



Network Remote Access and Security System

Infraon SecuRA offers you a multi-pronged approach to "Remote Security and Access" – one that gives you exhaustive and complete control over your IT infrastructure, no matter how complex and distributed.



Take Complete Remote Access Control



Web-based unified console



Enables privileged session management



Regulates access through secure channels

How SecuRA keeps you in the driver's seat



Secure and audited access of the Network Core via CLI protocols (SSH and Telnet)

These can be on-premises, at the edge, in the cloud, and hybrid environments – all controlled from a single console across multiple users with different privileges. A direct Single Sign On with no exposure to username and password is possible to these devices.



Remote work facilities

Wouldn't it be easy to quickly span and manage the entire workforce by enabling privileged access to sensitive corporate systems through secure CLI sessions. SecuRA also offers granular access controls for enterprise system administrators to provide users with just enough privileges to access the required devices and the commands they can execute in those given devices.



Remote access to the network via the CLI jump server

The CLI connection to the end device would always be initiated from the secuRA server and not from the client's device. This creates a boundary of security and provides much higher protection levels. In the event of any compromise of the client's device, it is never carried forward.



Administrators can now easily authorize user specific access to devices on the network and even approve what commands can be fired through it.



Temporary, role-based access for third parties

These can be granted for contractors, vendors, and outsourced employees to access networks and servers without the need for privileged credentials. Using SecuRA administrators can create custom roles for them with just the right access to conduct their tasks, while recording, logging, and monitoring their activities.



Conduct Audits

Gain clear insight into what has changed and which user/s have made changes in an easy searchable format.



Command Restrictions

Restrict commands that are potentially dangerous and unauthorised made by unwitting users.



Session monitoring

This helps promote organizational transparency while providing IT administrators with the ability to view and, if necessary, interrupt and terminate an active session. Easily record every user session with playback capabilities for forensic audits.



Infraon SecuRA grants clear and direct access to every component in their IT infrastructure often spread across public and private clouds.



Collaborative session settings

For administrators to join an ongoing remote session with a single click for brainstorming, and also offering assistance to users while monitoring their activities during troubleshooting sessions.



Configure Scheduled Jobs

The administrator can write CLI scripts and scheduled them to be executed by the system. System allows complex condition based scripts to be executed.



Secure file transfer capabilities

Ensures that all files transferred over the network are clear and secure. Any files that are suspect or infected are denied access.

Key Benefits



**Dramatically increase
IT investment ROI**



**Tighter security
control**



**Improve operating
efficiencies**



**Suited for all
enterprise environments**

Infraon Secura Features

| Features | Standard Version | Pro Version | Features | Standard Version | Pro Version |
|---|------------------|-------------|--|------------------|-------------|
| Web Based Application | | | Device Session Termination | | |
| HTTP(s) | Y | Y | | Y | Y |
| User Management | | | CLI Session Management | | |
| User Accounts | Y | Y | SSH and Telnet access V(Putty like Experience) | Y | Y |
| Enable/Disable Accounts | Y | Y | Live Session | Y | Y |
| Temporary Accounts | | Y | Session Controls (How many times and how much time) | Y | Y |
| Password Policy Management | Y | Y | Session Audit | Y | Y |
| User Groups | | | Command Search inside Sessions | Y | Y |
| Groups Based Configurations | Y | Y | Manual Session Termination | Y | Y |
| User Roles | | | Script Execution | | |
| Role Based Controls | | Y | Command Templates | Y | Y |
| Discovery | | | Direct Command Execution | Y | Y |
| Automatic Discovery | | Y | Execution on Bulk Devices | | Y |
| Bulk Discovery | | Y | Configuration Templates | | |
| Single Add Device | Y | Y | Scripts to Store, Share | | Y |
| Device Inventory | | | ACL | | Y |
| From Discovery | | Y | Server Self Performance Monitoring | | |
| CSV Import | Y | Y | | | Y |
| Device Groups | | | Global Search | | |
| | Y | Y | Multiple Devices Search | Y | Y |
| Device Credentials Store | | | Inventory Search | Y | Y |
| Advanced Encryption Techniques | Y | Y | Reports | | |
| Device Authentication Management | | | User Audit | Y | Y |
| Single Sign On | Y | Y | Session Audit | Y | Y |
| Device Authorization Management | | | Script Execution Reports | Y | Y |
| Command Block | | Y | Devices Inventory Reports | Y | Y |
| Auto Session Terminal | | Y | PDF, Excel and CSV Export | Y | Y |
| Command Notify | | Y | Offline Reports | | |
| Command Templating for Configuration | Y | Y | | Y | Y |
| | | | Approval Management | | |
| | | | Sessions and Script Execution Approval Control | | Y |
| | | | Approval Audit | | Y |



Contact Us

Bengaluru

No. 14, Axis One 4, 3rd Floor, 15th Cross,
100 Feet Ring Rd, JP Nagar 4th Phase,
Bangalore – 560078, Karnataka, India

Tel: +91 80 46567100

Mumbai

#108, 1st floor, Bldg. 2(A-3),
The Millennium Business Park,
Mahape, Navi Mumbai - 400710

Tel: +91 22 41270170

For Additional Information

Call us: +91 80 46567148

Mail us: marketing@everest-ims.com

Visit us: www.everestims.com