

Introducing Avert™ Access Control

**Data Protection Through:
Identity Access Management
and Endpoint Security**

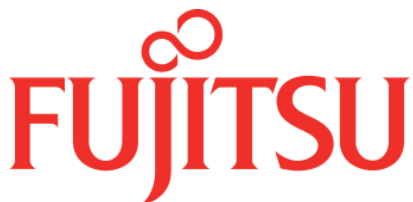


Presented by:



Crystal IT, Inc.

Crystal IT Partnerships



Technology Partner



Master Distributor
Kingdom of Saudi Arabia



Technology Partner



North American Reseller



Technology Partner



InfraGard®

FBI Information Sharing Network
(Crystal IT: Awarded Member)



Credit Facilities Partner

Why Secure Endpoint Access?



According to the Ponemon Institute's *2010 Governance Trends Survey*:

87% - of respondents believe that individuals have too much access to information resources that are not pertinent to their job description.

72% - say they cannot quickly respond to changes in employee access requirements.

57% - of organizations do not have enough technologies to manage and govern end-user access to information resources.

52% - cannot keep pace with the number of access change requests that come in on a regular basis.

Internal Attacks – What to Protect



Potential Threats



Information to Protect

Employees
Customers
Vendors
Temporary Staff
Cleaning Crew
Maintenance Workers

Employee & Customer Data

- Social Security Information
- Credit Card Numbers
- Driver's License Information
- Health Records

Intellectual & Proprietary Information

- Source Code
- Patents and Legal
- Engineering Designs
- Drugs and Formulas
- Business Development
- Financial Data, etc.

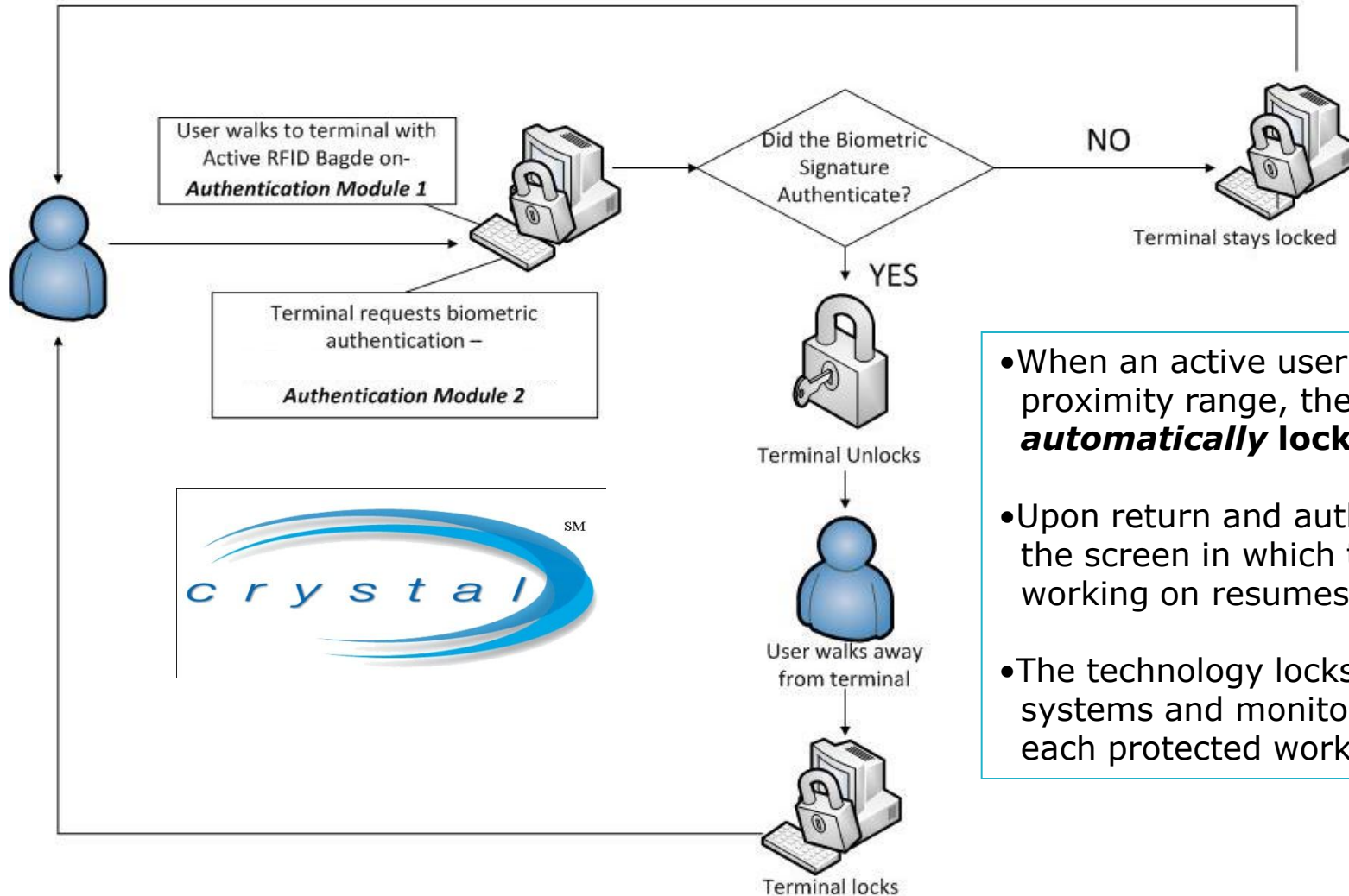
Key Benefits – **Avert**[™] Access Control



- ❑ Prevents Unauthorized Access to Computer and Network
- ❑ Utilizes Dual-factor Authentication to Validate the User's Identity
- ❑ Manages Multiple Passwords: Enterprise-Wide Universal Sign On
- ❑ Identifies and Logs Access Attempts
- ❑ Enforces Corporate Protocol
- ❑ Reduces In-House IT Support Expenses
- ❑ Meets the New Standard of AC²
- ❑ Increases Productivity with Results on Investment

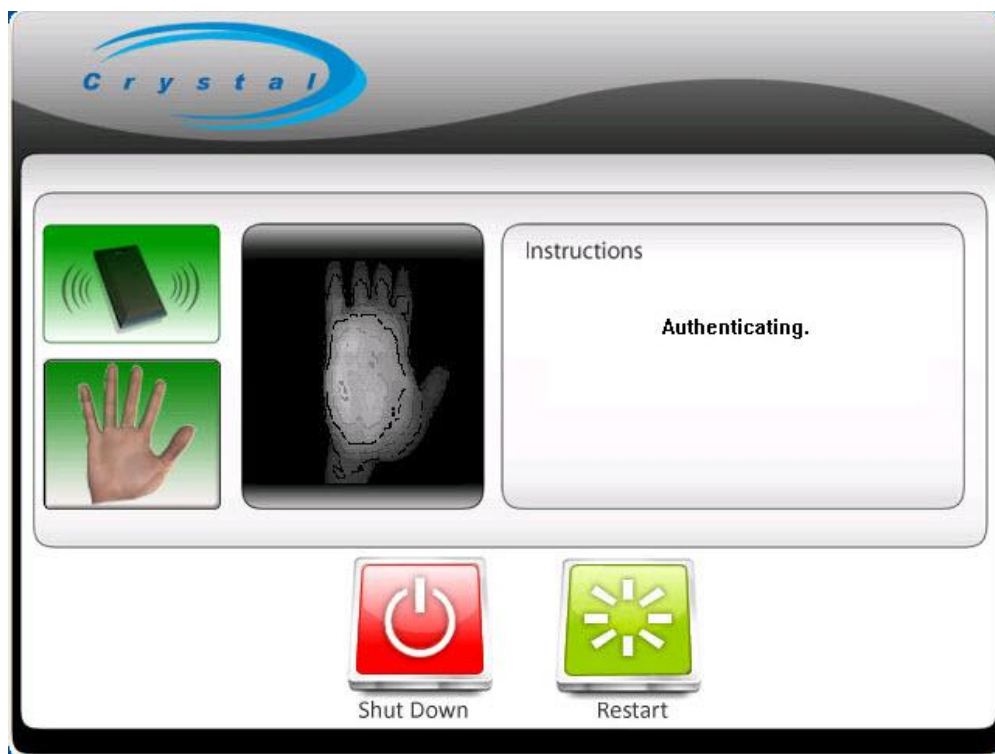


How Does **Avert**TM Access Control Work?



- When an active user leaves the proximity range, the workstation **automatically locks**.
- Upon return and authentication, the screen in which they were working on resumes.
- The technology locks unattended systems and monitors access to each protected workstation.

Workstation Security Module



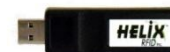
Screenshot: RFID Badge Recognized; User Submitting Vascular Biometric Pattern.

Avert™ Access Control client module includes the following components:

Client Software License



Active RFID USB Reader



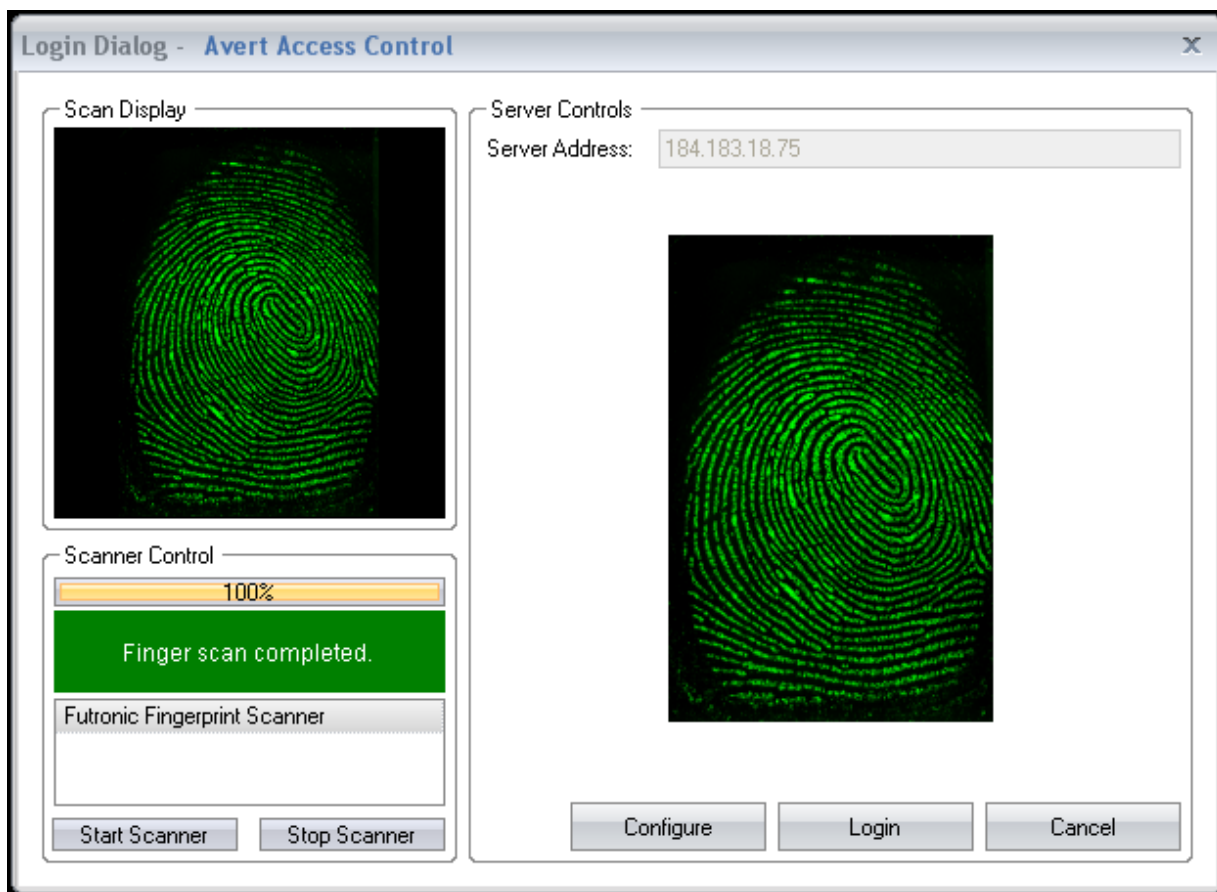
Active RFID Badge



Biometrics Scanner



Central Administrative Controls



Screenshot: Administrator Login Through Central Administrative Appliance.

Administrative Rights

Enroll Users

Monitor Activity

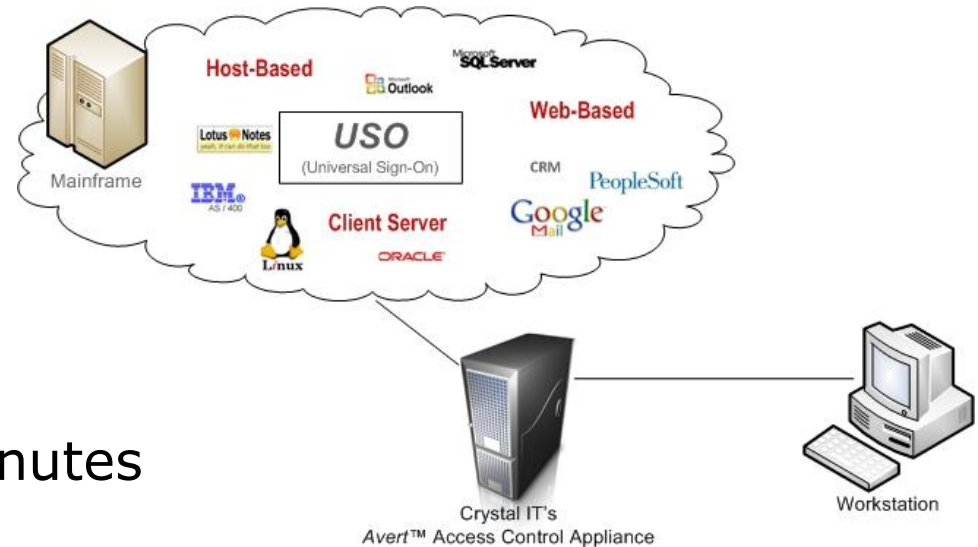
Print Event Log Reports

Grant or Revoke Privileges

Easily Configure Groups

Maintain Access Control

Featured Architecture



- ✓ Individual Registration in Minutes
- ✓ Administered from Centralized Location
- ✓ Superior Visibility for e-Forensics
- ✓ Deployed Through Administrative Appliance

Endpoint Security Comparisons



Case #1 – Endpoint Security Management

- Passwords Utilized for User ID and System Entry
- Access can be Gained thru Authorized Terminal with Compromised Credentials (No Strong User Authentication)
- Unauthorized User(s) able to Access System

Result: Terminal is not sufficiently protected against an internal attack. It will be difficult to pursue legal remedies due to lack of e-forensic evidence to identify offender.

Case #2 – Passive Proximity RFID Badge

- Employee Accesses System with RFID Badge
- Allows Access to Confidential Information
- System is Left Open While User is Away from Terminal
- Workstation Susceptible to Unauthorized Access

Result: Passive Proximity RFID Badges can be lost, stolen, or misplaced. Systems can be left open for data theft. Passive Proximity RFID Badges often carry a dual purpose for both logical and physical access leaving organizations **vulnerable to data theft and a physical breach at single or multiple physical locations.**

Case #3 – Smartcards (With or Without Biometrics)

- Employee Inserts Smartcard into Computer Terminal
- Allows Access to Confidential Information Using Personal Data Stored Directly on Smartcard to Validate Authorization
- Employee Forgets to Remove Smartcard When Leaving Terminal
- Terminal Left Open – Available for Unauthorized Access

Result: Smartcards can be lost, stolen, or misplaced. Even with biometrics, systems can be left open for data theft. Smartcards often carry a dual purpose of both terminal and physical access leaving an organization **vulnerable to data theft and a breach at single or multiple physical locations.**

Case #4 – Biometric Identification Alone

- Employee Accesses System with Biometric Credentials
- Allows Access to Confidential Information
- System Left Open While User is Away from Terminal
- Available for Unauthorized Access

Result: Although biometrics will identify who *originally* accessed the system, the terminal may be **vulnerable to unauthorized use when the employee steps away from terminal.**

Case #5 – Avert™ Access Control (Biometrics *With* Active Proximity RFID Technology)

- Employee Accesses System with Vascular Biometrics *and* Active Proximity RFID Badge
- Gains Access to Confidential Information
- System Automatically Locks When Authorized User Steps Away from Terminal
- Unauthorized Access Denied

Result: Biometric signature *and* Active Proximity RFID Badge credentials must match in order to access system. Unauthorized access not possible because **the system automatically locks when user steps away.** Undeniable e-forensic evidence if a data breach occurs at the hands of an employee and/or an authorized user.

Contact us today for more information or to
schedule a product demonstration
of **Avert**[™] Access Control.



Office: (888) 875-3646

Email: sales@crystalit.us

Global IT Security