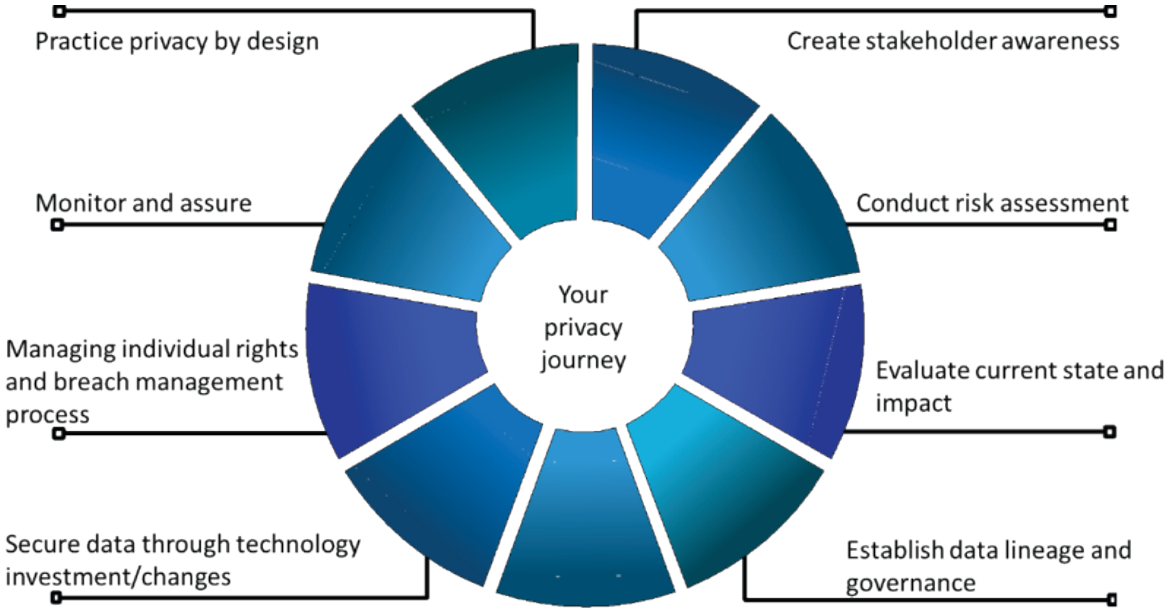
Principle 3: Detect Dynamically

Principle 4: Respond Effectively



05. Client Protection:

A one-of-a-kind bespoke awareness and protection tool created with data rich intelligence designed to proactively protect clients and their data. Through an integrated approach using various risk profiling and data management sources, client protection is achieved through awareness and proactive management of malicious IP's, sites, and more.



06. Information Security Awareness and Training:

Beyond South Africa's 26.92% current unemployment rate, the rest of the continent faces significant infrastructural and educational challenges, making it one of the region's most at risk. While technological changes can benefit the country, unskilled or semi-skilled people are going to find it more difficult to get jobs.

Talent development and up-skilling is crucial for Africa to address the current unemployment plight. But education systems require massive investments, particularly in key subjects in the sciences and technology.

FSI offers a diverse scope of training for any corporate that needs to upskill their staff. The training programs as developed and delivered by the FSI team are ones that focus on academia in conjunction with practical training. Our learning solutions include:

- Instructor led courses
- Online courses
- Custom course development
- System Learning Platform and Content

07. Password Assurance:

Password Assurance is a solution developed by the FSI team. The application is deployed to at least one domain controller in each domain on the client network.

The Password Assurance application identifies and encrypts all user account hashes. The user account information is then subjected to multiple hacking techniques to identify any weak passwords. This enables informing individual users of their weak passwords.

Any compromised account information is sent to the client technical teams for remediation.

08. Predictive Risk Analysis:

The benefits of employing predicative risk analysis is far reaching and mission critical, providing an overview of your current performance as perceived by local and international feeds (sentiment), your current risks and your potential future risks allowing your business to be proactive and resilient.

Predictive process mining enables the discovery of potential issues and the reasons behind them. It can leverage either **risk prediction or time prediction** categories:

- Risk predictions are categorial predictions that estimate and inform about risk levels in decision-making processes by configuring process risk indicators and examining historical data.
- Time predictions are numeric predictions that are applied to measure the delays or remaining time in a continuing process.

1. **Early warnings for possible threat actors**
2. **Peace of mind**
3. **Future-proofing your business.**
4. **Receiving a complete overview of your company's profile online**
5. **See what's trending when it comes to your company**
6. **Receive up to date analytics on what people are saying about you online.**

09. 3rd Party Risk Management:

Third-party breaches jeopardize IT systems and customer data, supply chain disruptions threaten business operations, and vendor compliance violations can impact your business. However, traditional approaches to third-party risk management (TPRM) are hampered by spreadsheet-driven processes, outdated information, and siloed teams. If you're responsible for hundreds (or even thousands) of third parties, how do you keep up, make sound decisions, and scale for the future?

FSI will assist the Client in defining the risk tolerance levels. Once defined, this measure will be used to analyse risks.

Services Catalogue





IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Security Assessments: Risk Assessment OT Assessment Vulnerability Assessment Data Privacy Assessment Third-Party Assessment Digital Footprint Cloud security Microsoft AD Posture Assessment **Security Testing:** Penetration Testing Breach Testing DLP Testing	**Managed Security Services:** Configuration Management (Hardening) Firewall Management Vulnerability Management EDR Management OT Security Management Third-Party Access Authorization **Audits** Compliance Operational Third-Party Access management across multiple systems **Training and Awareness Phishing**	**SecOps Monitoring:** SIEM Cloud Endpoint Network User Behaviour Access Third-Party **Threat Intelligence and real-time investigation** **Attack Simulations** **Threat Hunting**	**SOAR** **Digital Forensics**	**Post-incident activities**

Clients


adept advisory
KZN GROWTH FUND
Inspired Investing
MTN
SOUTH AFRICAN MEDICAL ASSOCIATION
UNITING DOCTORS FOR THE HEALTH OF THE NATION
Coca-Cola Beverages South Africa
UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG
BULLETPROOF
a GLI company
SibanyeGOLD
We are One
dube tradePORT
SPECIAL ECONOMIC ZONE
GLI GAMING LABORATORIES INTERNATIONAL
supergroup
SUZUKI
CYBERSENSE
City of STONNINGTON
TIGER BRANDS
Sun International
UNISA university of south africa
PEERMONT
BAM TELECOMS

CONTACT US

kenny@afri-ko.com