

SECURITY USE CASES & SOLUTIONS FOR WORK FROM HOME

Indian Start-ups

Compilation of capabilities of
Indian start-ups for securing
WFH environment



National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

A JOINT INITIATIVE BY



Ministry of Electronics &
Information Technology
Government of India

Index

| | | | |
|----------------------------------|-----------|--------------------------------|-----------|
| Introduction | 03 | Hypermine | 34 |
| Survey | 04 | Infinity Labs | 35 |
| Product Overview | 06 | Innefu Labs | 36 |
| 42 Gears | 09 | InstaSafe | 37 |
| Accops System | 11 | LTS Secure | 38 |
| Arishti Systems | 13 | Odyssey | 41 |
| AShield | 15 | ProgIST | 42 |
| Authbase | 16 | Seclore | 44 |
| Block Armour | 17 | SecPod | 45 |
| CloudCodes | 18 | Sectona | 47 |
| CloudSEK | 19 | SecureBlink | 48 |
| Cyberinc | 21 | Secure ID | 49 |
| Cyquirex | 23 | SecurelyShare | 50 |
| Data Resolve | 25 | Skynet Softech | 52 |
| DNIF | 27 | Smokescreen | 54 |
| Ensurity | 28 | Togglenow | 56 |
| Flexible IR | 30 | Wi-Jungle | 57 |
| Foresiet | 31 | About Us | 59 |
| Fortytwo | 32 | | |
| GajShield | 33 | | |

Introduction

Amid the fear of contagion, working from home has become the new normal for many professionals.

Fortunately, in this increasingly connected world, professional commitments can be managed virtually. However, with huge rise in the number of employees working remotely, it is of vital importance that we also take care of our cyber hygiene and be productive simultaneously.

As organizations grapple and brace this new normalcy, following are some of the Indian security product companies that can assist you in this journey.

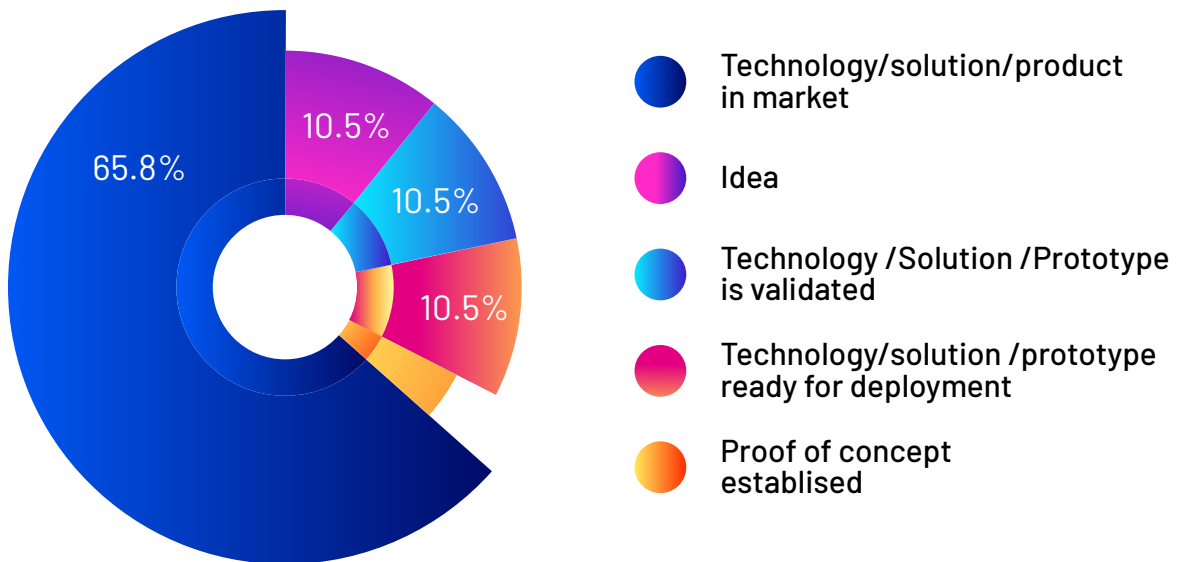
National CoE scouted for innovative technologies and security solutions for WFH which may emerge in the coming times and can be deployed immediately or in the near future. The purpose of the compilation is to create visibility of the innovation and efforts made in this area, increase the awareness about the ideas & solutions to solve the problems of the new paradigm, enhance the market potential, explore opportunities for the investment and engage with govt. start-up initiatives targeted at the COVID-19 pandemic.



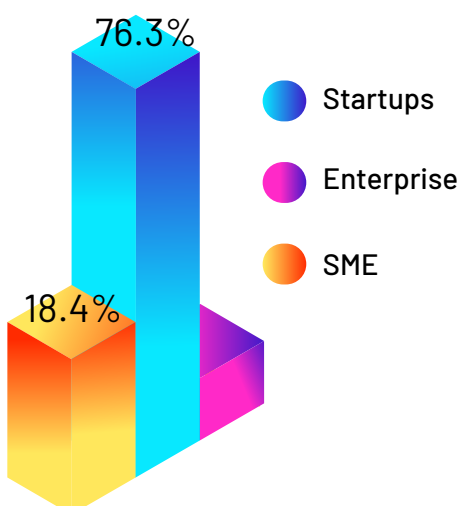
Survey

National CoE conducted a survey consisting 16 questions to understand the WFH security idea/solution of a start-up along with their stage of development. The survey received great enthusiastic participation from the industry. A total of 39 entries were received from various IT hubs in the country, namely Delhi-NCR, Bengaluru, Hyderabad, Mumbai, Pune to name a few. The detailed responses can be seen below.

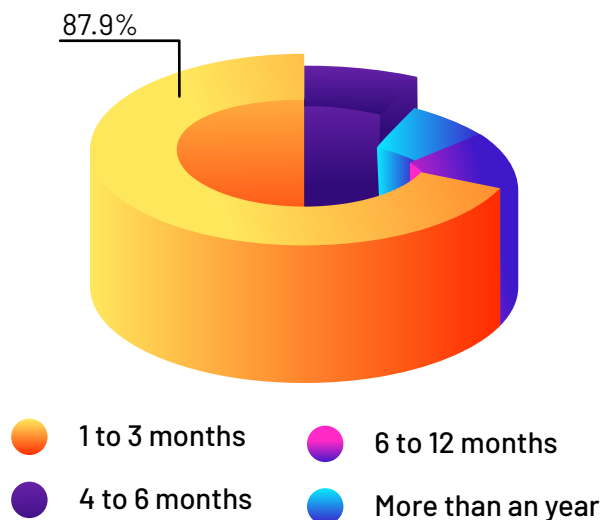
Stage of Start-up (WFH Security Product/Technology)



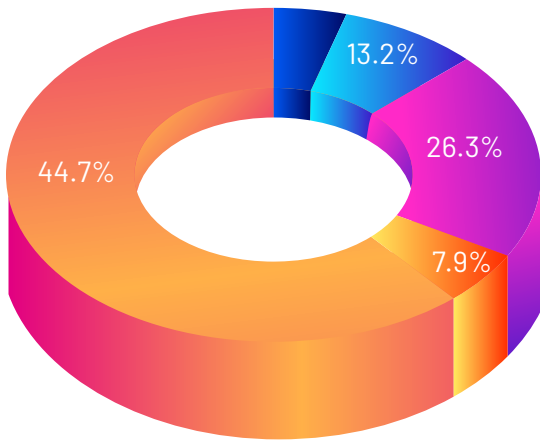
Nature of Company



Approximate time to market the product

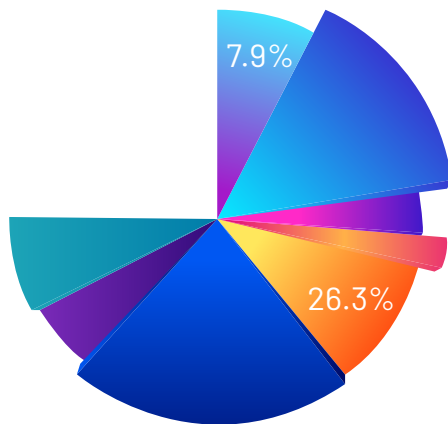


Stage of Startups



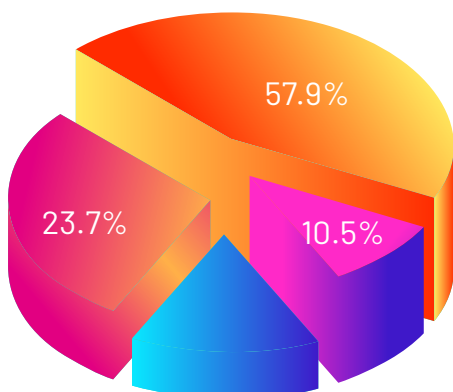
- NA
- Revenue generating start-up
- Growth stage start-up
- Idea/technology/prototype ready but start-up not registered
- Registered start-up

Use Case/Problem being solved by company



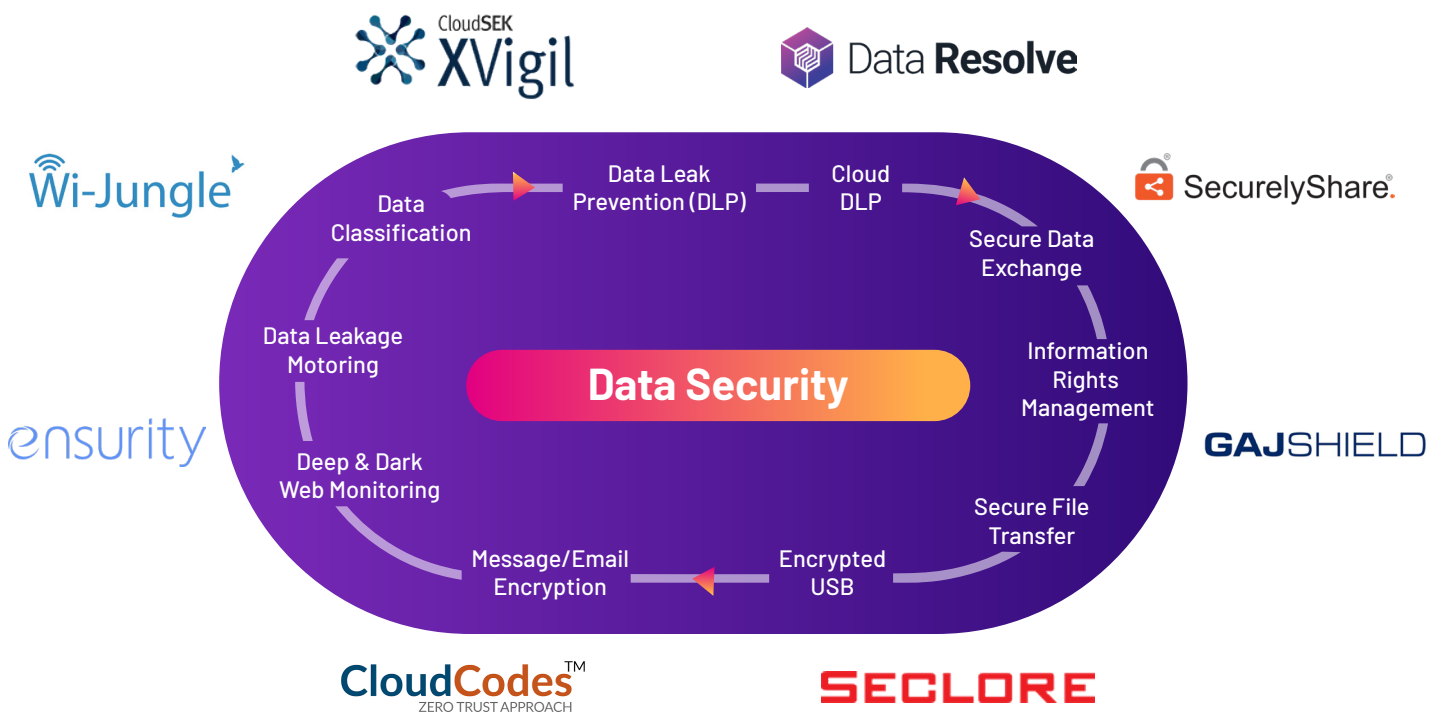
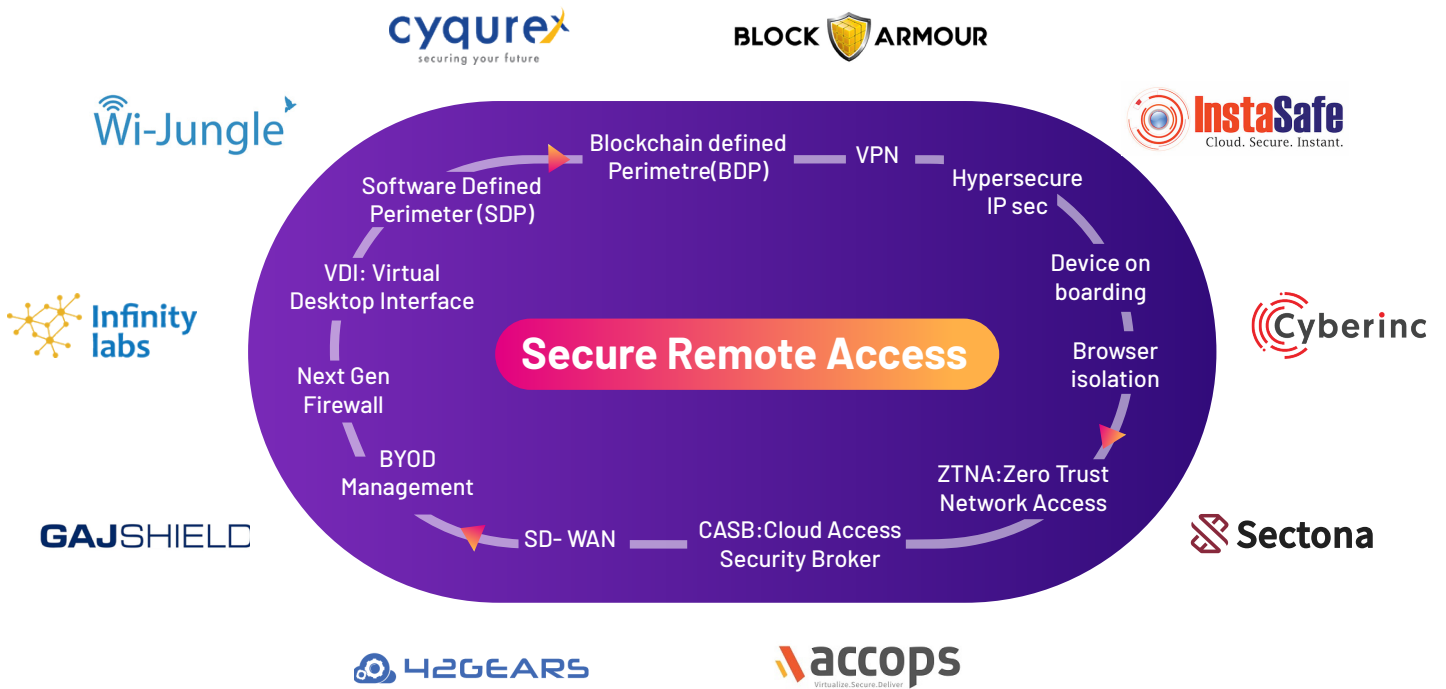
- Securing the BOYD connections
- Security in multi cloud environment
- Cloud access provisioning
- Monitoring
- Data Security
- Access Control
- Identity Management access provisioning
- Secure network access provisioning

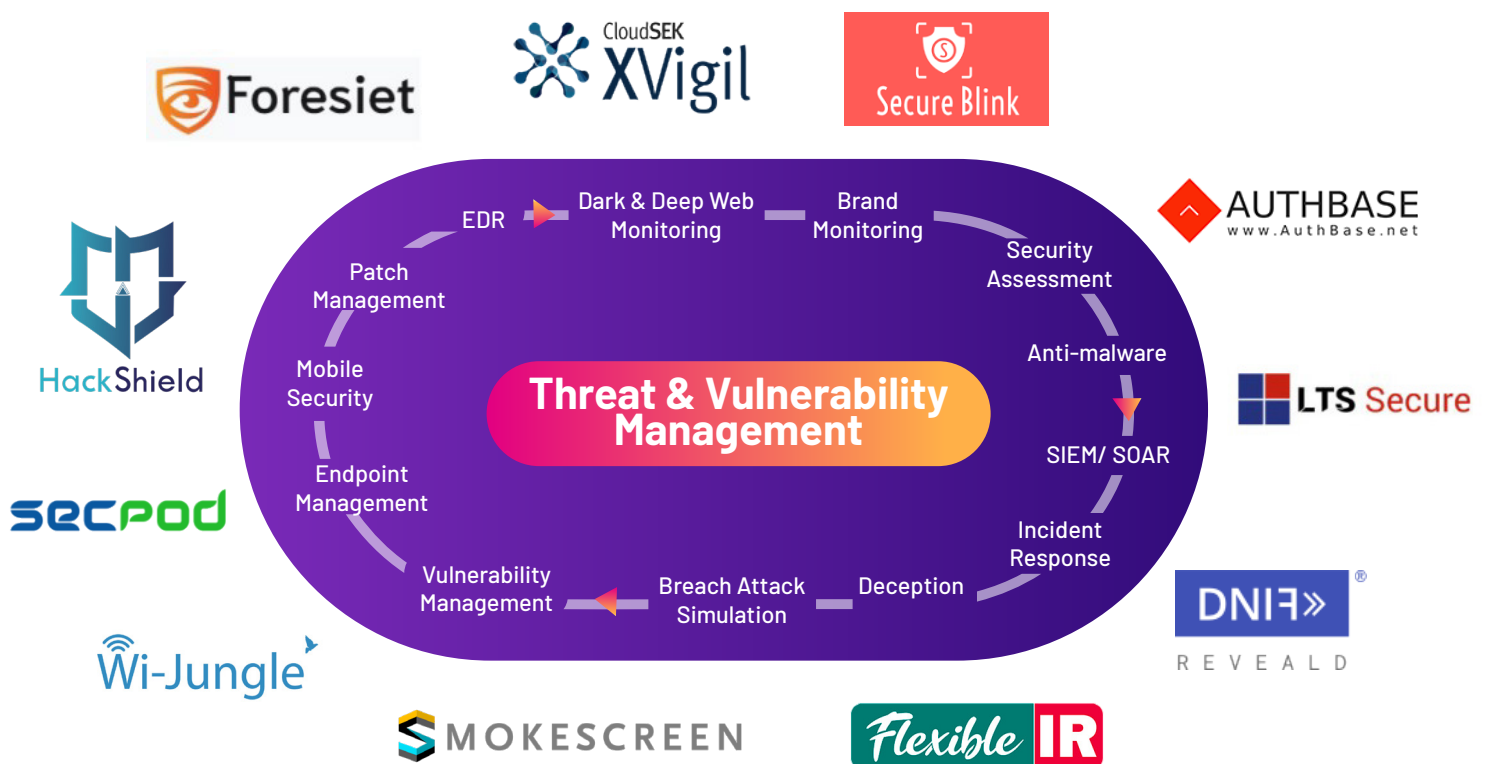
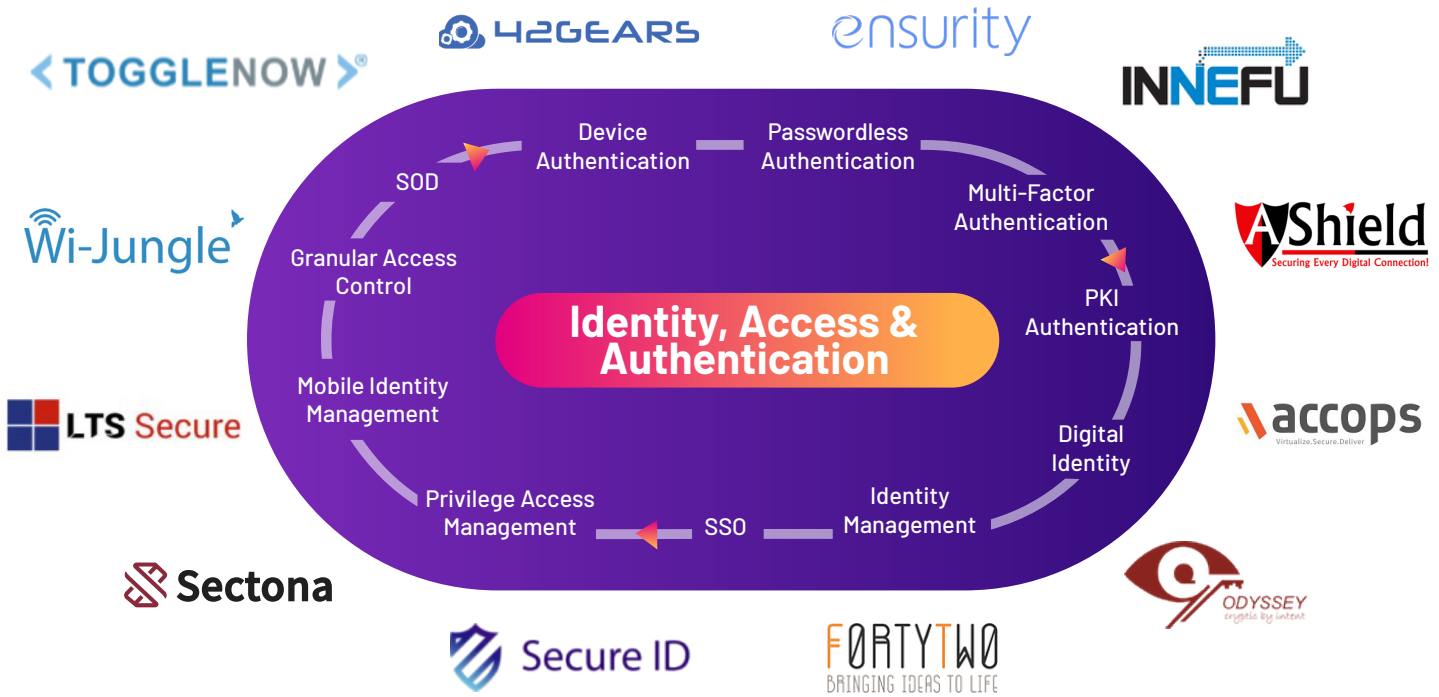
Investment Stages

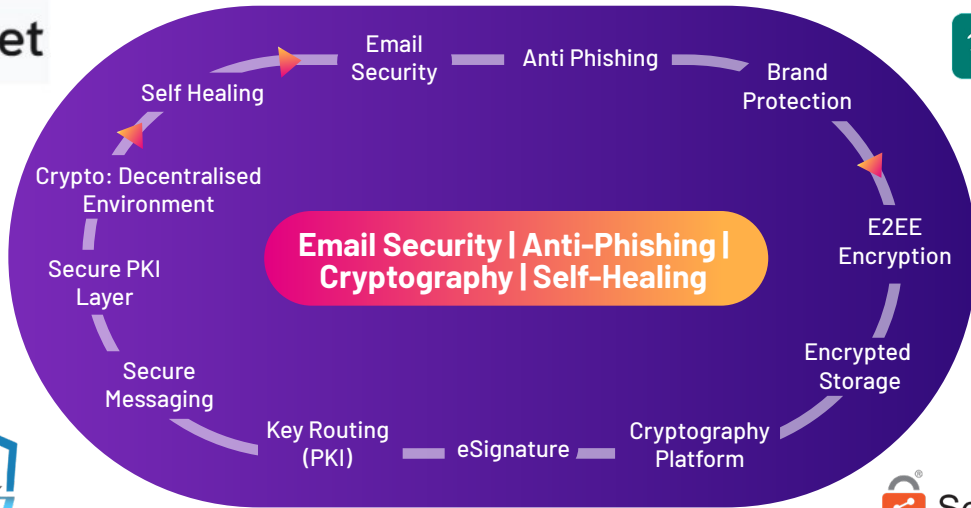


- Bootstrapped
- Seed/Angel investment
- Series A
- Series B and beyond

Work From Home Security: Indian Cyber Security Companies









Mobile Device Management | Mobile Application Management | Mobile Content Management | BYOD | Mobile Identity Management

 **Location:** Bengaluru



Stage of Company
Growth Stage Start-up



Solution Domain
Mobile Device Management



Stage of Investment
Bootstrapped

DSCI's Comment

Features like remote device troubleshooting, ability to push certificates to a device for additional security, device health monitoring is the need of the hour for ensuring security of mobile and BOYD devices connecting remotely to the enterprise network.

Mobile Device Management

- Remotely manage and secure the device fleet
 - a. Device Enrolment
 - b. Device Provisioning
 - c. Device Grouping
 - d. Device Health Monitoring
 - e. Location Tracking
 - f. Device Security; remote locking and pushing password policies.

Mobile Application Management

- a. Application Distribution
- b. Enterprise App Store
- c. Application Management

Mobile Content Management

- a. Content Delivery
- b. Content Security using containerization.
- c. Content Removal; remote wiping of data.

Bring Your Own Device

- a. Email Configuration of enterprise.
- b. VPN Configuration
- c. Wi-Fi Configuration

Mobile Identity Management

- a. Single Sign- On
- b. Certificate Management
- c. Device Enrollment
- d. Self-service Portal

Deployment

- Cloud Service
 - a. No server installation is required.
 - b. Enroll devices in minutes.
 - c. Data storage and cloud backup.
- On-Prem
 - a. Install SureMDM on the servers.
 - b. Higher level of safety and security.
 - c. Maintain organizational data policies.



HySecure gateway | HyWorks Enterprise |
HyWorks Enterprise in cloud | HyDeska

 **Location:** Pune



Stage of Company

Growth Stage Start-up



Solution Domain

Identity and Access
Management



Stage of Investment

Bootstrapped

DSCI's Comment

Desktop-as-a-Service solution with secure VDI facility not only for employees, but also for third party vendors and contractors enhances resiliency quite significantly. Also, direct access to internal applications using application tunnels, enabling zero-trust based access, and adds a layer of security.

HySecure gateway advanced edition with HyLite VPN

- HySecure gateway:
 - a. Enables a user to use a personal device to connect to the office network.
 - b. User can access internal web apps and servers through VPN.
 - c. Endpoint control
 - d. MFA
 - e. Enable device restrictions based on identity & health.

HyWorks Enterprise with HyID: virtual apps and VDI

- HyWorks Enterprise:
 - a. Users can use a personal device to connect to virtual apps, session-based desktop and personal virtual desktop.
 - b. Client and Clientless based access. Thin client: Linux based service.
 - c. VM provisioning and life cycle management.

Accops DaaS: desktop as a service HyWorks in cloud

- HyWorks Enterprise in cloud.
 - a. User session recording.
 - b. Encrypted VM
 - c. Desktop as a service.

HyDesk: live USB

- A Secure Linux based OS for making liveOS, running on a USB device.

Deployment

- On-prem and on cloud.



Arishti: AI and quantum cryptography based secure messaging application

 **Location:** Pune



Stage of Company

Registered Start-up



Solution Domain



Quantum Secure
Messaging App



Stage of Investment

Bootstrapped

DSCI's Comment

Quantum Secure Messaging App will help organizations communicate securely in upcoming post quantum world.

AI and quantum cryptography based secure messaging application

- Hyper Secure Messaging Application which is a security centric and privacy preserving product for organizational internal messaging.
- Uses Quantum safe random number generation algorithms for secure encrypted conversations.
- Application also provides hidden vault storage for sensitive messages or data.
- Application can also be used in remote areas using the Tetra connections.
- AI-based face aliveness detection which guarantees the user's identification, priority-based security levels, Time to Live, Message hiding, message poll system, etc.
- Follows least privileges; hence all the features are highly configurable and based on user needs, features can be activated.
- Secured screen sharing is an added feature using both mobile and web applications.
- The application logs the metadata information for cybercrime investigations.
- Application developed using National Cyber Safety and Security Standards (NCSS) for tracking data breaches when needed.

Deployment

- Mobile and Web based application.





Authenticator App based solution

 **Location:** Bengaluru



Stage of Company

Revenue Generating
Start-up



Solution Domain

Multi Factor Authentication,
Identity & Access
Management, AI/ML Based
Threat Intelligence



Stage of Investment

Pre/Series A
investment

DSCI's Comment

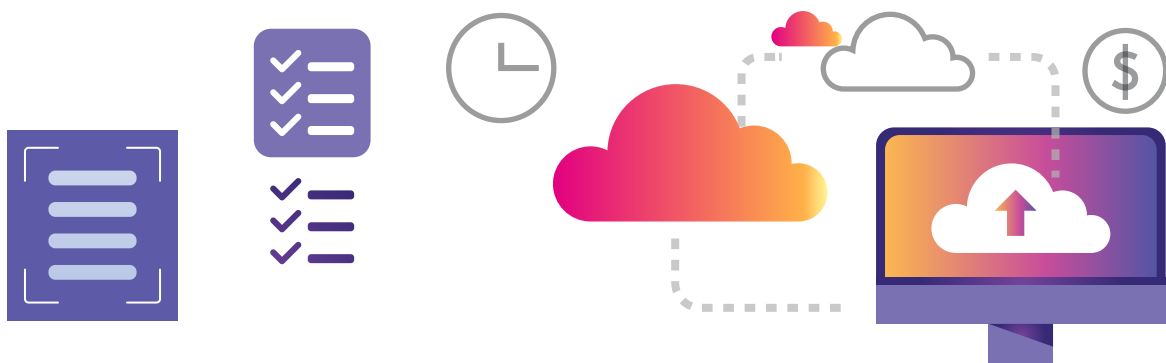
Authentication using quantum resistant crypto offers highly secure and reliable on-boarding of users and devices.

AShield

- AShield Authentication uses quantum-resistant encryption.
- Detects unique users and devices
- Overcomes user friction and negates security vulnerabilities associated with passwords and SMS based OTP which are compromised by devices infected with advanced Malwares.
- Offers a registration and authentication method with non-reusable, dynamic, and secure crypto shares.

Deployment

- Single API based integration, supports Cloud, On-Prem and Hybrid Deployment options.





AI based Signatureless Antivirus Solution

 **Location:** Hyderabad



Stage of Company

Revenue Generating
Start-up



Solution Domain



Signatureless
Anti-Virus solution



Stage of Investment

Bootstrapped

DSCI's Comment

Antivirus solution to avoid sophisticated signatureless and malware-free attacks.

AI based Signatureless Antivirus solution

- AI-based antivirus which identifies and mitigates attacks without rules and signatures and protect networks by reducing their attack surface.
- Prevents both malware and malware free attacks. Protects against Zero-Day exploits.
- Uses behavioral whitelisting to identify and mitigate threats and reduce the time taken by security teams to act.

Deployment

- Stateless and modular product so that it can adapt any platform, technology and environment. Plug and play product.



BLOCK ARMOUR

Secure Shield

 **Location:** Mumbai



Stage of Company

Revenue generating start-up



Solution Domain

Secure Access using SDP and Blockchain and Digital ID's



Stage of Investment

Bootstrapped

DSCI's Comment

Zero Trust approach using SDP and BDP, enables secure and compliant remote access not only to the employees but also to the IT administrators and external vendors.

Secure Shield: Blockchain based Zero Trust security model

- Provides secure RDP access to User Desktops within the Corporate LAN from authenticated and authorized remote users and computers.
- Harnesses Software Defined Perimeter (SDP) architecture enhanced with Blockchain Technology to deliver a Zero Trust security model called Blockchain Defined Perimeter (BDP).
- Using a Blockchain-Defined Perimeter, Block Armour renders an enterprise's most critical servers and resources invisible to external hackers.
- Creates digital IDs on the blockchain.
- Leverages multi-factor authentication by assigning digital IDs, not only to users but also to each device registered on the network.

Deployment

- Secure Shield can be deployed in agent or agentless mode. Agentless mode consists of a Secure Shield gateway through which access is provisioned and enforced.

Cloud Access Security Broker Solution

 **Location:** Pune



Stage of Company

Growth Stage Start-up



Solution Domain

Identity and Access
Management, Host
Based Security



Stage of Investment

Seed/Angel investment

DSCI's Comment

Shadow IT controls, Cloud DLP, email DLP, and Web Filtering plays a vital role in making the business leak proof when working from home and outside the organization network.

Cloud Access Security Broker (CASB) solution

- Provides access control that prevent unauthorized end-users from accessing confidential files and data on any internet browser. Only one browser may be used to ensure policy management.
- The program manages Google Chrome using Google admin chrome management console and pushes applications and extensions through it. Organizational unit-based granular control policies are also easily rolled out.
- SSO: Mobile compatible single Sign-On allows one-click access to all cloud applications using a single ID and password.
- DLP: Enables the IT admin of the organization to set up policies through the CloudCodes CASB dashboard to monitor, track and prevent business data.
- Identity Management: Controls the access to resources within the enterprise system by incorporating user policies and restrictions with the verified identity.

Deployment

- Deployed over the cloud.



XVigil: Digital Risk Monitoring Solution

 **Location:** Bengaluru



Stage of Company

Growth Stage Start-up



Solution Domain

Monitoring Solution,
Threat Intelligence



Stage of Investment

Series A

DSCI's Comment

Deep and dark web monitoring capabilities that include Source Code Leak Monitoring and Confidential Data Leak Monitoring with real-time alerts would help companies manage the security of their increasing digital footprint stemmed due to the pandemic outbreak.

XVigil

- Digital Threat Protection, Information Security, and Dark Web Monitoring with AI-based Security dashboard provide specific, actionable, and timely warnings analytics and actionable intelligence, needed to tackle external threats, by deploying comprehensive security scans and monitors.
- XVigil first gathers millions of data units from online sources and underground discussions. This raw data is filtered for noise, false positives, and anomalies, using a powerful AI engine. After which it is indexed, parsed, checked against the historical data lake, and mapped to clients' assets.

Solutions:

- a. **Cyber Threat Monitor:** Cyber Threat Intelligence includes real-time social media, surface web, dark web monitoring, credential disclosure, data leakage identification besides monitoring the web. Conducts Deep and Dark Web Monitoring, Detects Credential Disclosure, Data Leakages, Source Code Leaks, Hiring Scams, 3rd Party Data Leaks, email compromise attacks, Credit Card/Debit Card leaks, etc.
- b. **Brand Monitor:** The brand scan helps to combat fake pages, impostors, rogue applications, and domains that could harm the brand image. Conducts Fake Domain Monitoring, prevents Domain Phishing Attempts, finds Rogue Applications.

c. Infrastructure Monitor: Monitors internet exposed infrastructure, curates a list of all asset-inventory and then periodically monitors misconfigurations, and potential data leakages.

Web Application Scanner checks for security holes in APIs periodically. Checks for Misconfigured Cloud Storages, conduct port scanning.

Deployment

- SaaS-based easy-to-use platform
- Non-invasive technology





Isla Isolation Platform | Secure Web Gateway

 **Location:** Mumbai



Stage of Company

Growth Stage Start-up



Solution Domain

Endpoint Security,
Monitoring Solution



Stage of Investment

Series B and beyond

DSCI's Comment

As applications designed for a closed corporate network are opened for remote access, zero-trust security model for browser isolation and secure web gateway, would neutralized threats quite effectively.

Isla Isolation Platform

- Proactively stops web, email, and document-based threats using Zero Trust Security.
 - a. Using a Zero Trust model, Isla isolates all code coming through the web browser and neutralizes threats without the need for detection or compromising productivity.
 - b. Isolation-based security model doesn't rely on an alert-driven approach to protection, which greatly reduces the load on security teams, making them more efficient, more productive and more forward-looking.

Secure Web Gateway

- The Secure Web Gateway function allows the user to set policy-based controls based on URL classification for an added level of protection while also enabling enforcement of acceptable use policies.

Supports several core use cases such as:

- a. Web-based threats such as drive-by downloads, malvertising, zero-day attacks, etc.
- b. Document-based threats such as steganography attacks, rootkits, etc.
- c. Email-based threats such as phishing, spear-phishing, etc.

- d. Ransomware or crypto-mining attacks.
- e. URL-based blocking
- f. Enforce & report on acceptable use policies (AUP).
- g. Visibility & monitoring of web applications.

Isla helps meet PCI, HIPAA, MPAA, and other regulatory compliance requirements.

Deployment

- On-prem, On cloud or Hybrid.





SAIFE | GigaTrust | Command Control
Operations Platform (CCOP)

 **Location:** Bangalore



Stage of Company

Revenue generating
start-up



Solution Domain

Monitoring Solution



Stage of Investment

Series B and Beyond

DSCI's Comment

Establishes server to server communication and enables remote access to a virtual private cloud deploying modern approach to security, Software Defined Perimeter, for creating a secure, encrypted, hidden channel for data.

SAIFE

- Creates a zero-trust model with Software defined perimeter approach.
- Establishes access only to those data or applications that the user is entitled to access, enforcing agile perimeters in real-time.
- Creates individualized network segments for each user based on attributes such as their identity, device profile, location, and authentication method.
- Creates secure tunnels through the Internet by its dynamic perimeter overlay (DPO) network.
- Creates a "Virtual Air Gap" that provides protection of physical airgap while giving the ability to access these air-gapped assets from anywhere in the world.
- Eliminates the need of DMZs- ITSystems can be securely accessed be it on the cloud, in DC or at the customer location without the need to deploy them in the DMZs.
- Provides port level access depending on roles and responsibilities.
- Compliance reporting and provides visibility to what the users are accessing and how long (including screen capture features).
- Needs VMs for a touchless, remote deployment that is highly scalable and eliminates the need to manage complex firewall rules, networking routes, VLANs.

GigaTrust

- Endpoint email security and document in-use protection for on-prem private cloud or private cloud-based deployments for Windows, iOS and Android devices.
 - a. Enables intellectual property protection and confidentiality.
 - b. Applies and enforces security permissions down to the digital content level, protecting content from misuse throughout the entire lifecycle.
 - c. Includes a suite of patented security content management services that provides the benefits of encryption and the ability for authors to control the use of assets—even after they have been delivered and opened.

Command Control Operations Platform (CCOP)

- Management tool for deploying and monitoring security tools.
 - a. Ensures that all data coming in through various cyber security products are monitored, analyzed using machine learning algorithms and IT admins are provided with actionable insights.
 - b. Provides APIs that allow other cyber security products to integrate with it.

Deployment

- Solution can be deployed in a public or private cloud, on prem, or via its SaaS-based multi-tenant environment.
- Deployed as SaaS






inDefend | MobSec

 **Location:** Gurgaon

 **Stage of Company**
Growth stage start-up

 **Solution Domain**
Behavior Analytics,
Monitoring solution

 **Stage of Investment**
Series A

DSCI's Comment

DLP, OCR for intercepting sensitive content leakage, incident alerting, user behavior analytics and employee productivity monitoring help protect information, even in unstructured form and ensure integrity of sensitive activities.

inDefend

- Insider Threat Management: User behavior analysis by monitoring activities and communication habits.
- Real-time Alerts: Incident alerts for any data exfiltration activity.
- Enforced Encryption: Multiple endpoints security with implemented encryption on external storage devices to restrict the use of sensitive information or files.
- Optical Character Recognition (OCR): Extracts text from images and processes them further to detect the presence of sensitive content like keywords, regular expressions, or file types with OCR.
- Data Leakage Prevention: Monitors, alerts, and/or blocks Emails, File Uploads, Attachments by its Secure Email Gateway approach wherein it provides a protection layer on the content going via corporate email to any third party.
- Monitors the sensitive activities.

MobSec

- Uses Cyber Intelligence to analyze the information flowing within and outside the company.

- a. Mobile Device Management: Custom and thorough monitoring over enterprise mobility.
- b. Mobile Application Management: Enables blacklisting and whitelisting of application by the administrators.
- c. Content Management: Keeps all the data secure in a different container and access to business-critical data through secure apps.
- d. Employee Productivity Monitoring: Monitors device usage logs to examine employee productivity .

Deployment

- inDefend server can be hosted on cloud, on-prem or on any cloud-based server provided by the customer.
- MobSec can be deployed on cloud or on-prem.





Next Gen SIEM solution with SOAR, UEBA, Security Analytics, Threat Hunting and AI/ML.

 **Location:** Mumbai



Stage of Company

Revenue Generating Start-up



Solution Domain

SIEM with SOAR, UEBA, Analytics, Threat Hunting and AI/ML



Stage of Investment

Bootstrapped

DSCI's Comment

Comprehensive analytics, log management SIEM solution with SOAR, and UEBA would be the most critical and desirable security capabilities in the new paradigm.

Next Gen SIEM solution with SOAR, UEBA, Security Analytics, Threat Hunting and AI/ML.

- Data analytics engine which performs essential tasks such as threat hunting, threat intelligence layering, manage compliance, build attack models and perform machine learning to detect outliers.
- Log Management: DNIF aggregates all the server logs and metrics into a centralized system in real-time. It lets the user experience real-time response for searches through massive data volumes and over long time periods.
- SOAR: DNIF integrates with detection and response products across the enterprise to automate the investigation, response and mitigation process to a large extent. DNIF connects these products with a common API backplane that lets the user build scenario-based playbooks and reduce the possibility of "handlers' oversight" during investigation.
- Security Analytics: Streamlines the security investigations with the ability to detect threats in real time, perform efficient multi-step analysis and power the investigations with machine learning and smart automation.

Deployment

- Soft appliance that can be installed on any commodity or virtual machines.
- It supports on-prem and multi-tenant Deployment.



Secure Identity & authentication | Secure communications over smartphones | Encrypted USB storage



Location: Hyderabad



Stage of Company

Revenue Generating Start-up



Solution Domain

Identity and Access Management, Hardware Security Key



Stage of Investment

Seed/Angel investment

DSCI's Comment

In the borderless security paradigm, the security of data on portable media would be critical use cases. Specialized hardware for security attracts the attention of the mangers of security.

Ensuring designs and manufactures specialized secure hardware, software, and mobile application solutions.

Secure Identity and Authentication

- Single Biometric Key for Password less/2FA Login on FIDO2/WebAuthn-enabled multiple websites.
- Software based password less access with bidirectional authentication.

Secure communications over smartphones

- Secure Messaging Suite for Closed-User-Groups, On-Prem/Cloud
- Protects messages and calls with true end-to-end encryption
- Encrypted Message – each message is encrypted with a new Key
- Evaporated Message – erases at both source & destination after reading
- File Sharing & Tracking – know who else accessed the file as an owner

Encrypted USB storage

- Encrypted USB Storage device with Fingerprint Biometric Authentication will ensure data security and confidentiality. Encrypted fingerprint templates will never leave the device. The device also supports read only bootable operating system where VPN and VDI clients can be integrated to create a secure connection isolating the user's system so that no malware comes into the session.

Deployment

- FIDO2 Keys are hardware-based authenticators, very easy to configure. Your fingerprint becomes your password.
- Easy to deploy software which gives seamless passwordless access to multiple accounts
- Messaging suite is available on app stores and works in closed user group.
- These are hardware-based solutions which can be customized to the needs of the user.





Platform for Playbook Lifecycle Management

 **Location:** Mumbai



Stage of Company

Revenue Generating
Start-up



Solution Domain

Incident Response
management



Stage of Investment

Seed/Angel Investment

DSCI's Comment

Incident Response playbooks provide insights on how each task in an incident must be handled independently making it more useful when employees are working remotely.

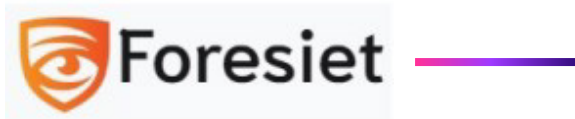
Platform for Playbook Lifecycle Management

- Playbook for all types of cyber attacks.
 - a. Playbook for social media attack
 - b. Playbook for DDoS attack
 - c. Playbook for system intrusion
 - d. Phishing Playbook
- Handle incidents in a predictable & consistent manner.
- In accordance with operation processes & ITIL frameworks.

Deployment

- Web-based incident platform
- SaaS - based platform





Dark Web Intelligence | Breach Incident Response Platform | Brand Reputation |
Automated Anti-Phishing | Security Assessment | Self-healing

 **Location:** Bangalore



Stage of Company
Registered Start-up



Solution Domain
Threat Analytics,
Monitoring Solution,
Incident Response



Stage of Investment
Bootstrapped

DSCI's Comment

Continuous monitoring of the digital risk by techniques like brand monitoring, and breach incident response would enhance resiliency. Self-healing capability would be critical as an organization may not have full control of remote machine for timely actions.

Dark Web Intelligence

- Deep identity investigation for account takeover.

Breach Incident Response platform

- Breach and threat intelligence feed integration platform.

Brand reputation and risk profile

- Brand monitoring with faked domain monitoring and sentiments analysis.

Automated Anti-phishing platform

- Real-time Protection against phishing attempts and alerts.

Security Assessment

- Comprehensive assessment for evaluating security.

Self-healing

- As system with self-immunity.

Indigenous Cryptographic Platform

 **Location:** Noida



Stage of Company

Revenue Generating
Start-up



Solution Domain

Access Control



Stage of Investment

Seed/Angel investment

DSCI's Comment

Digital ID using cryptography for secure authentication and access would be crucial for securing information and identities in the WFH environment. Strong cryptography capabilities can solve many uses cases of security in the paradigm imposed by the pandemic.

Indigenous Cryptographic Platform

- Pi-Control platform is based on an indigenous cryptographic identity technology called I-AM[®].
- E2EE Secure Remote Access: Pi-Control Platform provides a Secure Remote Access technology (WFH Solution) which provides End to End Encrypted (E2EE) access to enterprise applications with granular control. This technology is highly scalable to tens of thousands of end points.
- Authentication and eSignature Services: Using I-AM[®] Cryptographic identity Pi-Control platform provides password less authentication, Multi Factor Authentication, eSignature, provable consent with very simple integration methodology. We support NO-CODE integration with AD and ADFS Multi factor Authentication.
- The Pi-Control E2EE Secure Remote Access Solution uses I-AM[®] Multifactor Authentication service for enterprise application access.

Deployment

- On-prem, cloud and hybrid deployment models.

Network Security Field

 **Location:** Mumbai



Stage of Company

Growth Stage Start-up



Solution Domain

Network Security



Stage of Investment

Bootstrapped

DSCI's Comment

Managing user access to critical data, enforcing data security policies, ensuring the confidentiality of all the data sent across the network by routing it through the head office firewall enables employees to work from home securely.

Network Security Field

- GajShield's Next Generation Firewall (NGFW) Appliances provides deeper visibility into various threats and performance inhibitors.
- Contextual Intelligence Engine, Machine Learning etc. for Intelligent Security Solutions combined with Advanced Deep Visibility for ultimate security.
- GajShield firewall appliances provide powerful & integrated protection, enhance user productivity, granular policy definition, zero-day protection providing pro-active security to networks, and delivers real-time protection against fast-moving threats like spyware, phishing, masked applications like Malware, Adware, P2P, Instant Messaging.
- With its Data Leak Prevention, GajShield firewall appliances not only protects from external threats, but also critical data from being leaked.
- Protects by using Deep Inspection of Application Data, Controlling Data Inflow and Outflow, Context Sensitive Data Leak Prevention, Blocking Data Types, File Extensions, File Content, Preventing Data Leak on SaaS Apps, Controlling Entry Points for advanced Security, Restricting Personal use.

Deployment

- Deployed as an UTM Box.



Hypersign | HyperPay | adhat.io

 **Location:** Bangalore, Pune



Stage of Company
Registered Start-up



Solution Domain
Cryptography, Identity
Management



Stage of Investment
Bootstrapped

DSCI's Comment

As the world is moving to decentralized computing, specially devised cryptography platforms would help build the applications securely.

Hyersign

- Based on Public Key Cryptography: Hypersign enables users to access decentralized environments with their existing login credentials.

HyperPay

- Based on the next generation Public Key Infrastructure, Hyperpay is built on top of Hypersign's secure PKI Layer to create a secure P2P payment system. Build secure, privacy-based payment systems with the Hyperpay protocol.

adhat.io

- The world's first decentralized peer-to-peer marketplace for digital content. ADHAT empowers users to freely buy, sell, track and trade images, video, eBooks, software and games as we do in the real world whilst protecting the rights and rewarding content creators.

Deployment

- Mobile App
- PKI capability
- Peer-to-peer content built on Blockchain.



INFlxxt: NextGen SD WAN solution

 **Location:** Noida



Stage of Company

Growth Stage Start-up



Solution Domain

Network access provisioning



Stage of Investment

Seed/ Angel investment

DSCI's Comment

Virtualizes WAN for safer and faster deployment without traditional MPLS/leased line cost using Software Defined Networking capability.

INFlxxt: NextGen SD WAN solution

- Management portal: a single pane of glass for configuration network management for cloud-hosted and on-prem solution.
- Zero-touch provisioning.
- User can define policies on portal.
- SD-WAN controller: Establishes and manages Secure virtual overlay to sites.
- Interprets the global policy according to the knowledge collected from the network
- Defines service chains to enable policy goals.
- Manages distribution of interpreted Policy to individual elements.
- Secured communication using IPsec encryption.

Deployment

- On-prem deployment over the network.



Stage of Company
Growth Stage Start-up



Solution Domain
Multi-factor authentication



Stage of Investment
Series A

DSCI's Comment

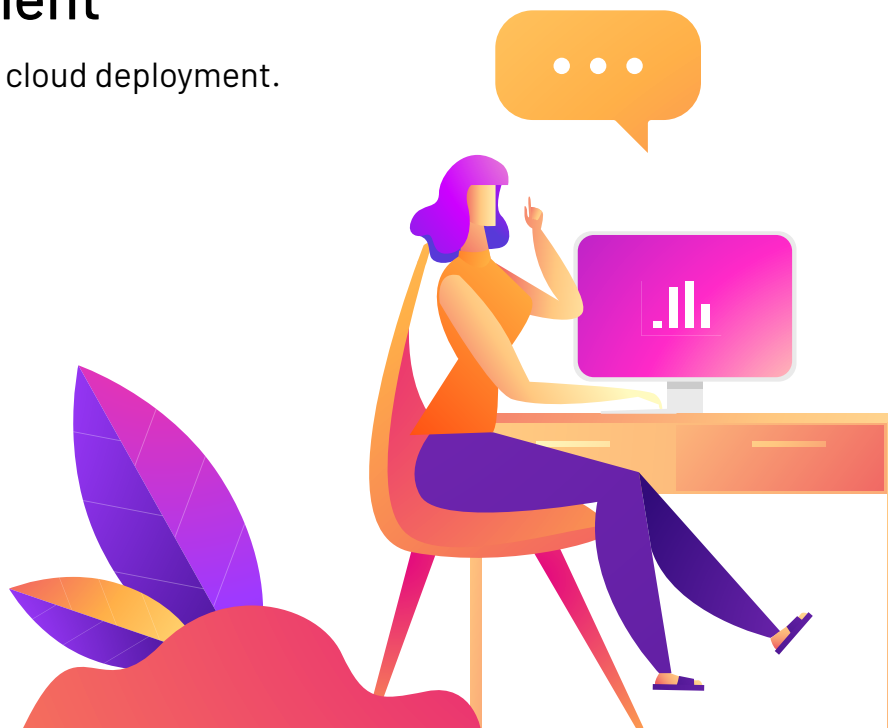
Two-factor authentication solution is essential for organizations to allow remote users to connect to their network for secure access and transmission of data.

AuthShield- MFA

- AuthShield is a unified authentication platform to authenticate every application in an organization. AuthShield can combine biometric on applications such as Windows Logon and web applications.
- MFA is supported on multiple form factors such as Hard Tokens, Soft Tokens, Biometrics, etc.

Deployment

- On-prem and cloud deployment.






InstaSafe Secure Access: Zero Trust Network Access solutions

 **Location:** Bengaluru

 **Stage of Company**
Growth Stage Start-up

 **Solution Domain**
Access Management

 **Stage of Investment**
Series A

DSCI's Comment

Zero Trust Network Access using SDP avoids remote access cyber threats by identifying the assets, improving visibility and granular access control.

InstaSafe Secure

- Based on the principle of Software Defined Perimeters (SDP) or 'Black Cloud' where the user and the device is verified before enforcing the application access.
 - a. The module of InstaSafe called Gateway is installed.
 - b. The gateway acts as the bridge between the applications and the users.
 - c. It is placed anywhere inside the network with only a private IP address and is not exposed to the internet.
 - d. It creates a tunnel to the InstaSafe controller.
 - e. Routes all user traffic destined to the applications protected by this gateway through that tunnel.
 - f. It provides privilege access management for complete control and verification of users and devices.
 - g. It provides capability for monitoring user behaviour and threat analytics.

Deployment

- It is delivered as a SaaS solution.



SIEM | CASB | Identity Management | Security Analytics

 **Location:** Pune



Stage of Company

SME



Solution Domain

User Entity Behavior
Analytics, Identity
Management, Visibility
Solution



Stage of Investment

Series A

DSCI's Comment

SIEM, CASB, identity management and Security analytics capabilities would not only help govern the remote access but also help in monitoring security.

SIEM

- Security Information and Event Management (SIEM), is a technology that provides real-time analysis of security alerts generated by network hardware and applications. Continuously monitors for all data center resources, anywhere in the enterprise.
- Receives real-time alerts on security or performance-impacting incidents.
- Automated compliance reporting.

CASB

- Secure mobile access for BYOD users:
Deliver applications and information to mobile devices securely so your BYOD users can access them anytime.
- Authorization:
Create sophisticated, context-based intelligent policies to deliver controlled access to resources with the GUI-based policy editor, using point and click, drag and drop operations.

- **Visibility:**
CASB provides a clear visibility across various cloud services that covers users, devices, applications, data, and actions.
- **Data Security:**
CASB helps implements data-centric security policies using controls such as encrypt, alert, block, tokenize, and audit.
- **Threat Protection:**
CASB prevents unwanted users and devices from accessing cloud services. CASB also covers User Behavioral Analysis (UBA) and Entity Behavioral Analysis (EBA) for determining anomalies in the network and threat intelligence formation.
- **Early threat detection:**
CASB has visibility of all the cloud applications, even the one using SSL encrypted connections which helps it in early detection of threat.

Identity Management

- **Role-based Provisioning:**
Create and manage roles assigned to users based on organizational need and structure such as job function, title, geo, etc.
- **Password Management:**
Ensure consistency across all applications and data stores, such as Active Directory and HR systems.
- **Synchronization and Reconciliation:**
Synchronization delivery guarantees enable roll-back if one or more remote systems are unavailable, for both on-demand and scheduled resource comparisons.
- **Self-Service & Profile Management:**
User self-service significantly reduces help desk costs and increases user productivity by automating password reset and ensuring compliance with a secure, centralized password policy.

Security Analytics

- **Identify New Privileged Accounts:**
LTS Secure helps to automatically monitor and report on the creation of privileged accounts and the elevation of permissions.

- Account Hijacking & Privileged Account Abuse:
Quickly detect compromised accounts and gain full visibility into threats associated with privileged accounts.
- Malware Detection & Lateral Movement:
Detect malware and other threat actors as they move laterally within your network and communicate with internal and external C&C servers.

Deployment

- LTS Secure deployed VSOC Box for centralization provided with a provision to automate some of the alarms where human eye is not required.





Xorkee -PKI solution

 **Location:** Chennai



Stage of Company
Enterprise



Solution Domain
PKI Technology



Stage of Investment
Series B and beyond

DSCI's Comment

Public key authentication and digital signatures provide fundamental security framework to communicate securely in the open world and infrastructure.

Xorkee -PKI solution

- Key routing service based on PKI framework: PKI Technology for (Authentication, Consent, Digital Signature, Data Encryption and Decryption in Transit).

Deployment

- SaaS based solution deployment.
- On-prem





Stage of Company
Growth Stage Start-up



Solution Domain
Threat Intelligence,
Email Security
Management



Stage of Investment
Bootstrapped

DSCI's Comment

Phishing cases are on the rise post outbreak of the pandemic. Protecting brand and countering phishing attacks need a special attention.

ProDMARC

- DMARC analytics platform, focused on protecting brands from mail-based spoofing & phishing threats.
 - a. Brand Protection: Blocks phishing emails.
 - b. Visibility: Gain visibility of unauthorized emails that might get sent from the user's domain.
 - c. Threat Intelligence: Actionable feeds to proactively block targeted attacks.

ProDiscover

- ProDiscover: Email based spoofing attacks are constantly mimicking the brand name. ProDiscover helps in identifying and blocking cousin and look-alike domains which may impact the stake holders.

ProPatrol

- ProPatrol: Facilitates reporting of phishing attacks that have bypassed all security controls to allow deeper forensic investigations.

ProPhish

- ProPhish: Simulation based solution to help identify and train employees who are susceptible to targeted phishing attacks.

Deployment

● Deployment on Cloud.



SECLORE

Enterprise Digital Rights Management

 **Location:** Mumbai



Stage of Company

Revenue Generating
Start-up



Solution Domain

Data classification,
Email Encryption
Solution



Stage of Investment

Series B and beyond

DSCI's Comment

When working remotely, organizations face difficulty in controlling sensitive email and data repositories going outside the traditional perimeter on unmanaged networks. Features like usage controls, rights management, channelizing the data repositories over public infrastructures would be useful.

Enterprise Digital Rights Management

- Labels the sensitivity level of a document.
- Secures and tracks sensitive documents.
- Visibility and streamlines compliance reporting.
- DLP solution automates detection, protection and tracking.
- Connects to Data Repositories (ECM, EFSS, ERP and file servers).
- Protects messages, attachments, and email content.
- Authentication and pluggable encryption technology.
- Connects to Analytics systems (SIEM, GRC).

Deployment

- Cloud-based deployment.



Saner Now | Saner Personal

 **Location:** Bengaluru



Stage of Company

Revenue Generating
Start-up



Solution Domain

Vulnerability management,
asset management, endpoint
detection and response



Stage of Investment

Bootstrapped

DSCI's Comment

Vulnerability management, Asset management and Compliance management, enable organizations managing their expanding exposure due to WFH and ensuring the compliance.

Saner Now

- Automate endpoint vulnerability and risk management to a daily routine. Saner helps keep endpoints secure by proactively assessing and remediating vulnerabilities.
 - a. Vulnerability management: Continuously identifies vulnerabilities, understand the risks, exploitation potential and mitigation.
 - b. Patch management: Apply operating system and wide variety of third-party application patches on Windows, Linux and Mac OS X. Automate the process.
 - c. Asset management: Discover and manage assets. Inventory of the applications and devices. Ensure efficient usage.
 - d. Compliance management: Comply with regulatory standards benchmark and stay compliant (PCI, HIPAA, NIST 800-53, NIST 800-171)
 - e. Endpoint detection and response: Detects and Responds to IoA (Indicators of Attack) and IoC (Indicators of Compromise).
 - f. Endpoint management: Manage the endpoints and ensure their well-being. Check the health status, deploy applications, control devices.

Saner Personal

- SecPod Saner is a lightweight, easy to use, an enterprise-grade security solution for proactively assessing and securing the personal computer. It identifies security loopholes and misconfigurations and remediates to ensure systems are secure.

Features:

- a. Identifies vulnerabilities in the applications and operating systems.
- b. Identifies common misconfigurations.
- c. Eliminates threats by proactively fixing vulnerabilities and misconfigurations.

Deployment

- Saner Now supports application deployment from an array of pre-defined software packages as well as applications and software packages that can be uploaded into the repository and manage. Saner Now agents can be deployed to endpoints.
- The flexible architecture of the Saner platform allows integration with other systems. The REST APIs expose access to all the data collected from the endpoints, threat, vulnerability information, IoCs allowing search queries through these APIs.





Privileged Access Management

 **Location:** Mumbai



Stage of Company

Growth Stage Start-up



Solution Domain

Identity and Access
Management



Stage of Investment

Bootstrapped

DSCI's Comment

The Privileged Access Management solution helps manage the remote access to critical IT assets securely.

Privileged Access Management

- Cross-Platform Access : Uses the OS, platform or browser of the user's choice to access privileged sessions from anywhere with cross-platform access technology.
- Privileged Account Provisioning : Manages the lifecycle of privileged accounts from provisioning to de-provisioning across a range of systems with account provisioning.
- Integrates & combines password management, session management, privilege access management and task management capabilities into a single solution.
- Automatically on-boards assets across AWS, Azure, VMWare and Network Discovery.

Deployment

- SpectraMSP PAM is purpose-built for providing Password Management Solution as a service and managing access needs of service providers to securely access customer assets from any location.



Threat Spy

 **Location:** Jaipur



Stage of Company
Registered Start-up



Solution Domain
AI based
vulnerability
scanner



Stage of Investment
Bootstrapped

DSCI's Comment

AI based vulnerability assessment and automated scanning helps organizations preemptively detect increasing threats. With increased exposure due to WFH, the scale, complexity, and timeliness of security assurance can't be achieved by relying only on human intervention.

Threat Spy

- Next-Gen AI enabled vulnerability scanner that enables the user to predict the potential threat and provides real-time vulnerability assessment reports across Technology Stack.
- AI-enabled scanner which predicts the possibility of threats on the web application and server.
- Get Instant Alerts for Critical Vulnerabilities.
- Early Prediction of Cyber Attack for preemptive action.
- Technical and High-Level Manager reports can be fetched.

Deployment

- On Cloud



Secure ID

MacLock / Two Factor, Multi Factor
Authentication | SSH 2FA with SSO

 **Location:** Hyderabad



Stage of Company

Revenue generating
start-up



Solution Domain

Monitoring solution,
Access Management



Stage of Investment

Bootstrapped

DSCI's Comment

Features like SSO, auto-lock / auto-unlock of Mac by sensing the phone's proximity will help employees work from home seamlessly and securely.

MacLock / Two Factor, Multi Factor Authentication

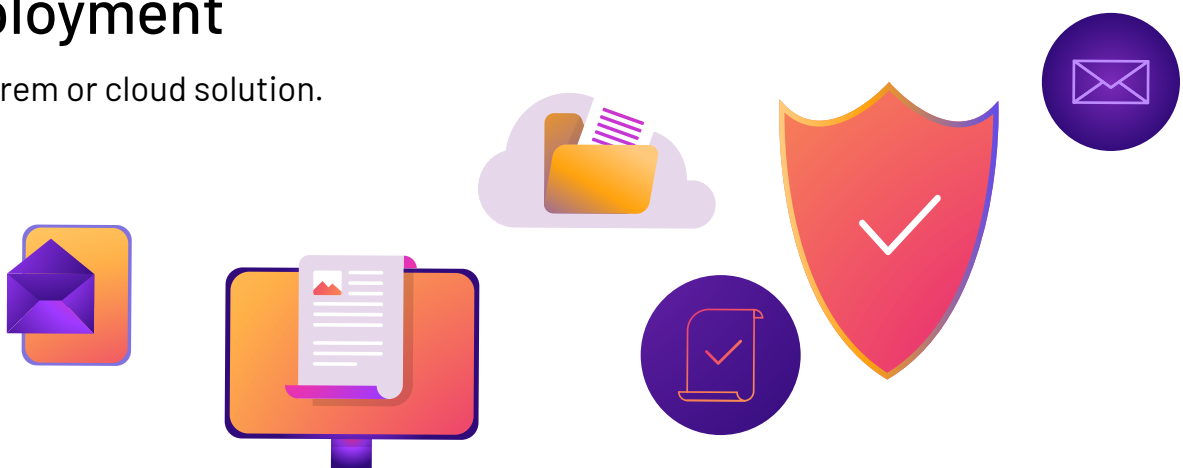
- With smartphone Near or Far, SecureID will automatically lock & unlock. Walking away from the Mac will lock all by itself. Use QR Scan to unlock.

SSH 2FA with SSO

- Two factor authentication and SSO.
 - a. Proactively monitors and centrally controls access to privileged credentials, on-prem or in the cloud.
 - b. Secure access control via SSO reduces identity sprawl and password management risk and securely provides direct access to critical assets.

Deployment

- On-prem or cloud solution.





DSG Vault File Sync | DSG Vault Outlook Plug In

 **Location:** Bengaluru



Stage of Company

Revenue Generating
Start-up



Solution Domain

Access Management,
Policy Enforcement



Stage of Investment

Bootstrapped

DSCI's Comment

Storage and delivery of data maintaining privacy security and governance help managing threats associated with increasing data share in WFH environment.

Unified data privacy, data security, & data governance.

DSG Vault File Sync

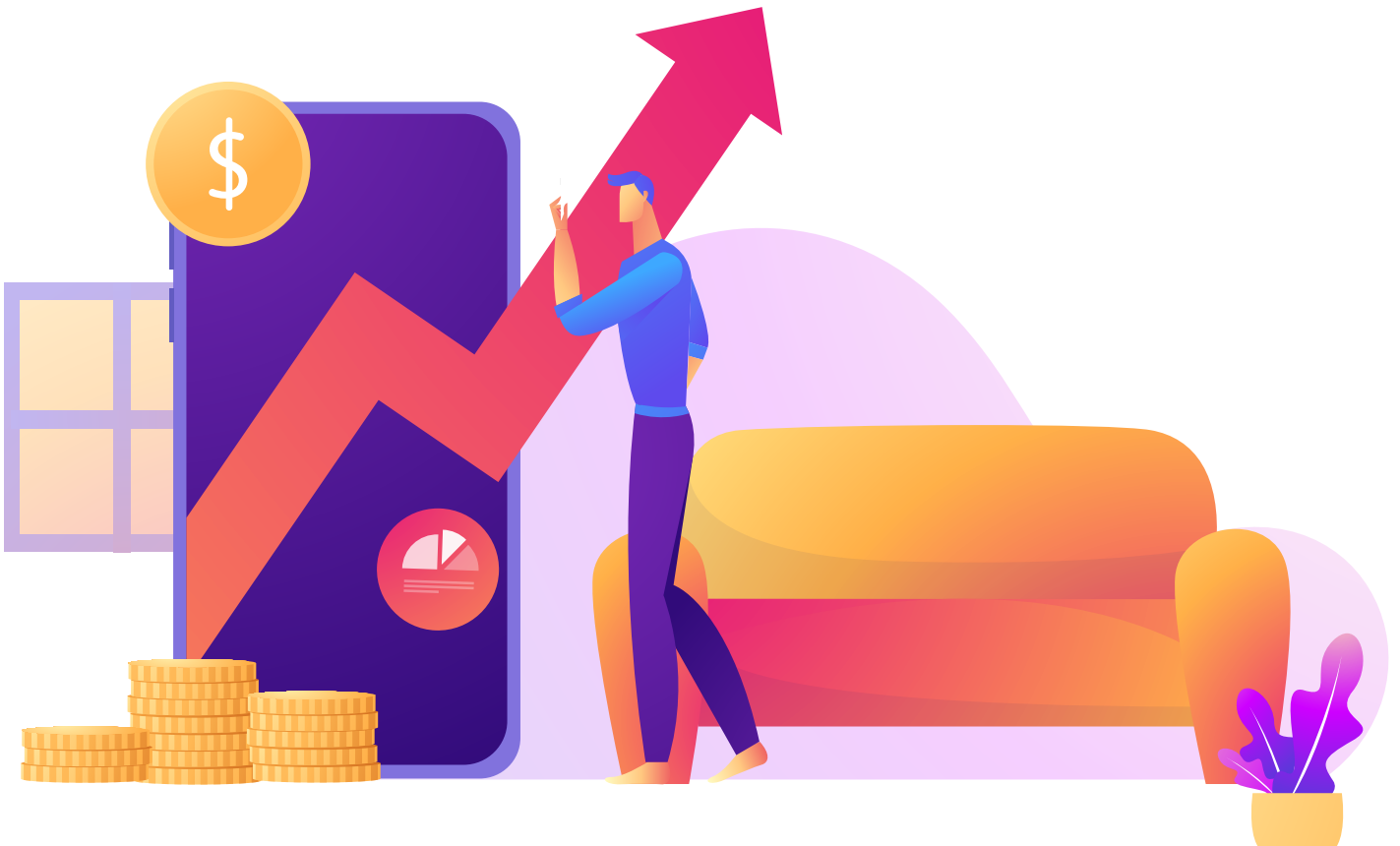
- FileSync is a digital file transfer solution that provides a powerful foundation for organizations to protect their sensitive files and achieve regulatory compliance. It enables the sharing of large-sized files internally & externally while providing end-to-end security at rest as well as in motion.
 - a. Enforce Policies: Controls file sharing by enforcing policies such as read-only/full access, expiry dates, access control, etc.
 - b. Track User Activity: Complete audit trail to track user activity at the file level.

DSG Vault Outlook Plugin

- DSG Vault - Outlook Plugin enables enterprises to protect and govern emails.
 - a. Controls data with read-only option to email attachments.
 - b. Restricts the forwarding of messages.
 - c. On-demand encryption of internal & external email communication.
 - d. End-to-end security of emails, only authorized users can access the information.
 - e. Complete audit trail brings visibility of unscrupulous data access, providing preventive measures on data breaches.

Deployment

- Flexible deployment models – On-prem, Private/Public/Hybrid cloud.
- Integrates with MS Outlook for client-initiated security and with Exchange Server.
Ready to use apps: Outlook plugin, File sync, Secure Data Exchange.



Skynet Softtech Pvt Ltd

HackShield iOS and Android Anti Hacking Solution

 **Location:** Mumbai



Stage of Company

Idea/technology/
prototype ready but
start-up not registered



Solution Domain

Vulnerability
Management



Stage of Investment

Bootstrapped

DSCI's Comment

Anti-phishing, privacy mode, network analysis features let the user understand if data is being compromised by online service providers when working remotely.

HackShield iOS and Android Anti Hacking Solution

- Comprehensive Anti-hacking solution for iOS and Android devices.
- Effective way of preventing hidden apps from stealing data or accessing applications.
- Secure mobile applications to secure mobile transactions, chats, passwords.
- Identify if USB debugging is enabled.
- AntiVirus search for malicious applications and features in user devices.
- Jail Break alert: Alerts if someone has tried to jailbreak your device.
- Two Factor Authentication for additional security.
- Allows user to understand if data has been stolen by online service providers.
- Privacy mode allows users block microphone and Wi-Fi access.
- Password Manager: helps users store/access passwords and sensitive data.
- Social Accounts: helps users monitor places and devices from where the account has been accessed.

- Secure Chat: enables users to chat using an encrypted channel, including video calling, voice calling.
- Apps and App permissions: helps users identify hidden apps, installed apps, apps secretly acquiring permissions and monitors permissions.

Deployment

- Mobile Application.





Smokescreen Deception

 **Location:** Mumbai



Stage of Company

Growth Stage Start-up



Solution Domain

Deception-based
threat detection



Stage of Investment

Bootstrapped

DSCI's Comment

Perimeter deception technology is a significant way to detect attacks on remote access services and credential thefts hence making work from home secure.

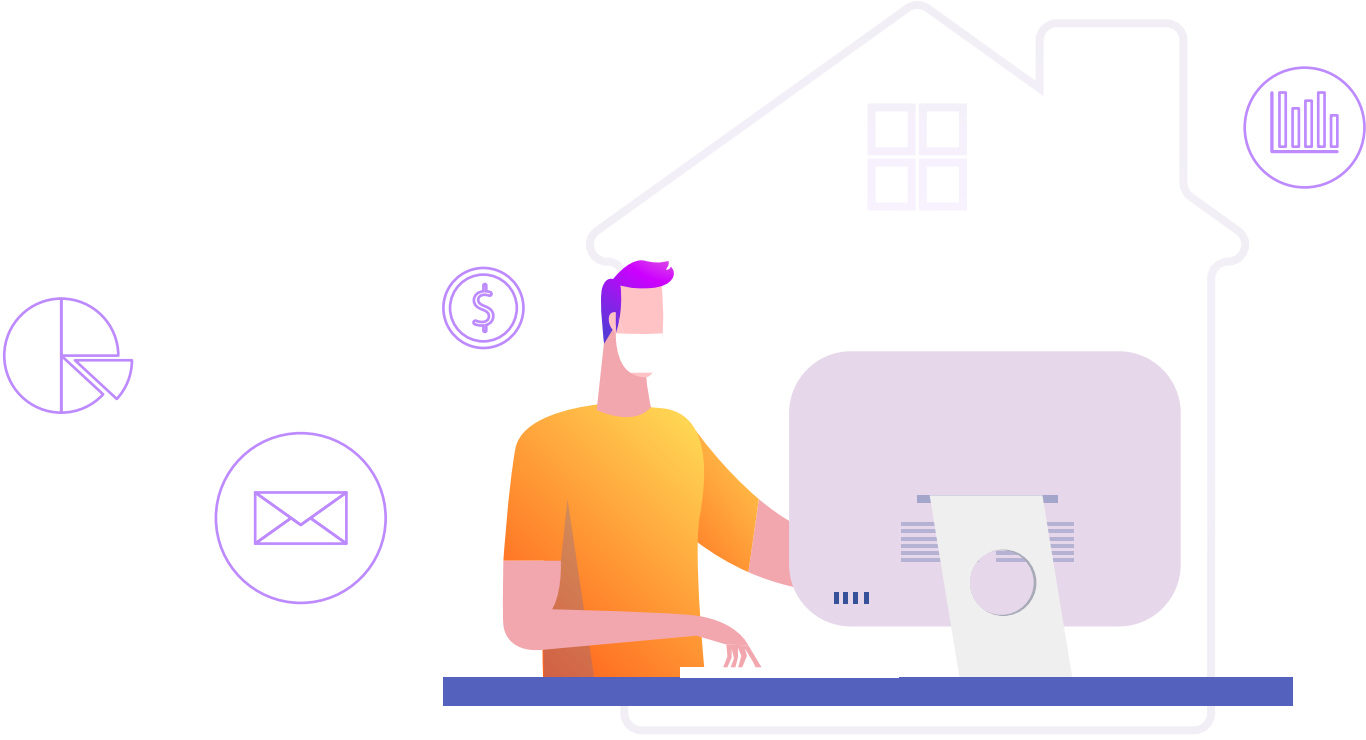
Deception to detect bad actors

Smokescreen Deception

- Detects manual and automated web-application attacks using deception technology. Reveals attempted business logic manipulation. Integrates with both web and mobile applications.
- Integration of decoys in Active Directory.
- Detecting network spreading ransomware.
- Works by injecting unpredictability into the attacker's process. The following features protect against targeted threats.
 - a. Unique deception for every organization.
 - b. Defenses that are attack-vector agnostic.
 - c. Continuously changing deception patterns.
 - d. Deception campaigns that address specific business risks.
- Deception technology creates fictitious personas – seemingly real people who match the target profile that an attacker is looking for.
- Detects the intent of the adversary rather than their tools. Instead of looking for malicious software, deception is injected to control the attacker's view of the network.

Deployment

- Deployment over the network and endpoint.





SAP GRC

 **Location:** Hyderabad



Stage of Company

Growth Stage Start-up



Solution Domain

Compliance



Stage of Investment

Bootstrapped

DSCI's Comment

MFA and SoD analysis would not only secure access to applications but also help to manage compliance.

SAP GRC

- Works on SAP authorizations, governance risk and compliance (GRC), automations with powerful algorithms.
- Efficient SoD analysis and management solution with capabilities of analysis and mitigation of risk at the user and role levels.
- Accelerated and automated authorization design in keeping with compliance guidelines and your business requirements.
- Enhanced security through two-factor authentication/multi-factor authentication and other sophisticated security protocols.
- GRC Audit Management System (GAMS) and reporting solution with capabilities of IT General Control (ITGC).
- Automation of User Management activities bundled with the Risk Analysis capabilities and self-service capabilities.
- Time-bound admin/config ID access to SAP product clients for the execution of direct and critical changes.

Deployment

- SAP services with customization on the cloud .



Wi-Jungle: Unified Threat Management Solution (UTM)

 **Location:** Jaipur



Stage of Company

Growth stage Start-up



Solution Domain

Network Access
Provisioning,
Access Control



Stage of Investment

Bootstrapped

DSCI's Comment

DLP, Cloud Sandboxing, zero-day protection, access control to network resources, VPN for IPsec and SSL, Multilayer authentication provide the key ingredients for the new paradigm of security

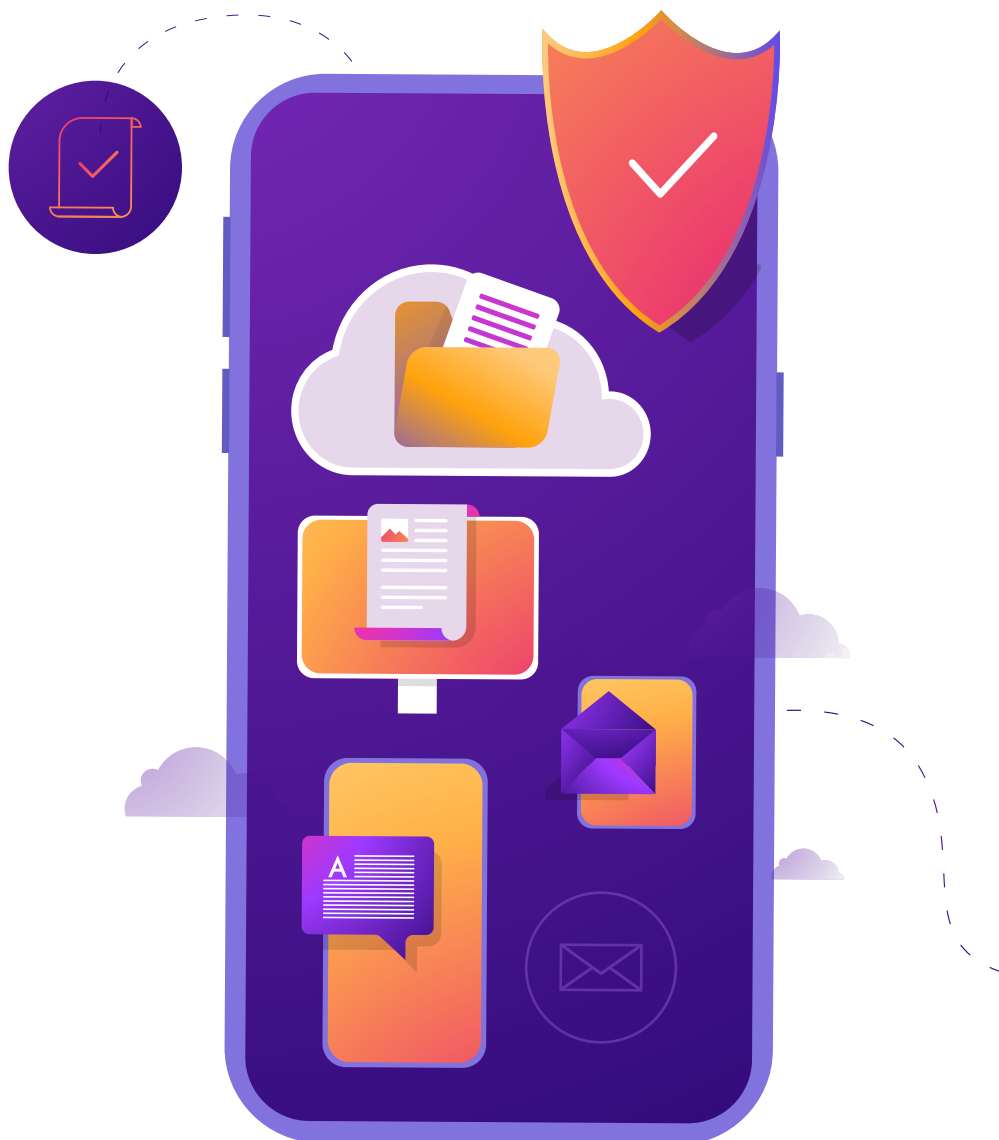
WiJungle – Unified Threat Management Solution (UTM)

- **Data Leakage Prevention:**
Helps control the transfer of important data on HTTPS/HTTP/FTP/P2P & other file sharing applications. Blocks attachments, chats based on predefined keywords.
- **Vulnerability Assessment:**
Scans to enumerate possible vulnerabilities on IT assets. The summary presents a risk score with mitigation steps.
- **Bandwidth management:**
Feature to limit data and speed usage along with the time for easier user management. Allocates different speed, data and FUP usage policies to users/guests based on their profile/room type.
- **High Availability:**
Run the two appliances in active-active and active-backup mode with stateful failover.
- **Anti-Malware and Ransomware Protection:**
Scans a packet of various ports based on the file type. Signatures automatically updated via the cloud to increase security.
- **Intrusion Detection & Prevention System:**
Has 25000+ default signatures along with the auto-update feature. Admins can also create their custom IPS signatures and Rules.

- **Anti-Spam:**
Inbound and outbound scanning of packets, real-time white/black listing of IP & domain and MIME header check.
- **Access Management:**
Robust Authentication, Authorization and Accounting feature to manage several users at a time. Authorise host based on User, MAC and IP policies.
- **Surfing and Threat Logs:**
Stores user surfing logs to help organizations handle easy tracking. Inbuilt logs storage facility for 1 year with a searchable feature.

Deployment

- Enterprise Network Deployment.



About Us

DSCI's National Centre of Excellence (National CoE) is a joint initiative between Data Security of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY) with the objective of providing impetus to the startup ecosystem in India. DSCI has set up a facility, which houses technology research lab, experience zone for demonstration of national cyber capability, experimental SOC, co-creation spaces, training facility for niche capability building, and an incubation centre.

National Centre of Excellence for Cybersecurity Technology Development & Entrepreneurship

A JOINT INITIATIVE BY




Ministry of Electronics &
Information Technology
Government of India

Disclaimer: This is a content series for National Centre of Excellence to dissect the emerging security technology products to reveal use-cases, technology stack and deployment strategies. This effort is to create awareness and understanding of technology and not to promote any particular product or company.

 @nationalcoe

 @CoeNational

 company/nationalcoe

 www.dsci.in/content/national-centre-excellence-cyber-security-technology-development

 ncoe@dsci.in