

## Return On Investment

Technology managers understand the intrinsic value of IT security. They also understand the ROI from productivity gains due to investments in software tools and systems. However, CEOs and CFOs want quantifiable proof of an ROI before they invest in new technology.

This presents a problem for some vendors of security products who are primarily selling their products based on 'insurance' value and 'soft' ROI. Yet, the portion of the IT budget allocated to improving corporate security continues to grow. Today, IT managers are confronted with a plethora of security products offering 'soft' ROI and daunting TCO figures for deploying and maintaining sophisticated perimeter security products. Given this environment, how does the technology manager select a product that delivers the value inherent in tightened security with a demonstrable ROI and low TCO that will appease both the CEO and CFO?

SureID offers the solution to this conundrum faced by IT managers. SureID's Suite of Biometric Authentication products protect your company's most valued IT resources at all points of access in a manner that is both secure and convenient! Now IT Managers can adopt a security technology that offers ROI metrics on two axes: Security and User Productivity. Our Biometric Single Sign On technology offers unparalleled security by providing the most secure authentication method available in a solution that increases the productivity of both users and administrators. Consider the following ROI factors of both Security and Convenience:

## Improved Operational Efficiencies

**Reduced Administration Costs.** IDC estimates that Password Management costs between \$200 and \$300 per user per year. With SureID employees are no longer required to remember passwords, PINs or tokens for dozens of different accounts. Administrators need not implement and enforce strict password policies that require user to continually adjust to new passwords. Passwords are now a thing of the past. They are beyond the user purview hence, they can't be compromised or forgotten. Furthermore, complex processes to provision new, temporary and transferred employees with resources and access to business information are simplified and reduced to a single point of administration. And while the use of shared accounts at the system level is still permitted to further ease administration headaches, SureID provides a Biometric audit trail to determine the access achieved by individual users.

**Increases Employee Productivity:** According to a 1996 study by the Network Applications Consortium, a typical user spends as much as 44 hours per year performing multiple login tasks to access applications. SureID releases users from Password Purgatory. Users no longer waste time typing usernames and passwords. Additionally, Hurwitz Group states that most users can't remember more than 3 passwords, yet are expected to remember 6 or more. SureID increases productivity as users no longer try to access systems using incorrect passwords.

**Passive Integration:** Due to SureID's "Passive Integration" technology, critical systems and applications do not need to be taken out of service during the deployment of our products. This insures revenues streams dependent upon are your critical IT servers and systems continue to produce, even while the system is being deployed.

**Leverages ROI of Prior Investments:** SureID's patented "Passive Integration" allows our system be seamlessly overlaid upon your existing IT Infrastructure. The benefits from these prior investments does not terminate, but is enhanced by the Biometric features of SureID.

**Reduces Help Desk and Technical Support Costs:** User access to systems and applications is streamlined. Dozens of separate sign-on procedures that often require complex instructions are reduced to a simple finger scan. There is further hard ROI data. Meta Group analyst Chris Byrnes says 45% of total help desk calls are for password-reset assistance. Those users are attempting to identify themselves, but instead cost the company money in lost productivity and strained IT resources.

## Enhanced Security

**Enhances security:** Tighter security minimizes the chance of costly intrusions or leaks of sensitive data. Centralizing identity management with policy-based controls reduces the number of access points and ensures consistency in the way applications and services grant or deny access.

**Remove the Weakest Link in Security:** User Authentication: According to the 2002 CSI/FBI Computer Crime and Security Survey, while external breaches of security are on the rise, the greatest financial loss to business occurs from systems being compromised internally. This is the result of both malicious activity and intentional, but inadvertent access. Further, although external hackers use sophisticated techniques to penetrate the perimeter, once inside, they use low-tech password attacks to do their damage.

**Virtually Eliminate Identity Theft:** A credit bureau employee using unsecured usernames and passwords committed the largest identity theft fraud in US history. Philip Cummings used username and passwords on a Teledata Communications "credit prompter" to request credit reports posing as a Ford credit representative thereby stealing the identities of thousands of individuals.

**Controls Access to Corporate Information:** According to the 2002 CSI/FBI Computer Crime and Security Survey, while the theft of proprietary information has remained relatively stable, the costs associated with this type of activity has soared. In one case involving Avery Dennison, one lost secret formula was quantified as being worth over \$40 million - and this only considered the cost of the investment to develop the formula!

**Secure the Danger from Within:** According to a Yankee Group Survey, a third of all network outages are self-inflicted. Of 229 business and government institutions surveyed, 31% of all outages were caused by user error. Half these companies had unauthorized changes to their networks, 70% used shared password access control and 83% had no way to associated network down-time with user access. All these problems could be solved with SureID.



© 2002 Sure ID, LLC. All rights reserved.

## About Biometric Identification

Biometric identification is a proven and reliable form of identification. In fact the US military has selected Fingerprint biometrics as the standard means of identification. SureID adheres to this de-facto standard and uses patented biometric authentication as the basis for Identity management and corporate information access control. Biometric Credentials, in the form of a mathematical model, are stored in a tamper-proof encrypted container.

## Total Cost of Ownership

The SureID solutions are unmatched in providing low TCO. Unlike IDS, FW, NFAT solutions whose protective capabilities are obsolete by the time they are installed due to the continued inventiveness of hackers, the SureID solutions do not require continuous upgrades, expensive consultancy or dedicate support staff to install, maintain and administer. SureID is a wise investment for the cost conscious CEO, CIO, and SIO..

## Find a SureID Dealer

To find out more on how SureID can protect your IT infrastructure and simultaneously allow you to derive the ease of use benefits listed here, refer to our website at [www.sureid.com](http://www.sureid.com) to find the SureID dealer nearest you.

Sure ID  
201 Yorktown Drive, Suite100  
Mullica Hill, NJ 08062  
Toll-Free: 1.866.4.SUREID  
Email: [support@sureid.com](mailto:support@sureid.com)