Privilege User Account Management using Strong Authentication
Privilege Account Problem

“67% of privileged accounts across the global enterprise are either unknown or unmanaged correctly”

“51% of Privilege Account Passwords are shared”

IT environments deal with many different types of passwords: network device passwords, storage device passwords, local account passwords, Windows local administrator passwords and Linux root account passwords. Passwords can be easily snooped, phished, cracked, guessed or even shared - so is the user logging in, really who they claim they are? Privilege user accounts with special permissions authenticate with just a password. Such environments, though considered acceptable till now, is becoming a risk that can severely damage the reputation and integrity of an organization. Today, these risks lay their foundation on “HOPE” - hope that such accounts are used only for its intended purpose, hope that passwords are changed at regular intervals to meet compliance needs, hope that people would not share credentials among each other, hope that every individual always carries a unique identity and finally, hope that people would not use it for malicious activity after they leave the organization.

Some organizations have delegated the management of service and administrative account passwords to a security team or even a single person, thereby, converting a highly trained security engineer to a full-time password resetter. But is this right resource utilization or right way of meeting compliance and regulations?

But then an obvious question would be why? This is because when a new security policy is added or an existing security policy is modified on a network device, it must not distort the accessibility rights of remote users. Otherwise, the security policy could be disastrous, impacting hundreds of users and hurting business productivity. Most administrators are aware of this but the larger the organization, the more painful this process is.

Managing privileged in controlled and regulated environment can be a complex job, and can make a “simple” task, like applying a software patch, complex process that would introduce risks beyond our imagination.

86% of large Enterprises do not know or have underestimated the magnitude of their privileged account security problem.
EPMCOM’s Multi-Factor Authentication: Strong Authentication for Privilege accounts

To effectively comply, control and monitor all privileged user logins, organizations should consider deploying Multi-Factor authentication solutions for all privileged user sessions. Once all privileged session logins are forced through additional level of authentication, organizations can make the user identity fool-proof. An ideal solution would also enable interactive search so that audit and security teams can quickly and easily locate specific activities and incidents. With such a solution in place, organizations can effectively address compliance requirements, speed up audit time, reducing costs.

EPMCOM’s Multi-Factor Authentication Platform supports the choices that enable organizations to strike the right balance between security, cost and convenience to meet their IT challenges. Offering a multitude of authentication methods, organizations have the versatility they need to deploy risk appropriate security that effectively protects their access to critical resources, network, system and cloud-based applications.

Protect your IT environment

- Windows Environment
- VMware Environment
- Remote Access VPN Environment
- Application Virtualization Environment
- WiFi Environment
- ERP Applications
- E-mail
- Web applications for websites, blogs, and team collaboration
- Cloud applications
- RDP, SSH
- PAM, Identity Provider software

EPMCOM’s Multi-Factor Authentication Platform can be integrated with most devices and systems that support RADIUS for authentication. We’ve verified RADIUS compatibility with a wide variety of vendors and devices, including but not limited to:

- Cisco ACS / ISE / ISR / Catalyst / SSH Network Device Access / IPsec VPN / ASA
- Juniper and Pulse Secure SSL VPN
- FS BIG-IP VPN
- Citrix NetScaler Gateway (XenDesktop/XenApp)
- Palo Alto IPSEC and SSL VPN
- SonicWALL TZ, NSA, SMA, SRA, and Aventail series
- VMware View

EPMCOM has several configurable modes and options available for RADIUS.

EPMCOM’s Multi-Factor Authentication Platform can be easily added to any Unix system to protect remote (SSH) or local logins with the addition of a simple pam_radius module. It has been tested on Linux (RedHat, Fedora, CentOS, Debian, Ubuntu, Amazon Linux), BSD (FreeBSD, NetBSD, OpenBSD), Solaris, and AIX.

EPMCOM also integrates with Microsoft operating system – Windows Server 2008, 2012, 2016, Windows 7, 8.1, 10 for Strong Authentication on Login, RDP. Additionally, Outlook Web App (OWA), SharePoint, other IIS web applications.

By implementing EPMCOM’s Multi-Factor Authentication Platform that supports the vast majority of IT systems, you can prevent users from bypassing or sharing credentials and store the audit histories. Organizations can more easily comply with regulatory requirements and effectively audit & investigate incident with reduced costs.
EZMCOM is a security access provider for innovative and easy-to-use technology that can be deployed to protect users, data, and applications from credential theft, account takeover and breaches. EZMCOM is working with companies worldwide to change the way we authenticate and authorize — across mobile devices, servers, workstations within enterprise and cloud services.

If you have questions, or would like a demo of EZMCOM’s authentication solutions, talk to an EZMCOM representative today!

1 (510) 396-3894 | 60 (0) 12 570-1114