

Manage Passwords to Secure Your IT Environment

Mark Nicolett

An effective password management policy is critical to secure your IT environment. Combine password formation and usage best practices with tools that promote attack resiliency to ensure that your systems are protected.

ANALYSIS

The overall security level of an enterprise is the sum of many security foundation elements: strong perimeter defenses, the proper configuration of system resources and effective controls for resource access. Protecting application and data resources requires, among other things, authenticating the people that access those resources. In turn, the integrity of the authentication process depends on uncompromised, secure passwords. IT security directors can manage passwords effectively, and thus better secure the IT environment, by following these best practices.

Establish a password management policy. Develop a single password policy that is implemented consistently across users and systems. Consider potential external and internal threats, as well as user behavior. Communicate the policy to employees and other users, and monitor for compliance (see "Best Practices for Managing Passwords: Overview").

Develop and enforce password formation and usage guidelines. Password formation and usage guidelines are the external representation of the user and system administrator portions of a password management policy. Password formation must achieve a balance between password strength and usability. This will minimize help desk calls and avoid the possibility that users will write down their passwords, thus making them vulnerable to discovery by attackers (see "Best Practices for Managing Passwords: Formation" and "Best Practices in User ID Formation"). Password usage guidelines define acceptable user and system administrator behavior in the areas of password secrecy and integrity throughout the password life cycle (see "Best Practices for Managing Passwords: Usage Guidelines").

Deploy password management technologies and technical safeguards. The operational implementation of a password management policy requires the deployment of technologies that reduce user and administrative burdens, as well as techniques that protect passwords from internal and external attacks. Password synchronization and single sign-on technologies can significantly reduce the password management burden (see "Best Practices for Managing Passwords: Tools"). Self-service password reset technologies can dramatically reduce the volume of help desk calls relating to passwords (see "Best Practices for Managing Passwords: Self-Service Q&A"). Finally, IT security organizations must understand the different internal and external attacks against passwords and users, and implement technical safeguards (see "Best Practices for Managing Passwords: System Security").

IT security organizations that implement these policy and technology best practices will achieve a required foundational element for a secure IT environment: effective and efficient password management.

Mark Nicolett

Vice President, Research Director

securitymember@gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509