



Tutis Biometric Logon

Case Study – National Security & Intelligence Agency

Industry – National Security & Intelligence

History - Established in the early post independence India, the Agency is one the oldest and most efficient internal security and intelligence organization. Shrouded in secrecy the agency works closely with other investigation agencies and has its operations across the length and breadth of the country. Though the understanding of its arcane working is largely speculative, it can be said that the agency handles several sensitive cases and critical issues related to national security.

Requirements – Maximum Security for data. The Agency has a huge database and highly sensitive data on their systems and PCs/Laptops. The data is of utmost importance to national security and is highly sensitive. Even officers within the organization are given selective access to these databases. The Agency required a flawless and foolproof system for their data security.

Existing System – Stringent physical security policies. Memory devices, Mobile Fone, camera etc are not allowed in the premises. Computer system is protected by strict code of conduct

- Password protected access control within network and individual PCs
- Periodic password changes to ensure data safety
- Physical tracking of officers based on entry-exit time at entrance to premises
- Access control based on physical approvals in accordance with the organizational heirarchy

However, the existing system had several security lapses and was not fool proof,

- Password and identity theft was possible by internal officers
- External hacking of the computer / system was possible
- Exchange of password within colleagues in emergency situations
- Windows password protected login could be bypassed by booting the system in 'Safe Mode'
- Encryption of confidential data was not based on fingerprint authentication

Security Enhanced By Tutis Biometric Logon – Tutis helped the agency discover and redefine their security system for data protection.



- Fingerprint Based Server protection for predefined conditional access to sensitive data
- Data Encryption by officers can be viewed later on only by themselves after verification of their fingerprint.
- Hacking / Duplication of the fingerprint is not possible
- Password related problems and drawbacks were eliminated
- Employee / Officer movement can be traced with the help of event log for login and log-out

Scope – Agency has operations across the country and required rapid deployment of the product in over 200 locations. These servers had officers (enrolled in to the system) accessing various databases for various purposes. The product is further scalable depending on growth and expansion of the organization.

Customization – Tutis Biometric Logon typically does not protect systems from password bypass by administrator in the Safe Mode Start-up. However, the Agency required the security system to disable this privilege even for the administrator. Keeping in mind, the importance of data security, Tutis customized its product for this functionality. Even the administrator logging in the Safe Mode can not access the data without fingerprint authentication.

Benefits –

- Agency can ensure its data is fully protected, both from external threats as well as leakage within the organization
- Password management cost and effort eliminated
- Un-intentional password leakage eliminated
- Event Log available to determine employee/officer movement within the system
- Simplified process to define conditional access to officers