HARDWARE SECURITY

Overview

National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

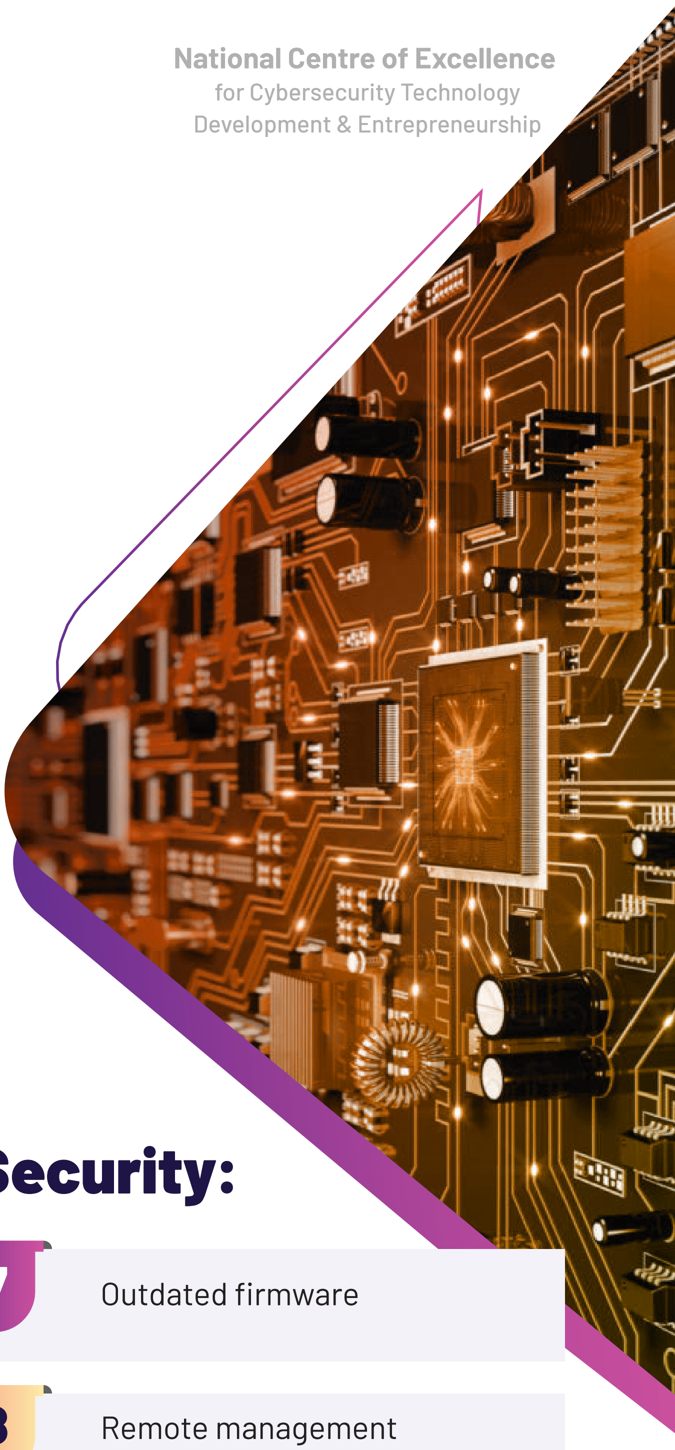
A JOINT INITIATIVE BY

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

सत्यमेव जयते
Ministry of Electronics &
Information Technology
Government of India

National CoE Content Series Product Dissection
Doc ID: NCoE:0006

Index



Hardware Security

Today's world and economies are highly interconnected. With this interconnection, supply chains for major organizations are highly globalized, with OEM's supplying various hardware components to device manufacturers from across the globe. This increasing globalization has also brought with it, increasing threats in supply chain such as counterfeit hardware, untested and unpatched hardware, insecure authentication protocols being followed, and a new wave of hardware exploits at kernel and BIOS level. With consumers now interacting with hardware technology such as IoT, mobiles, computers on a scale like never before through global supply chains, hardware threats and therefore the need to resolve them have become critical for national security.

Challenges in Hardware Security:

1 Kernel exploits

2 Malicious modification such as Hardware Trojan of an integrated circuit

3 UEFI rootkits and bootkits

4 Network device implants

5 System Management Mode (SMM) code injection

6 Malicious code in the system firmware

7 Outdated firmware

8 Remote management backdoors

9 Unauthorized firmware modifications

10 Malicious add-on devices

11 Inside job to recalibrate meters

12 Load bad software during manufacturing using social engineering

Organizations are dealing with solutions in the following categories:

A
Firmware self-healing solution

B
Secure connection between an IoT device and its origin server and deploying virtual patches

C
Endpoint hardening

D
Firmware monitoring and threat detection

E
Kernel hardening using policy-based temporal isolation

F
Self-encrypting plug and play drive

G
Side channel utilization to assess the integrity of the electronic device

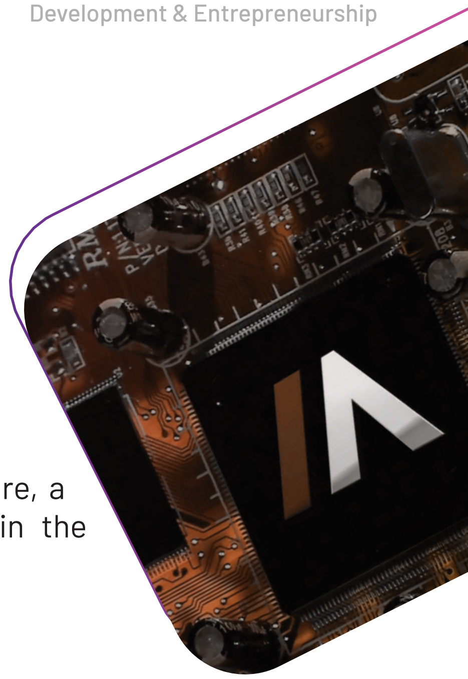
H
Generating pattern analysis using advanced profiling system

I
Firmware monitoring by leveraging open source firmware extraction tool

J
Hardware behavior tracking using advanced profiling system

Absolute

Absolute Platform: Endpoint visibility and control solution



- Persistence module is built into the firmware of desktop, laptop, tablet, and smartphone devices during its manufacture by the OEM.
- If the Persistence module is not already embedded in the firmware, a software version of the Persistence module can be installed in the partition gap on the hard drive.
- An Absolute agent is installed onto devices by the customer.
- The agent creates a two-way digital tether between the activated device and the cloud-based Absolute console.
- It's the step that turns everything on and it's through this agent that device information is transmitted to IT so they can remotely track, manage, and secure devices.
- A Monitoring center is operated by Absolute to which the agents connect periodically (referred to as 'agent calls' to the monitoring center).
- Persistence gets activated.
- A web-based console is available that the customers use to log in to their Absolute environment.
- Application Persistence is the self-healing capability that runs periodic health checks across the device fleet and seamlessly remediates applications that are either not installed, not running or missing critical operational files or directories

a. Absolute's console must be installed on each endpoint for an organization to leverage Application Persistence.
b. Policy files are deployed by Absolute based on the specific third-party software application.
c. The device calls into the Absolute Monitoring Center on a regular basis.
d. A custom agent script is retrieved and executed on the device.
e. An XML policy file, configured specifically, is downloaded to the device.
f. This policy file validates specified pre-deployment conditions (e.g. device type, operating system, device group):

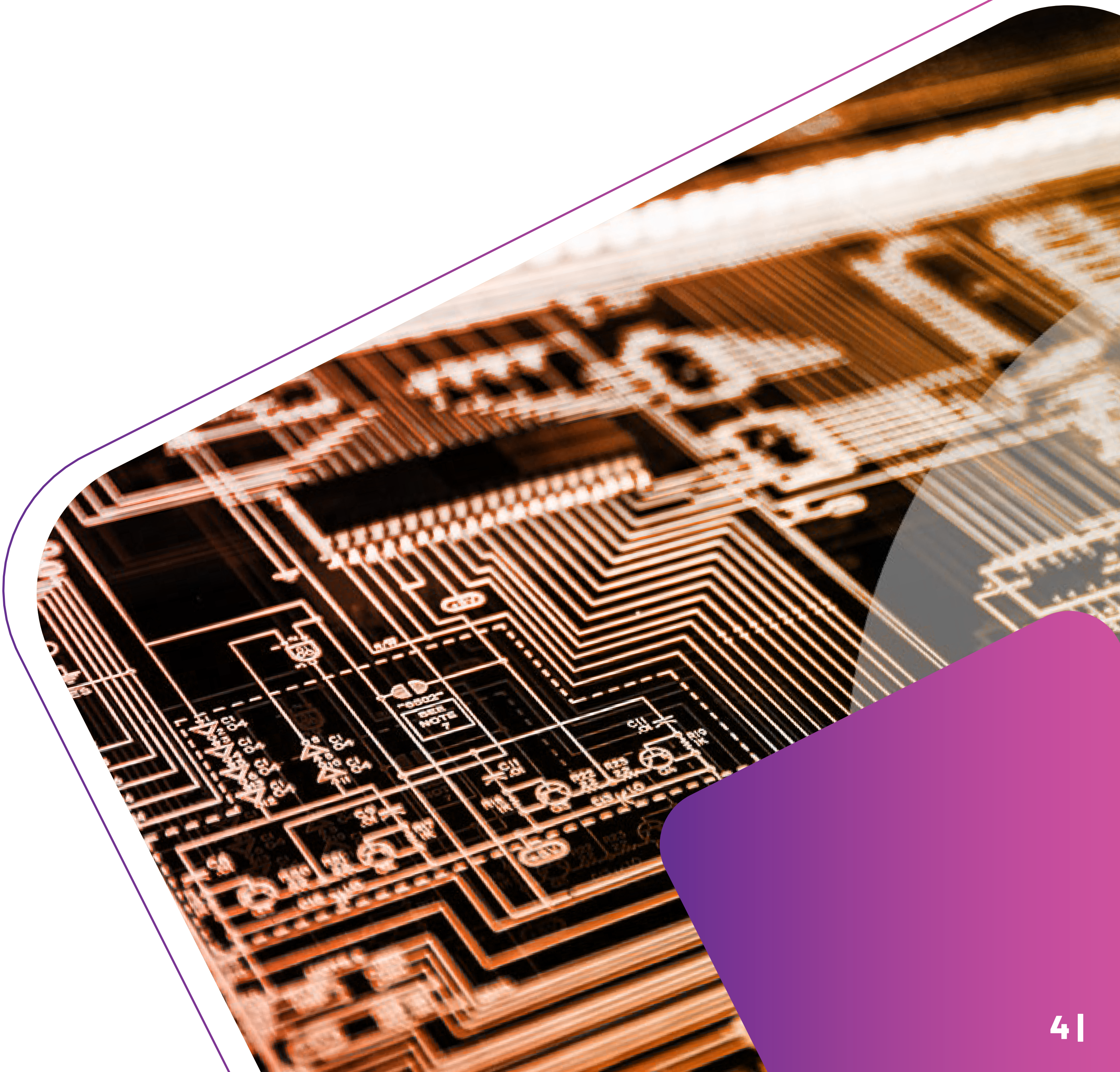
- If conditions are met, the correct application is already present on the device.
- If conditions are not met, the application components are downloaded and installed as per policy file.

- Absolute Reach: Detects, understands, and remediates vulnerabilities of the endpoint.

  a. When risks and exposures are identified, it responds immediately with pre-built or custom commands.
  b. Execute any script across any of the devices with a script once, deploy anywhere model.
  c. Custom data points are needed to be retrieved and incorporated into custom reports.
  d. In case of a new threat, an existing script can be leveraged, specific devices are targeted to execute the command.
  e. Successful delivery of it is validated.
  f. Absolute ensures that the script 'reaches' the device and is executed, giving assurance in risk response or compliance scenarios.

Deployment:

Firmware Persistence is embedded in the BIOS of machines manufactured.



Eclypsium

Eclypsium Platform: Firmware Monitoring and Threat Detection Platform

- Deployed as a targeted dissolvable scan to uncover integrity issues upon delivery of hardware or run as a periodic scan to identity threats in real time.

a. Works below the operating system layer to find threats.

b. Analyses the firmware information.

c. Checks firmware against millions of firmware hashes across dozens of enterprise hardware vendors to identify changes to baselines, find outdated firmware and expose tampering.

d. Scanning reveals the firmware inventory of enterprise devices including the system firmware (e.g. BIOS, UEFI, etc.) as well as the firmware within device components such as drives, chipsets, PCI devices, network devices and much more.

e. Leverages IOCs, static, behavioral, and heuristic analysis to find known or unknown threats or changes to firmware integrity.

f. The analytics server is constantly updated based on industry-leading threat and vulnerability research.

g. A web-based user interface provides access to information from any location.

h. Integrable with other security and orchestration tools.

i. Gain visibility into weaknesses and threats during device operations, IR & forensics.

j. Provides virtual patching to offer protection until a more permanent fix is available from manufacturers of the system.

k. Protected hardware and firmware within servers, laptops and network devices from rootkits, implants and backdoors.

l. Eclypsium extends visibility and protection to all the components that make up the internal attack surface including processors, network interface cards, UEFI and EFI firmware, Baseboard Management Controllers (BMCs), Intel Security Management Engine, Trusted Platform Modules.

m. Supply Chain Security:

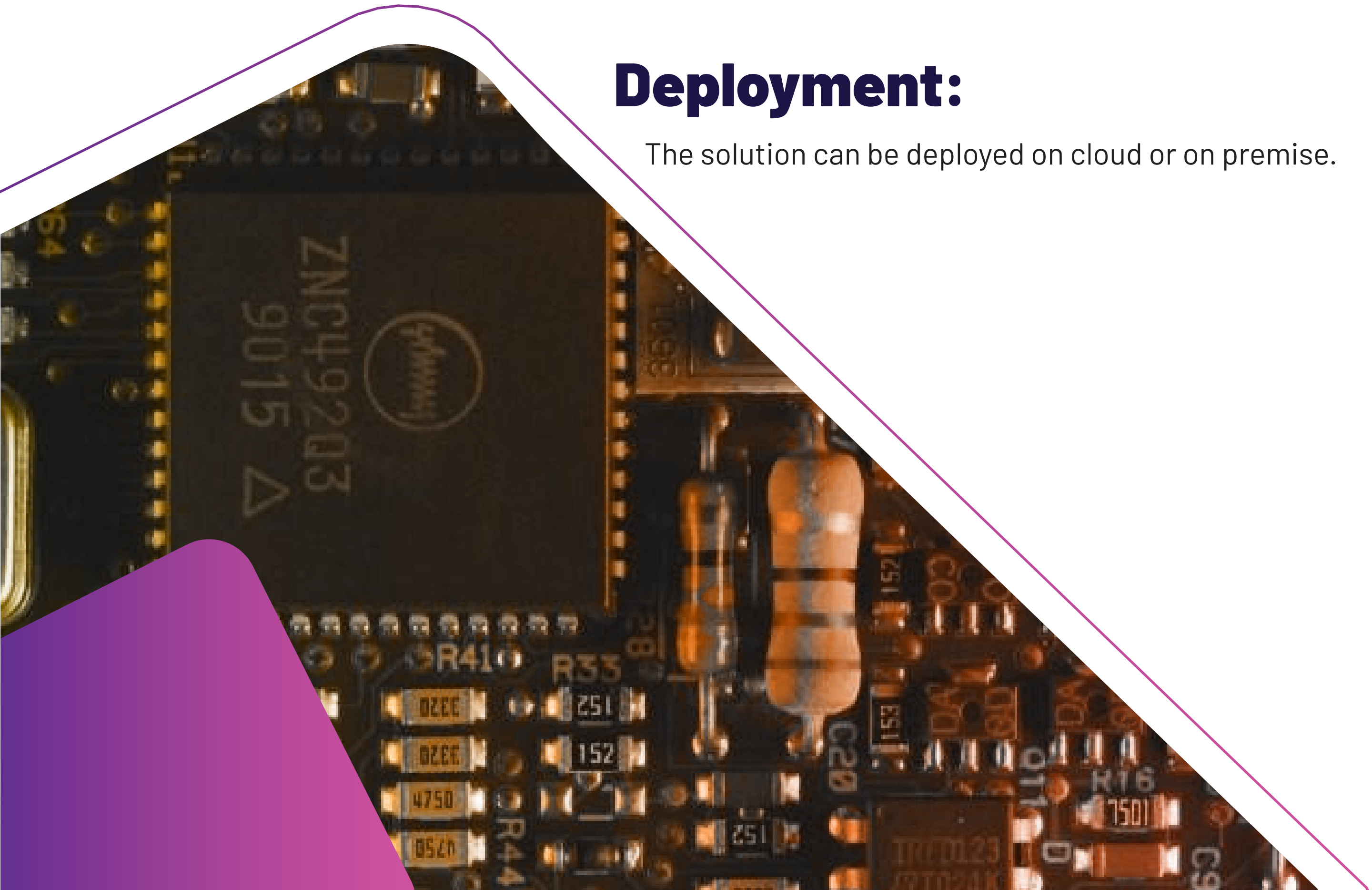
- The platform scans each system, including its many subcomponents, and automatically analyzes the firmware and how it is configured.
- This analysis can reveal the presence of implants and backdoors, vulnerable or unpatched firmware, and a variety of missing protections.
- This analysis can be used during the evaluation phase, upon delivery of new hardware, and even with trusted distributors within the supply chain.

n. High- risk travel:

- Get real-time alerts on critical events such as a failed integrity check or a threat that has been detected.
- Reveal the presence of any known/unknown implants based Eclypsium research and intelligence.
- Travel laptops can be grouped and have an alert set to monitor for tampering.
- Once a scan has revealed a change, the alert is triggered.
- The device page of the platform reveals if the integrity is compromised.

o. Remote Work:

- Integrates with VPNs and verifies device integrity before allowing remote access into the enterprise.
- Ensures remote access network gear including VPN appliances are up to date and free from backdoors and implants.
- Cloud-Based Remote Updates and Patching.



Deployment:

The solution can be deployed on cloud or on premise.

Redwall Technologies

Redwall Mobile: Mobile security solution

- The policy-based system uses temporal isolation to ensure that processes and data from one mode do not co-mingle with processes and data from another mode.

a. Hardens Android's kernel (below the application stack) against malware and exploits.

b. Creates a segmented system with multiple personas for both personal and business use (based on their security policy).

c. Uses cryptographic keys to isolate data and apps for each persona.

d. On switching, no data leakage to memory.

e. Each mode on a device is based on a security policy which can be tailored to specific user need or operation context.

f. Only one policy can be active at a time allowing a single device to operate in multiple security contexts.

g. Redwall security is built into a device at multiple layers, providing security enhancements for each layer.

h. RCore:

- Runs in a separate security context from the kernel, and guarantees that critical resources have not been modified.
- Ensures that rogue processes cannot insert privileged code.
- Provides cryptography and system logging via an API.
- Monitors all system calls, inspects their parameters, and determines whether or not the call is permitted by the current security policy.
- Uses access control lists (ACLs) to regulate file, device, and network address usage.

i. RInit:

- Lives in the Android layer and builds the startup process by providing mode-specific policy settings and the ability to switch between modes.
- On a mode switch, RInit tears down the existing Android instance, and replaces it with a new one that includes only the drivers, partitions, keys, and data appropriate for the new policy.
- This process provides cryptographic and temporal isolation, keeping one mode from being able to contaminate another.

j. RClient:

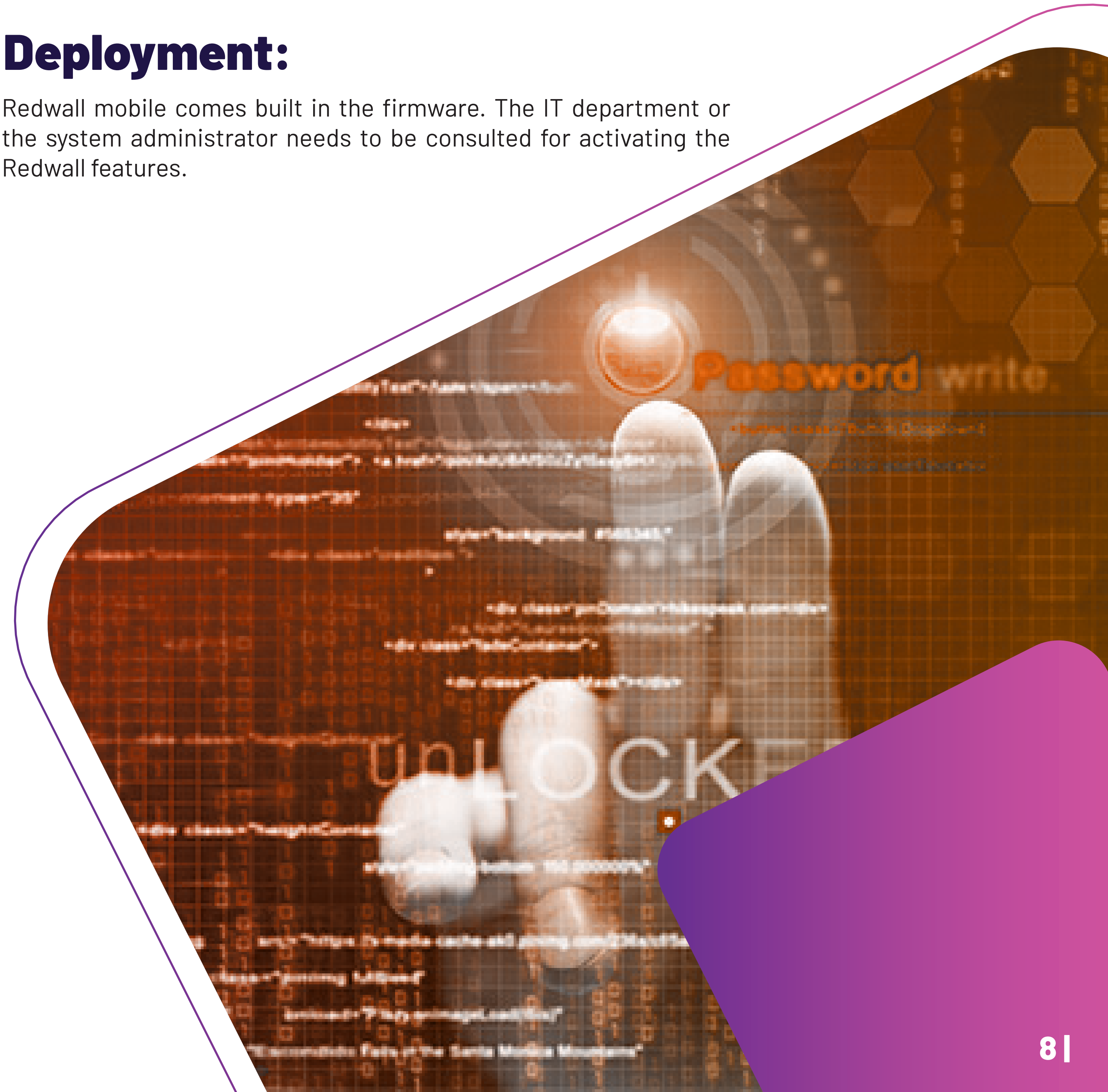
- Runs as a small Linux daemon or RT task.
- Communicates with RServer over a secure channel.
- Processes requests to upload/download files, wipe data, switch modes, update policies, update cryptographic keys, execute commands, reseed the random number generator, etc.

k. RServer:

- An application for Linux platforms accessed by authorized users and devices over HTTPS.
- It is completely optional - Redwall does not need to be connected to the policy server to operate.
- The server can be on VPN, private-cloud, or Internet protected with proxies and web application firewalls (WAFs).

Deployment:

Redwall mobile comes built in the firmware. The IT department or the system administrator needs to be consulted for activating the Redwall features.



Refirm Labs

Centrifuge Platform: Monitoring Solution

- Firmware security, vetting, analysis and continuous IoT security monitoring platform.

a. IoT and firmware security solution that detects and reports potential zero-day vulnerabilities, hidden crypto keys, backdoor passwords and known vulnerabilities without needing access to source code.

b. The compiled firmware images of the devices need to be fed in the platform with some additional details.

c. Monitors the entire inventory of uploaded firmware images for new threats.

d. Leverages Binwalk which is an open source firmware extraction tool to unpack and extract the filesystems from the firmware.

e. Also has cloud based Binwalk Pro tool as the extraction engine to identify and extract the filesystems and also creates a central repository for all firmware images and extraction work.

f. Binary Hardening Analysis: Provides supports for Binary Hardening Analysis reports across different hardening features for all executable code in firmware.

g. Centrifuge Guardian is the real-time warning system which warns the user of potential exploit before it happens.

h. The Software Bill of Materials feature generates a list of open source components that are present in a firmware image by comparing the files found within the firmware and matching them up with components.

i. Delivers detailed remediation recommendations to guide the developers and suppliers on how to make the firmware meet the security policy.

Deployment:

The Centrifuge platform is delivered as API integration

Cyqurex

MicroCloud X4

- Developed in MicroSD form factor- Creates a plug-and-play security envelope for stand-alone or networked devices, making them impregnable from most harmful types of cyber attacks.

a. Programmable hardware that enables mobile and IoT host devices to secure both Data at Rest and Data in Transit.

b. It is a self-encrypting drive which obfuscates and encrypts all data created.

c. The embedded linux processor creates a copy of the data and securely moves it from an open partition to the highly encrypted, fully hidden BlueVault.

d. Only applications using BlueSDK with the appropriate keys can access this data.

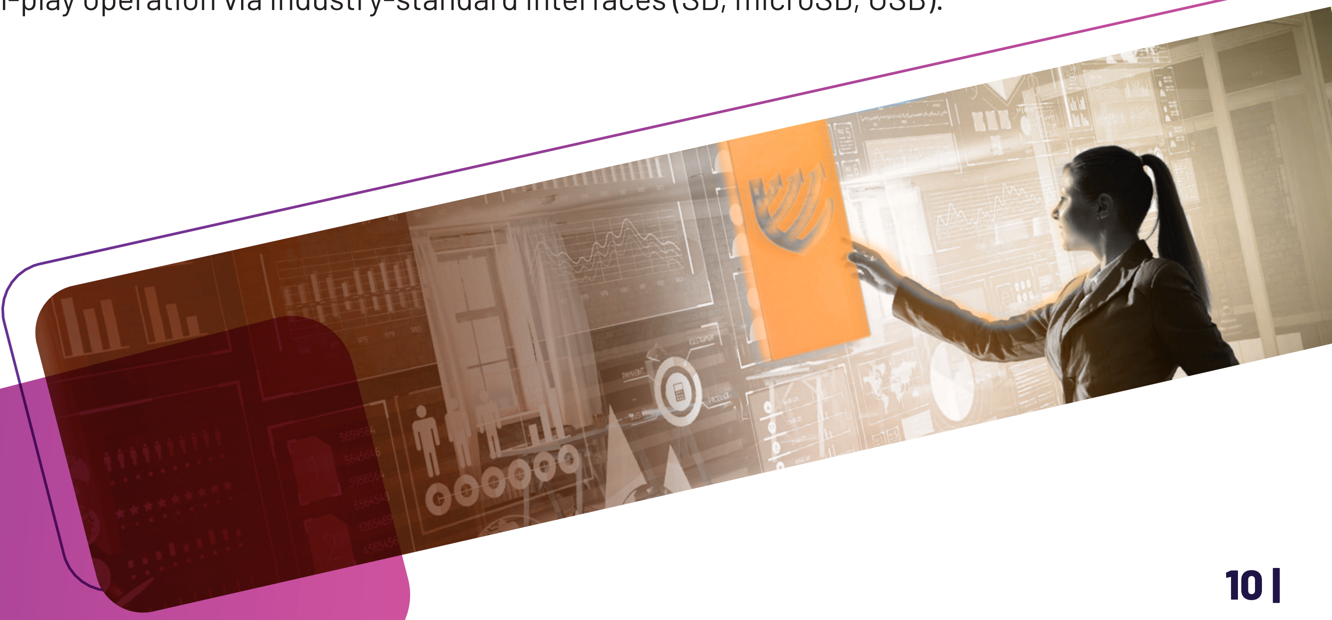
e. Non-encrypted data captured is sent to crypto-engine and encrypted data is sent out.

f. It helps in securing:

- Mobiles: Sensitive user data in phones, tablets, flash drives and security cards.
- Drones: Encrypt their ground to air traffic.
- Camera
- IoT devices: work with devices such as smartmeters for securely storing and transmitting data from sensors to the X4 encrypted BlueVault.
- Wearables: Adding computational capabilities, and securing critical personal health data both at rest and in transit.

Deployment:

Plug-n-play operation via industry-standard interfaces (SD, microSD, USB).



Sepio Systems

Sepio Prime Rogue Device
Mitigation solution

- Firmware security, vetting, analysis and continuous IoT security monitoring platform.

a. Discovers all the physical device assets, analyses their capabilities and monitors their communication and behavior in real time so it provides full visibility across the entire organization at all times.

b. A centralized management server recommends best practice security policy and provides security rankings for discovered elements.

c. Once the chosen policy is deployed, the system will detect any attack attempt or usage breach and immediately report and block it.

d. Provides alert on bad behavior devices even if they are a part of the allowed policy.

e. Sepio Network Security works at the Physical Layer, polling switches to analyze what's happening at that layer and detecting all rogue devices plugged into the Ethernet network.

f. Sepio Endpoint Protection guards against rogue devices connected to USB ports through multiple security layers, including real-time behavior analysis of suspicious devices.

g. Sepio Prime leverages:

- Physical Layer fingerprinting: Calculates a physical layer fingerprinting of all devices connected to the endpoint and compares them against a known set of a malicious devices.

- Machine Learning: Scans and clusters similar devices to their physical layer and looks for deviation of rogue or modified devices outside clustered devices.

Deployment:

Deployed as SaaS solution.

Exein

Exein Core: Firmware security software and middleware solution | Exein IDS | Exein CVECheck

- Functions as an antibody in the hardware while tracks hardware behavior and management of memory packets.

a. Open source security framework for IoT and embedded devices that works from within the hardware.

b. It operates as an embedded component building the device’s immunity with the help of an advanced profiling system.

c. Automatically extracts and analyzes large amounts of data about device behavior.

d. This data is sent to the remote AI brain and is used to identify a model representing the device's correct behavior.

e. The generated pattern analysis is sent back to the device. Once Exein has familiarized itself with the model, it can distinguish anomalies.

f. Therefore, making it autonomous.

g. Uses Convolutional Neural Networks to learn the expected behavior of a device and uses this understanding to constantly monitor its functioning and provides with the necessary tools to recognize and protect it from cyber-threats, both known and unknown.

h. Exein brings full autonomous protection to the device in every situation against all threats even unknown ones.

i. Network Fingerprint Obfuscation: Randomizes the hardware fingerprint for unauthorized network crawlers and scanners.

j. Profiles system behavior at the hardware abstraction level using machine learning.

k. Integrable with self-monitoring technologies using Exein SDK.

l. Parallel Learning: Reduces the time taken to learn and create correct pattern analysis.

m. Interpret malicious behavior with embedded decision tree.

n. Allows for improper or malicious behavior to be detected in real-time.

o. Exein provides the right toolkit to help IoT developers.

- Exein IDS

a. Support for multiple alert and logs systems.
- Broadcasts alerts to multiple json REST APIs over HTPP/S at once.
- New SIEMs, log aggregators and remediation systems can be integrated with ease by defining a new API payload format and target URL.

b. Uses active probing and passive network traffic sniffing to recognize the devices on the network and maintain a network inventory.

c. By integrating the IDS with the Exein platform, bad firmware update can be detected.

d. Its detection engine is protocol-agnostic, which makes it flexible enough to not only support common network protocols but also gives it the ability to integrate with custom protocols with ease.

- Exein CVECheck: Continuously analyzes your firmware components to search for possible security problems

a. Searches for known vulnerabilities and common software weaknesses in CVEs database and other sources of vulnerability.

b. Provides an intuitive dashboard which displays the vulnerabilities detected, sortable by score, impact, and other features so that these vulnerabilities can be managed and prioritized.

c. Helps to identify code with known vulnerabilities at each stage in the SDLC.

d. Uncovers known vulnerabilities and common software weaknesses in third-party code used in your embedded software.

e. Finds vulnerabilities and detects only CVEs (Common Vulnerabilities and Exposures) that influence your specific firmware.

Deployment:

Open source security framework.

Can be deployed on any cloud or in-house environment regardless of the underlying platform.

PFP Cybersecurity

PFP solution IoT Monitoring solution using power usage data

- Uses dynamic power behavior analysis to detect anomalies caused by hardware and software tampering, such as counterfeits, cloning, implants, and hacking of configuration and data by insiders.

a. Constantly monitors power behavior of devices/IoT in data centers, critical infrastructure & more; then, data is sent to the cloud where PFP detects malicious actors.

b. Power fingerprinting (PFP) utilizes side channels to assess the integrity of an electronic device (Side channels are physical measurements that can be made from outside the specific component, but which contain information about the execution status of the target. For instance, features such as power consumption or electromagnetic emissions are side channels intrinsic to device operation).

c. PFP monitoring setup uses a physical sensor to capture the fine-grained side-channel signals, which contain tiny patterns or fingerprints that emerge during operation that are unique to the hardware and software executing within the device.

d. Power traces are processed using signal detection and classification techniques on an external device which reduces memory and processing overhead on the target.

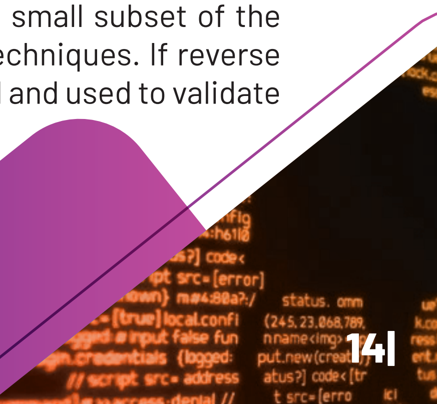
e. PFP monitors can be built using Commercial off-the-shelf (COTS) components.

f. PFP's tamper detection performance is determined by the availability and quality of the reference baselines.

g. Baseline Extraction: A baseline easily can be formed by the OEM as part of the code update. This "known-good signature" can then be loaded for all devices in the field when the new update is applied by the user.

h. In other cases, statistical analysis can be performed on a set of incoming parts to detect outliers. Such approach can be effective when only a subset of the parts is tampered or counterfeits. An example of this situation is "salting", where the genuine parts are mixed with counterfeits.

i. Another approach is to perform regular PFP characterization on a small subset of the parts. The subset is then reversed engineered using destructive techniques. If reverse engineering shows no tampering, the PFP references can be trusted and used to validate the remainder of the parts as well as all future procurements.



j. It comprises of :

i) Monitors:
- Captures the signals from the devices
- Could be a device which resides in close proximity to the target, or it could be embedded in devices such as sensors, PLC, and HMI
- Observes the instantaneous current drain or emission of the processing element during execution
- Example of the monitors include the Keysight instruments, ARM-based Stem-on-Chip IC with an on-chip digitizer and the PFP DIN railed mount pMonitor Model 751
- The pMon-751 allows the user to monitor a wide variety of target devices, from chips, to boards, and to systems, directly EMI, or via DC using an inductive current probe.
- The pMon-801 is a rack-mount security appliance that continuously monitors and detects anomalies in routers and other devices and is ideal for data centers and router farms.
- pMon-801 and pMon-751 are two products that work in conjunction with PFP's patented power analytics to detect malware in machine time.

ii) Power IQ Analytics: Detects anomalies from trusted baselines in machine time.

iii) P2Scan: provides a user-friendly interface for identification, analysis, and monitoring to scan for deviations
- Once the baseline is created, P2Scan monitors the user's system. It continuously looks for deviations from the baseline to determine whether an intrusion has occurred.
- During Runtime Monitoring, P2Scan provides a number of data views which allow the user to review and interpret the system performance in real time. A persistent graph provides a quick, easy display showing status.
- 3Scan is PFP's open platform software that lives in the cloud (on AWS) or on-premise. The product is web-enabled and dashboard accessible from any location. Users can log-on and monitor their data through the web.

k. Supply Chain: provides dynamic verification of hardware systems and a non-destructive process for tamper and intrusion detection at the supply chain.
- For large component volumes, the manufacturer would integrate PFP sensors into the Automatic Test Equipment (ATE) setup used to validate functional correctness. While the ATE is performing functional tests, the PFP monitor captures side channel signals and transfers them to the PFP analysis engine. Assessment results are then provided in the PFP Dashboard and logged for subsequent reporting and traceability.

l. Utilities: The Utility can have PFP technology incorporated by the OEM meter supplier, allowing remote monitoring and instantaneous remediation by directly embedding PFP capability in new smart meters.

Deployment:

The platform can be deployed on cloud or on premise.

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

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

सत्यमेव जयते
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