

Securing a Dynamic Network

How to Safeguard Privileged Access to Changing Applications and Hardware



Summary

The IT managers at a large US healthcare provider believed the network was secure until an audit uncovered servers and applications that were deployed without basic safeguards. In one case a server that was hosting a clinical trial application at one laboratory had been configured with null administrative passwords that made sensitive patient data available to anyone with physical access to the machine.

The staff was concerned that without a means to continuously detect non-compliant hardware and applications as they were deployed on the network, the organization risked data breaches and failed compliance audits.

This paper outlines the security risks that can arise when new computers and applications are deployed on a network. It describes the steps that organizations can take to secure privileged identities on new and changing platforms, and presents a study of how one organization developed processes to eliminate risks posed by new hardware and software deployments.

Dealing With Too Much Change

Whenever new hardware and applications are deployed they can introduce unforeseen security risks. Shared and widely-known privileged account passwords are introduced through deployment scripts, ghosted images, default appliance credentials and developer "back doors." And by not always documenting every privileged account credential embedded in their products, hardware and software vendors can also introduce a slew of security holes.

Once discovered, changing privileged passwords that are present in embedded service accounts, system logins, and elsewhere introduces a risk of disrupted service and system lockouts in the event that other, dependent services fail to be updated. As one network appliance vendor said,

"Our appliances monitor the core switches at the majority of the Fortune 500. Years after deployment, customers have told us that they haven't changed the default logins and privileged service account passwords on these devices. Many of those organizations – including supposedly PCI DSS compliant ones – either don't know how to find all of the privileged service accounts on the appliances or are unwilling to make changes for fear of causing service outages."

Regulatory standards covering virtually every industry require you to have a process in place to discover and manage every privileged account introduced by new operating systems, applications and services. For example, PCI-DSS, HIPAA, and others require default passwords to be changed before new computers and applications are deployed.

Despite these standards, few organizations are able to comply because:

- Identity access management (IAM) frameworks from leading vendors like Microsoft, Oracle, IBM, Sun, and others don't detect or control privileged identities.
- Organizations that lack automated processes to maintain complete, authoritative lists of the systems, applications and services where these credentials reside, and can't chart their interdependencies.
- Since privileged account interdependencies are rarely documented, changing a single privileged password has the potential to lock out other, dependent services that share the same credentials. The result can be cascading system failures and disruptions in critical business services.

Regaining Control

A single server can have privileged identities present in local and domain accounts, in configured services and scheduled tasks, and in a wide range of applications including COM+ and DCOM applications, IIS websites, databases such as Oracle, SQL Server, and so on. Multiply these by the many computers and network appliances present in your organization to get an idea of the difficulty to manually document each account and its interdependencies, and to change each account password frequently enough to comply with regulatory mandates.

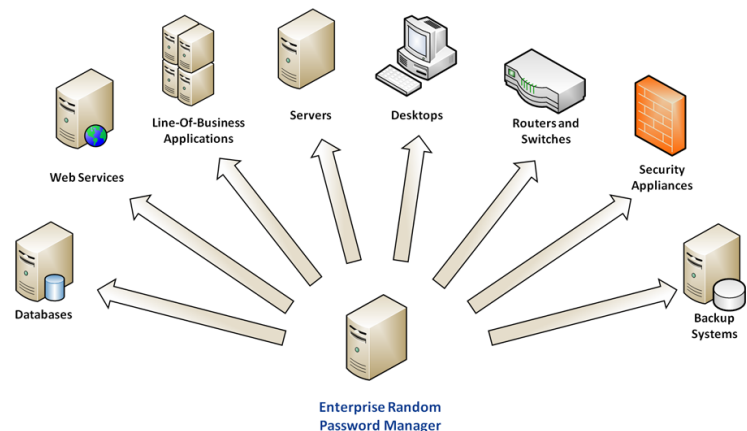
Fortunately automated processes exist that can reliably help organizations regain control in a cost-effective manner. The processes can be described as four key steps that are abbreviated as *I.D.E.A.*:

- **Identify** and document all critical IT assets, their privileged accounts and interdependencies.
- **Delegate** access to credentials so that appropriate personnel, using least privilege required, with documented purpose, can login to IT assets in a timely manner at designated times.
- **Enforce** rules for password complexity, diversity and change frequency, synchronizing changes across all dependencies to prevent service disruptions.
- **Audit** and alert so that the requester, purpose, and duration of each privileged access request is documented and management is made aware of unusual events.

Privileged identity management software can automate the task to track an organization's privileged accounts, change privileged passwords according to the organization's policy, facilitate rapid password recovery so that IT staff can perform routine services and emergency repairs, and change each privileged password after check-out to prevent unaudited access.

Lieberman Software Solution

Enterprise Random Password Manager (ERPM) is software that discovers, updates, stores, and allows secure recovery of every local, domain, and process account in an organization. It detects and reports every location where privileged accounts are used – including local and domain accounts, configured services scheduled tasks, applications including COM+ and DCOM, IIS websites, databases such as Oracle, SQL Server, and so on – and then rapidly propagates password changes everywhere that each account is referenced in order to prevent account lockouts and service failures that can occur when manual processes create obsolete credentials.



Enterprise Random Password Manager (ERPM) Identifies a Wide Range of Privileged Accounts and Interdependencies

ERPM identifies, safeguards and manages the privileged identities found throughout the IT infrastructure, including:

- **Super-user login accounts** utilized by individuals to change configuration settings, run programs and perform other administrative duties.
- **Service accounts** that require privileged login IDs and passwords to run.

- **Application-to-application passwords**, the credentials used by web services, line-of-business applications, custom software, and virtually every other type of application to connect to databases, middleware, and other application tiers.

ERPM secures its passwords in an encrypted database that can be accessed from any web-enabled device. Users check out privileged account passwords through an automated processes that takes advantage an organization's existing identity access management framework to allow expedited, delegated access. Passwords are automatically re-randomized after check-in, and restricted recovery periods, forced check-ins, periodic verifications, web session timeouts, and phonetic spelling options are provided.

Customer Case Study

Lieberman Software was first contacted by a US healthcare provider after an IT audit revealed problems with the security settings on hardware and applications at various sites. For example, a lab server at one remote clinic had null administrative passwords that granted anyone with physical access to the machine the ability to view and modify patient records and sensitive trial data.

Following the audit, IT managers in the organization were eager to close any remaining security holes. They said their priorities were to:

- As quickly as possible, remediate any remaining privileged account vulnerabilities.
- In the future, when new hardware and software components will be deployed anywhere on the network, detect the presence of these resources, scan them for any privileged account vulnerability, and immediately remediate the issue.
- Strengthen existing privileged password controls, without disrupting any IT services, to prevent access by unauthorized personnel or malicious programs.
- Monitor and control administrative access to servers and applications.
- Spend less time preparing for future IT compliance audits.

After deploying Enterprise Random Password Manager (ERPM), one of the organization's IT managers reported that the software achieved the team's goals of finding and remediating insecure privileged accounts throughout the network. The manager said the team was surprised by how many issues had been detected and remediated by the product; specifically, ERPM helped find and address privileged passwords that had been unnecessarily shared among different servers and applications; and, numerous privileged accounts that were present but stale (unused).

The manager reported that the product helped the team achieve its goal of remediating these issues without any service disruptions as a result of the process.

Next Steps

Organizations that desire more insight into potential risks of the unsecured privileged accounts in their IT environments can contact Lieberman Software for an ERPM software trial. ERPM documents potential risks present in the infrastructure, enumerating privileged accounts by hardware platform, account and service type. It then continuously secures privileged accounts everywhere on your network and provides an audit trail of each access request. ERPM trial software is available at no cost to qualified organizations. For more information, email ERPM@Liebsoft.com.

About Lieberman Software

Lieberman Software Corporation, established in 1978 as a software consultancy, has been a profitable, management-owned organization since its inception. Lieberman Software pioneered privileged account password management software, releasing its first product to this market in 1999. Since that time, the company has continuously updated and expanded its privileged password solutions while growing its customer base to include many of the world's most secure enterprises.

Lieberman Software is a Microsoft Gold Certified Partner and has technical partnerships with such other industry leaders as Cisco, Novell, Red Hat, Hewlett-Packard, IBM, RSA and Intel. The company is headquartered in Los Angeles, CA, and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States.

For more information, visit www.liebsoft.com
or call 800-829-6263 (USA and Canada) or 01-310-550-8575 (International).