



The Complete Solution

CRITICAL EVALUATION CRITERIA

Important to the selection of computer security that safeguards access and mitigates intrusion.



While there are various vendors who claim to have an access governance, identity or password management solution, buyers would be wise to consider the following security requirements to determine the capabilities and criteria necessary to truly secure, control and govern workstation and network access throughout their organization. It takes a truly comprehensive solution utilizing the right technology, not just *any* technology, to lock down endpoints and mitigate a potential breach.

COMPUTER SECURITY

Endpoint Security, Access Governance and Identity Access Management – What's the difference? Simply put, for the “complete” solution there is no difference! For a truly comprehensive solution, all components will be present to govern access to each computer, actively monitor each log on attempt with detailed reports, unequivocally verify the identity of the individual who is accessing each system and automatically lock the system when the user steps away. However, there are various products on the market that only provide one of the several necessary components needed to secure terminals which may lead to open holes in security and vulnerability to the organization.

Automatic Workstation Locking. Automatic locking which requires any degree of user interaction is not automatic locking of a system. Any procedure requiring user intervention allows for mistakes and lapses in judgment or forgetting to perform a task. People make mistakes and simply will not perform the tasks in any reliable form. It is imperative to find out whether or not user intervention is required when a vendor purports their solution automatically locks when the user walks away. Automatic locking is just that, absolutely no user intervention at all. They get up and walk away; their system locks up *immediately*. PERIOD!

Session Lock Outs. Other access governance solutions which operate under the Windows Operating System have the capability to lock out after a pre-determined time of inactivity of input (i.e. keystroke, mouse movement, etc.) by a user. Many users have bypassed this function because of the inconvenience and security holes presented by its use. For example, if set to a few minutes, the user is constantly interrupted from work production to re-enter credentials simply for inactive input. Likewise, if set to a long time period of inactivity, someone with malicious intent has the ability to resume functioning in the same capacity as the authorized user by simply accessing the terminal when the user steps away prior to the timer lock out. This technology is not sufficient for protecting an organization and is an obsolete option for security.

PASSWORDS

Passwords – Unreliable and Insecure. While utilizing passwords for computer security was once the norm, this method has proven time and again to be one of the easiest security measures for hackers to penetrate. In today's enterprise environment, employees have numerous passwords in order to access the multitude of software applications and websites needed to conduct business on a daily basis. Studies have proven that it is nearly impossible for a person to “remember” each password that must be unique in characters (numbers, letters, uppercase/lowercase, etc.) for each program accessed. Because of this, the individual will have the tendency to 1. create passwords that are either generic, personal, or easily remembered; 2. write the passwords down on sticky notes or papers easily found by those with malicious intent; or 3. use the same password for every program accessed. This is a compulsory trait inherent to all human beings which is why removing the responsibility of password recall and generation from the user's perspective is paramount in today's security protocol.

Managing Passwords – SSO and USO. Single Sign On (SSO) solutions, often called Universal Sign On (USO), can be seen as a necessary security component to eliminate the huge bulk of daily passwords that are expected to be managed within a large enterprise environment. Simply sign in once using your standard morning user name and password, and the solution takes care of all the passwords a user is required to manage for subsequent applications on a daily basis - verified entry is handled for them. Sounds great...except for a very large problem known as Key Loggers - a well known exploit and rogue program that is easily loaded onto a computer which allows an intruder to track all the key strokes from any computer. All that is needed are the first 25 key strokes from a computer on any given day for them to gain access. It is reasonable to assume that within those first 25 key strokes, an employee will enter their user name and password. Hackers will now have complete and full access to all the programs including potential financial, proprietary and customer information. The only way to prevent Key Loggers is to eliminate passwords completely. The most advanced password management solutions will utilize a user's biometric signature, presented at log in, for access to the system and each subsequent application. A Key Logger cannot read biometric signatures.

Password Resets. Password reset software can often be seen as a solution to reduce the burden placed on IT administrative staff. However, the information generated for each password reset can, once again, be easily accessed by an outside source with malicious intent. Eliminating passwords from the user's perspective is the only way to ensure information contained within the network is protected.

Access Governance, Identity & Password Management Solutions

IDENTITY VERIFICATION

Dual Authentication. Often referred to as two-factor authentication, dual authentication is the process whereby two forms of technology are utilized to verify the identity of the user at the terminal. Although one form may be sufficient to gain access to the workstation and network, utilizing two forms, one being a biometric device, will ensure that e-forensic evidence is available to account for the individual accessing the terminal and ensure entry is gained only by the *authorized* user.

Credential Protection. There are authentication tools (Smart Cards, Passive RFID cards/readers, and Key Fobs) that are being used for workstation security; however, understanding the risk of their use is imperative for the mandatory protection of your entity. Because these technologies only work to *grant* access and do not validate the specific individual utilizing the tool to gain access, the credentials of the particular user are never fully validated. These tools seem to meet the minimum access requirement until you understand that the Smart Card, badge or Key Fob may have been dropped in the parking lot or cafeteria and any user could access the system simply by possessing and presenting the specific tool at the workstation terminal. Likewise, many Smart Cards carry a chip that can easily be decrypted allowing hackers the ability to gather sensitive credential information directly from the card itself – posing a significant flaw in its use for any form of security.

Contactless Identification Devices. Many employees in various industries (including healthcare, manufacturing, and scientific laboratories) work within environments that will require contactless authentication devices for varying reasons including hygiene and environment exposures. In order to maintain safety protocol, it is wise to investigate whether or not a vendor offers such an option to maintain your organization's compliance initiatives.

TECHNOLOGY COMPONENTS

Scalable to Your Needs. If there is already established technology in place to handle one piece of the several components needed for a comprehensive access governance and identity management solution, it is wise to utilize a vendor that has the ability to provide and integrate the remaining components without unnecessary overlap. For example, if a single sign on password management solution is already being utilized within your company, the remaining technologies to monitor and control workstation access while verifying the identity of the user should easily integrate into the already established component.

Centralized Configuration, Deployment and Administration. Any access governance solution should allow an organization's IT staff the ability to easily initiate, manage and control all workstation access from one centralized location. By having these audit controls in place, IT staff have the ability to control which employees have approved access to confidential information, immediately eliminate access to an individual if needed, and view in real time all access across the network. When staff are able to control workstation access and employees are no longer required to enter daily passwords, the burden placed on IT administrators for help desk calls is reduced by 50% or more and significant return on investment (ROI) can be seen.

Security Layers – SS7 v. SSH. SS7 security layer protocol has been widely documented and known to be open to “man-in-the-middle” attacks. This means that anyone technically savvy enough to be in the enterprise has the ability to sniff the network, watch and log all the traffic. This includes all HR files, credit card transactions, financial information, sales numbers—any information that is currently protected by an obsolete user name and password management solution can be broken into. This provides a significant false sense of security.

Interference with Other Technologies. Several vendors utilize technology that has been known to cause disruption in vital technical equipment already established within an entity. In a healthcare setting, this can not only cause disturbances in equipment but put patients at risk as well. Be sure to find out whether or not this is an obstacle when evaluating a solution.



About Crystal IT



Crystal IT, Inc. is a leading developer and computer security solutions provider for governments, corporations, universities, healthcare providers and financial institutions worldwide. The company's proprietary enterprise access governance and identity management software combines with leading-edge hardware to provide clients with differentiation that cannot be achieved by other vendors. In addition, Crystal IT is recognized as an expert in IT security and is available in an advisory capacity. Crystal IT maintains North American headquarters in Phoenix, Arizona.

34406 N. 27th Drive, Suite 198, Phoenix AZ 85085 | 888.875.3646 | Email: sales@crystalit.us | Website: www.crystalit.us