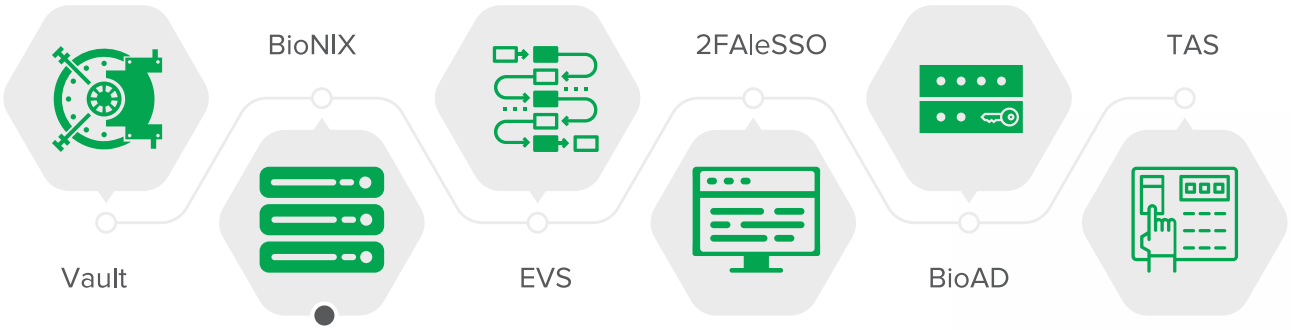
www.innait.com

InnaIT®
IDENTITY SECURED

BioNIX

Biometric protection to secure privileged access to Servers

InnaIT Framework



BioNIX

BioNIX uses Biometrics to enhance security, eliminate Credential sharing, identity theft and establish Non-Repudiation for Privileged Users (Admins). It creates audit trails for any activity increasing accountability for these privileged users.

BioNIX is a module in the InnaIT Framework. Recognizing the increasing need for reliable identification and uncompromised authentication, Precision has developed a holistic solution suite called 'InnaIT' comprising of biometric hardware and software modules that can suit all common usage scenarios across industry segments. The modular design of the InnaIT framework provides flexibility – the organization may choose the specific modules that are needed and expand as the user base grows.

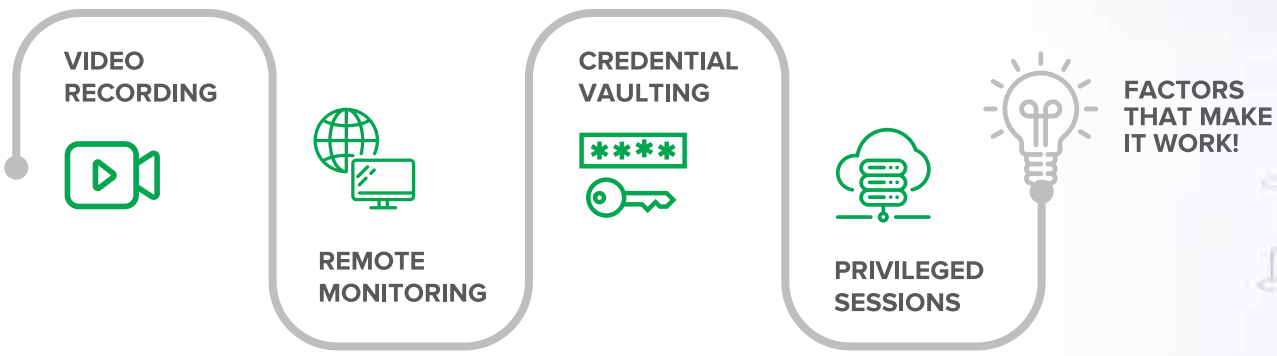
Identity Protection (PIM):

Privileged Identity Management (PIM) focuses on securing and managing the identities and credentials associated with privileged accounts. It ensures that privileged credentials are stored securely, rotated regularly, and accessed only by authorized individuals.

Access Control (PAM):

Privileged accounts typically have elevated permissions and access rights, allowing users to perform critical administrative tasks, configure systems, and access sensitive data. Privileged Access Management (PAM) solutions mitigates organization's risk by maintaining accountability, traceability, and security over privileged access.

What Constitutes a PIM/PAM?



Looming Threats With Privileged Accounts

A significant proportion of cyber attacks involve the compromise or abuse of privileged accounts, 79% of surveyed organizations experienced a privileged access-related breach.

Innovation and expansion in technology, although positive, means greater cyber threats for organization. Organizations need to proactively adapt to advancement in cyber space, access management systems and employee awareness to stay ahead of cyber attacks.

Cyber Security Risks associated with PAM

A PIM/PAM is critical because privileged accounts can pose major security risks to businesses. A major risk associated with privileged account is credential compromise. Attackers may target privileged credentials through techniques like phishing, social engineering, or malware. An attacker who compromises a privileged user account will have far greater access and possibly the power to destroy systems. The protection and management of these accounts is therefore key to securing client information and protecting brand reputation.

We understand that developing and managing regular security assessments, user awareness training, and incident response planning can be time consuming and resource intensive. This is where **InnaIT's BioNIX** Module will help you. It will not only be of assistance in defining your PIM/PAM strategy and solution approach but along with our flagship product InnaIT^{Key} (PKI + Biometric), it will ensure stronger secure authentication, eliminate credential sharing & identity theft, create audit trails and significantly reduce the risk of cyber attacks related to privileged access.

Significant Features of BioNIX

PASSWORDLESS
Passwordless Biometric & PKI based login eliminates sharing of credentials.

ADMIN CONTROL
BioNIX Users Identity and credentials are managed separately, allowing the Privileged users to access the server seamlessly.

CREDENTIAL VAULTING
Privileged Users will use just the User ID and Biometrics thus protecting the exact credentials of the server.

PASSWORD POLICY
Password Policy per requirements will be managed by the module.

PRIVILEGED SESSIONS
SSH and RDP logs maintained separately for each privileged user, even when server credentials are common.

VIDEO RECORDING
RDP stores access logs as video for the entire session and these will be stored separately for each privileged user.

ADMIN CONSOLE
Management Console for administrators to map and remove servers from privileged users.

MULTI AUTHENTICATION
Multiple Authentication methods are available for accessing the server like Hard/Soft Tokens, TOTP & QR Code.

REMOTE MONITORING
Biometric Authentication for servers can be done even while using a VDI/VPN.

BioNIX is niche functionality that is part of the InnaIT Framework. You can combine other modules of InnaIT across the organization on the same platform and future-proof your organization's IAM needs.

PRECISION BIOMETRIC

Precision Biometric India Private Limited
22, 1st Floor Habibullah Road, T.Nagar, Chennai 600 017
T : +91 44 4501 5000 | Sales : **sales@precisionbiometric.co.in**
Technical Support : **biometricsupport@precisionit.co.in** | **www.innait.com**