ThIRU

SOC | NOC | BOC | COC

Edge Device to End Point

RAPID RESPONSE TO CYBER WARFARE

www.thirulabs.com

CONTINUOUS MONITORING & ORCHESTRATION
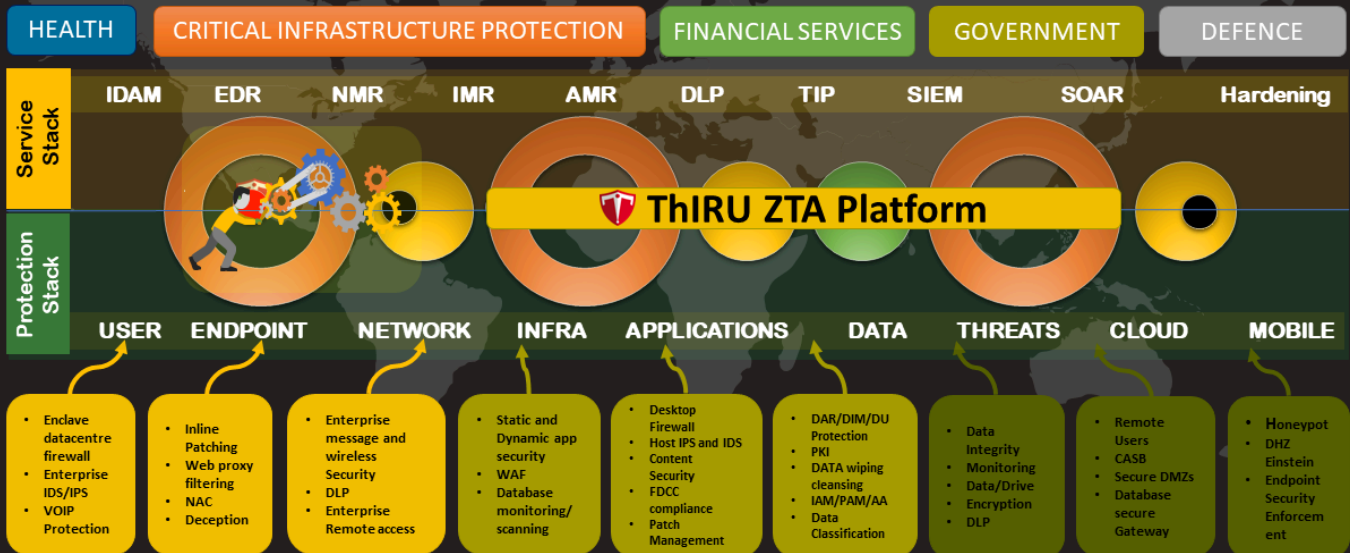

THREAT INTELLIGENCE RESPONSE UNIT(ThIRU) PLATFORM
PROTECTING FUTURE GENERATIONS

ThIRU
SOC | NOC | BOC | COC
Edge Device to End Point

BUSINESS & MISSION CRITICAL SYSTEMS

| HEALTH | CRITICAL INFRASTRUCTURE PROTECTION | FINANCIAL SERVICES | GOVERNMENT | DEFENCE |

Service Stack: IDAM, EDR, NMR, IMR, AMR, DLP, TIP, SIEM, SOAR, Hardening

ThIRU ZTA Platform

Protection Stack: USER, ENDPOINT, NETWORK, INFRA, APPLICATIONS, DATA, THREATS, CLOUD, MOBILE

USER	ENDPOINT	NETWORK	INFRA	APPLICATIONS	DATA	THREATS	CLOUD	MOBILE
• Enclave datacentre firewall • Enterprise IDS/IPS • VOIP Protection	• Inline Patching • Web proxy filtering • NAC • Deception	• Enterprise message and wireless Security • DLP • Enterprise Remote access	• Static and Dynamic app security • WAF • Database monitoring/scanning	• Desktop Firewall • Host IPS and IDS • Content Security • FDCC compliance • Patch Management	• DAR/DIM/DU Protection • PKI • DATA wiping cleansing • IAM/PAM/AA • Data Classification	• Data Integrity • Monitoring • Data/Drive • Encryption • DLP	• Remote Users • CASB • Secure DMZs • Database secure Gateway	• Honeypot • DHZ • Einstein • Endpoint Security Enforcement

Zero Trust Architecture (ZTA) : The Future of Cyber Security

Network and Infrastructure Security	A breach of a company's infrastructure or network can cost the company millions of dollars.
Web Security	Abuses of Web Security. Without a proactive security strategy, business risks are escalated.
Endpoint Security	Entry points can be exploited by hackers to cause loss of customer data, resulting in massive damage.
Application Security	Attackers can make use of vulnerabilities found in applications, exposing a potential risk to the business and its assets.
Data Security	A business' data is the key to growth and success. Data must be protected from unauthorized access, to prevent it from being tampered with, destroyed, or disclosed to others.
Risk and Compliance	Legislative Audit and Compliance reporting, conformance to standards, Penetration Testing, and Threat Risk Assessments are all mandatory requirements.
Security Operations and Incident Response	Incident response refers to the way in which a security breach is addressed and managed, in order to limit damage and reduce discovery.
Threat Intelligence	Addressing today's threats requires reliable intelligence which will keep companies informed of the advanced threats, exploits and zero-day threats, and how to take action against them.
IOT Security	Hackers exploit weaknesses in IOT security, not to attack the devices themselves, but as a launching point for all kinds of malicious behaviour.
Identity Access Management	Identity Access Management addresses insider threat and user related risks.
Cloud Security	With businesses moving towards cloud solutions and cloud infrastructure, Cloud Security is important for both businesses and personal users.

MITIGATE CYBER RISK

Core Products

SKU	Product	Description
ThIRU-P-1ce-2023-2.0-APAC	ThIRU 1Ce	Identity Management
ThIRU-P-EDR-2023-2.0-APAC	ThIRU EDR	Endpoint Detection & Response
ThIRU-P-NMR-2023-2.0-APAC	ThIRU NMR	Network Monitoring & Response
ThIRU-P-IMR-2023-2.0-APAC	ThIRU IMR	Infrastructure Monitoring & Response
ThIRU-P-AMR-2023-2.0-APAC	ThIRU AMR	Application Monitoring & Response
ThIRU-P-DLP-2023-2.0-APAC	ThIRU DLP	Data Security
ThIRU-P-PHISH-2023-2.0-APAC	ThIRU PHISH	Phishing Protection
ThIRU-P-CRYPT-2023-2.0-APAC	ThIRU CRYPT	Data Encryption
ThIRU-P-SIRP-2023-2.0-APAC	ThIRU SIRP	Security Incident Response Plan

THIRU 1CE - LEADING IDAM SOLUTION

- AUTHENTICATION & AUTHORISATION
- IDENTITY LIFECYCLE
- ORGANISATION MANAGEMENT
- APPLICATION MANAGEMENT
- BUSINESS WORKFLOW MANAGEMENT
- USER BEHAVIOUR ANALYTICS
- REAL-TIME REPORTING

THIRU EDR- ENDPOINT SECURITY

- BLOCK RANSOMWARE AND BAD CODE
- MONITOR ENDPOINTS CONTINUOUSLY
- MITRE ATTACK PATHWAYS
- DEVICE HEALTH
- MAIL SCANNER
- USB LOCK
- REGISTRY CLEAN, OPTIMIZER, DRIVE UPDATE

THIRU NMR - NETWORK MONITORING & RESPONSE

- REAL-TIME PERFORMANCE METRICS
- AUTOMATIC DEVICE DISCOVERY
- INTELLIGENT ALERTS
- ISSUE DIAGNOSIS AND ROOT CAUSE ANALYSIS
- NETWORK MAPS
- CUSTOMIZABLE DASHBOARDS
- NATURAL SCALABILITY

THIRU IMR - INFRASTRCUTURE MONITORING & RESPONSE

- REAL-TIME PERFORMANCE METRICS
- AUTOMATIC DEVICE DISCOVERY
- INTELLIGENT ALERTS
- ISSUE DIAGNOSIS AND ROOT CAUSE ANALYSIS
- NETWORK MAPS
- CUSTOMIZABLE DASHBOARDS
- NATURAL SCALABILITY

THIRU AMR - APPLICATION MONITORING & RESPONSE

- WEBSITE MONITORING
- WEB TRANSACTION MONITORING
- WEBSITE DEFACEMENT DETECTION
- WEB APPLICATION FIREWALL
- HTTP MONITORING
- SSL CERTIFICATE MONITORING

THIRU DLP - DATA LEAKAGE PREVENTION

USER: LOGIN AA, MFA, OTP, VAULT ACCESS, FOLDER ACCESS, FILE ACCESS.

APPLICATION: SECURE ACCESS & DATA, SECURE STORAGE OF THE CREATED DIGITAL ASSETS IS A KEY FEATURE OF THE SOLUTION.

DATA: ON SAVE CLASSIFY, ENCRYPT, VERSION.

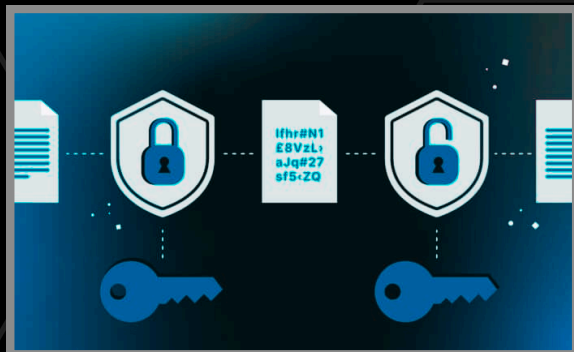**CLOUD USAGE:** VAULT STORAGE, ENCRYPT FOLDER, TIME STAMP & LOG USER AUDIT REPORT.
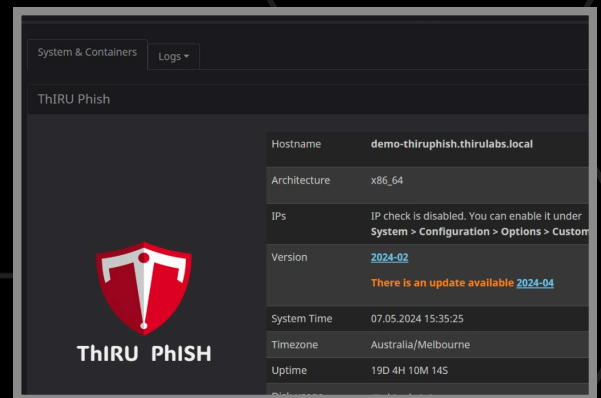
EMAIL: SCAN, LOCK AND PROTECT.

DEVICE: USB, MOBILE DEVICES & EDR.

THIRU PHISH

- EMAIL CLIENT PROTECTION
- EMAIL GATEWAY PROTECTION
- REAL-TIME THREAT DETECTION
- ANTI-SPOOFING MEASURES
- URL LINK SCANNING
- ATTACHMENT ANALYSIS
- SIMULATED PHISHING CAMPAIGNS

System & Containers	Logs ▾	
ThIRU Phish		
	Hostname	demo-thiruphish.thirulabs.local
	Architecture	x86_64
	IPs	IP check is disabled. You can enable it under **System > Configuration > Options > Custom**
	Version	2024-02 There is an update available 2024-04
	System Time	07.05.2024 15:35:25
	Timezone	Australia/Melbourne
	Uptime	19D 4H 10M 14S

ThIRU PhISH

THIRU CRYPT- DATA ENCRYPTION

- DISK ENCRYPTION
- FILE ENCRYPTION
- CLOUD ENCRYPTION
- KEY MANAGEMENT
- CROSS-PLATFORM COMPATIBILITY
- SECURE DELETION

THIRU SIRP - SECURITY INCIDENT RESPONSE PLATFORM

- IT HELP DESK
- ASSET MANAGEMENT
- PROJECT MANAGEMENT
- ADMIN MANAGEMENT

ThIRU SIRP

Security Incident Response Platform

⬇ On-premises   ☁ Cloud

THIRU VAS - VULNERABILITY ASSESSMENT SCANNER

- DISK VULNERABILITY ASSESSMENT
- OPERATING SYSTEM ASSESSMENT
- FILE INTEGRITY CHECKING
- REAL-TIME MONITORING
- CUSTOMIZABLE SCANNING PROFILES
- AUTOMATIC UPDATES
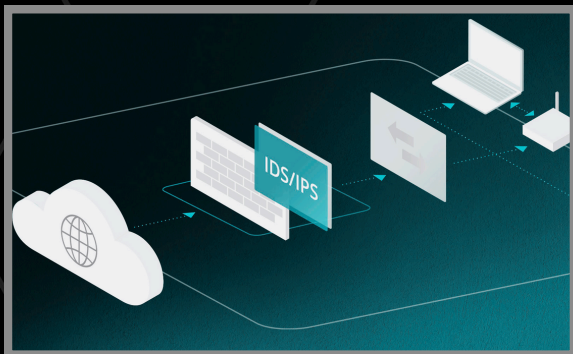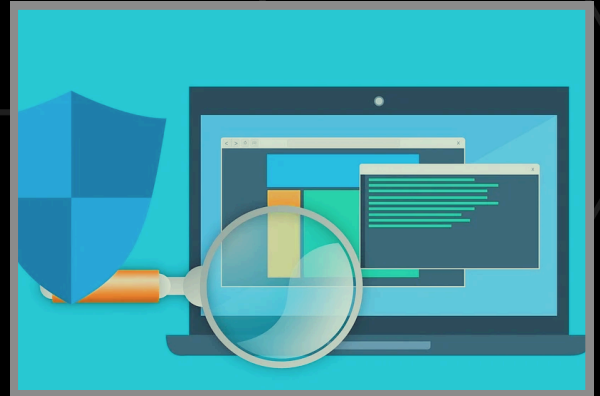
THIRU IDPS - INTRUSION DETECTION & PREVETION SYSTEM

- REAL-TIME INTRUSION DETECTION
- BEHAVIORAL ANALYSIS
- ANOMALY DETECTION
- PROTOCOL ANALYSIS
- CUSTOMIZABLE RULE SETS
- THREAT INTELLIGENCE INTEGRATION

CONTINUOUS MONITORING & ORCHESTRATION

NETWORK SECURITY	Endpoint Security Solutions		//SCAN NETWORK
Privilege Access Management	ThIRU SIEM	Threat Intelligence	Vulnerability Management
	SIEM	Cyber Threat INTELLIGENCE	
Application Security	Attack Matrix	Infrastructure and Cloud Security	Penetration Testing
	Plan your strategy / Assess and close gaps / Build your defense / Find solution methods / Monitor attack trends / Determine threats / Reference as a guide		PENETRATION TEST

Managed Security Services

THIRU ZERO TRUST PLATFORM

Core Service
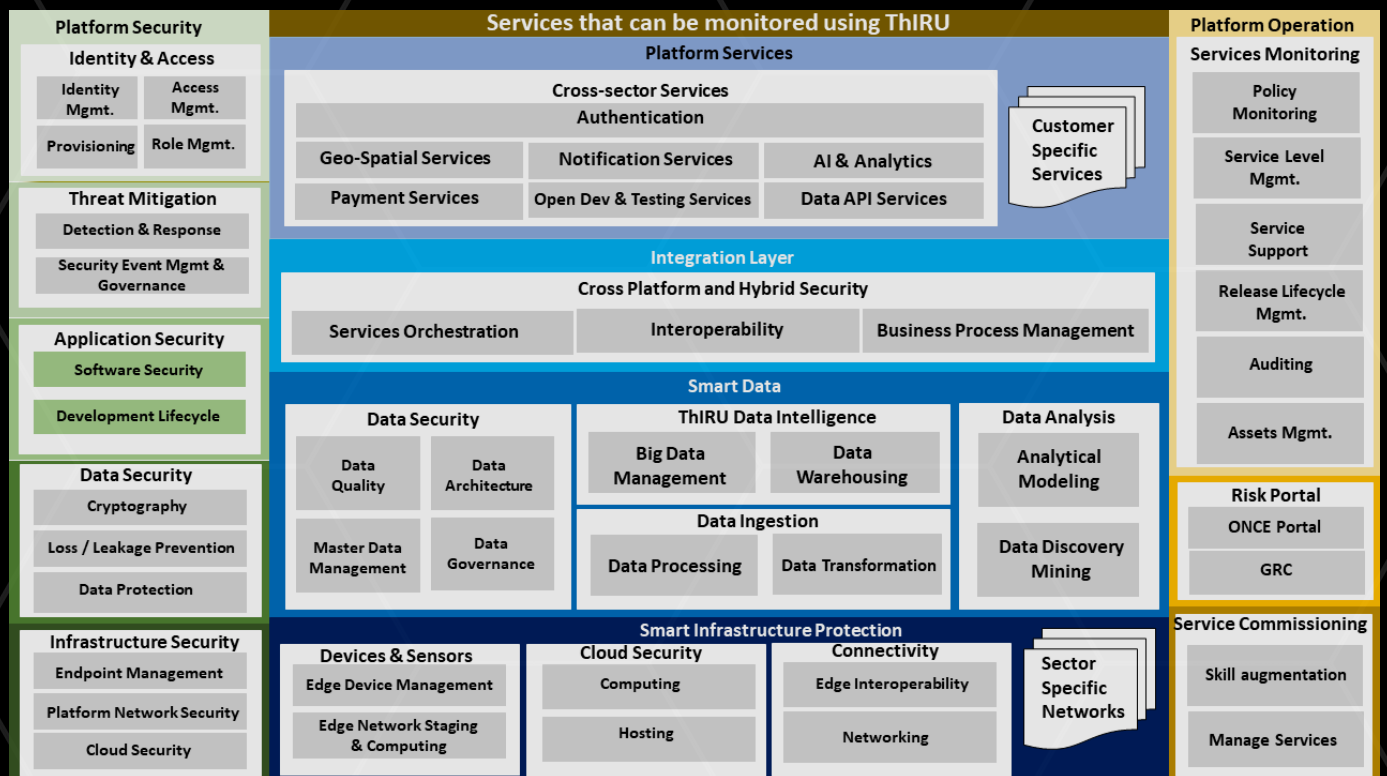
SKU	Product	Description
ThIRU-S-ORCH-2023-2.0-APAC	ThIRU Orchestration	Infrastructure and network orchestration including automatic patching
ThIRU-S-FOREN-2023-2.0-APAC	ThIRU Forensics	Law enforcement investigations
ThIRU-S-NOC-2023-2.0-APAC	ThIRU NOC Services	NOC Services
ThIRU-S-SOC-2023-2.0-APAC	ThIRU SOC Services	SOC Services
ThIRU-S-ZTW-2023-2.0-APAC	ThIRU ZTW	Zero Trust Workshops
ThIRU-S-ZTA-2023-2.0-APAC	ThIRU ZTA	Zero Trust Assessment

**Transport
& Infrastructure**

**Financial
services
Banking
Insurance
Investment
Houses**

**Government
Departments
Agencies
Statuotory
authorities**

**Critical
Infrastructure
Electricity
Water
Airports
Infrastructure
Telecommunications**

**Health
Hospitals
Community centres
Field emergency**

**Defense
Airforce
Land force
Navy**

AUSTRALIA

NEW ZEALAND

UAE

QATAR

INDIA

SURAKSHA PTY LTD.
305, 65 VICTOR CR
NARRE WARREN VICTORIA
AUSTRALIA 3805
Email : info@suraksha.com.au
www.thirulabs.com

Thiru Labs

suraksha
INFORMATION SECURITY