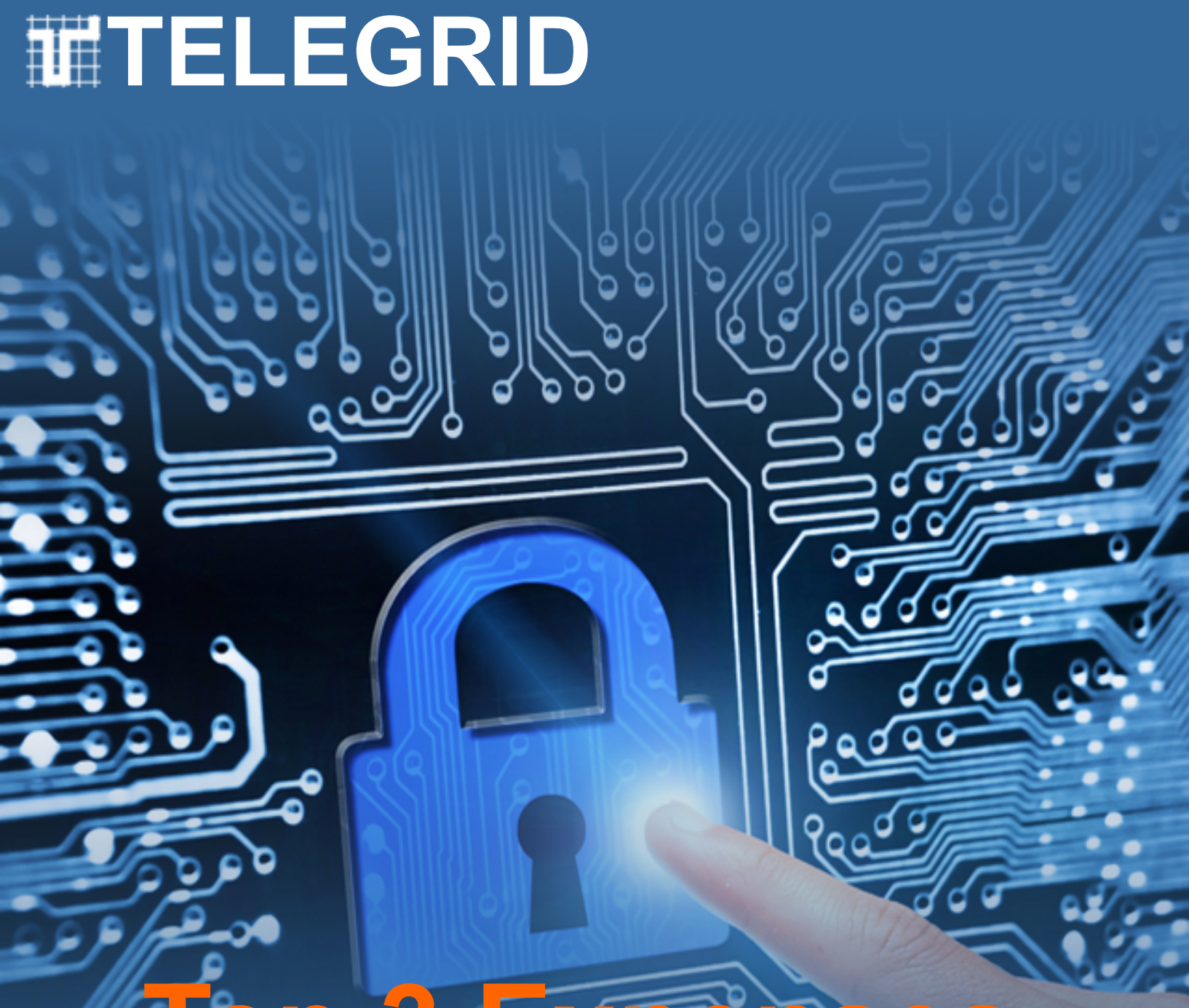
TELEGRID



Top 3 Expenses From Two-Factor Authentication for Privileged Access

TELEGRID

This paper describes the top 3 expenses involved in deploying Two-Factor Authentication (2FA) to protect Privileged Access and prevent insider threats. We have seen 2FA use increase for remote access into networks (e.g., VPN, remote desktop) but its use for Privileged Access inside of a network is still limited. Indeed Gartner estimated that, as of 2015, Privileged Access Management systems had only been deployed by 20% of companies. This is in sharp contrast to general 2FA adoption which is over 50%, according to Gemalto. TELEGRID believes that this disconnect is due to the 3 expenses described in this paper.

THE CASE FOR 2FA

The security issues surrounding use of passwords are well documented. According to a 2015 IBM study, 63% of data breaches were caused by weak passwords. Another concern is the reuse of passwords among both secure and unsecure applications. Companies have tried to combat weak passwords and password reuse by requiring complex passwords and periodic password changes. However, password complexity only frustrates employees and forces them to store passwords in unsecure manners, like in unencrypted excel worksheets. Taking liberties with network security is one symptom of what NIST refers to as "security fatigue". The answer to securing access to network devices and applications is 2FA. So why aren't companies deploying 2FA inside of a network to protect Privileged Access?

Top 5 Passwords from the Adobe hack:

- 123456
- 123456789
- Password
- Adobe123
- 12345678

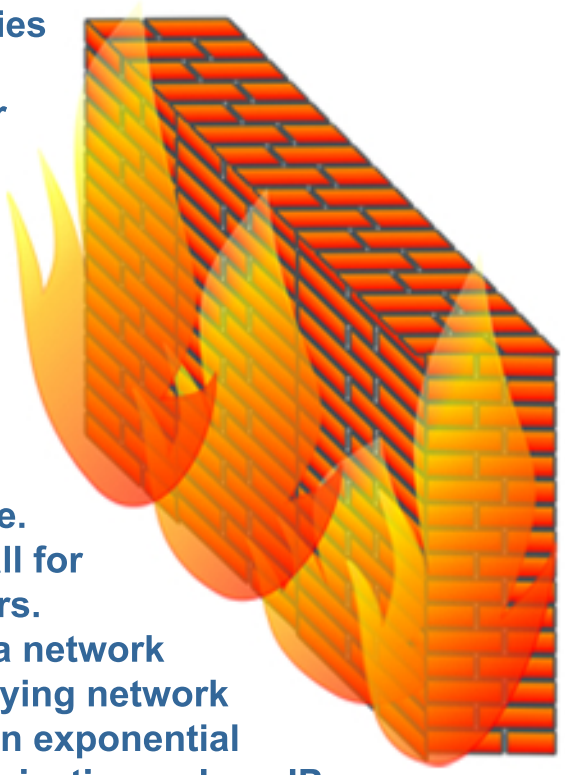
EXPENSE #1 – ADDING CLIENT SOFTWARE

In order to facilitate 2FA, vendors require the installation of client software on a network device or application. When a user attempts to log in, the client software speaks to a central server to authenticate the second factor (e.g., OTP, OOB, hard token). Each network device and application requires its own specific client software based on access type (e.g., web server, SSH, etc.) and manufacturer.

Deploying client software requires administrators to upload and configure software on potentially thousands of devices with each instance tested to ensure that there are no

issues. Additionally, in cases where client software is unavailable, full software redesigns may be necessary. Finally the client software must be maintained to correct any bugs or vulnerabilities.

EXPENSE #2 – ADDING NETWORK BARRIERS



To avoid the expense of adding client software, companies deploy network barriers including firewalls, gateways, jump servers, or reverse proxies. In this scenario a user will log into the network barrier with 2FA and then be given access to underlying network devices and applications. These network barriers prevent the possibility of brute force password attacks by "hiding" network devices and applications. This approach basically recreates the concept of a VPN but this time inside of a network.

The problem is that these network barriers are expensive. They are priced based on network capacity with a firewall for large networks costing in the tens of thousands of dollars. Additionally, deploying these network barriers requires a network redesign, including changing the IP addresses of underlying network devices and applications. Network re-architecting has an exponential effect when taking into account server to server communications where IP addresses must be changed throughout the network. Finally these network barriers raise the cost of business operations due to increased latency and network bottlenecks.

EXPENSE #3 - PASSWORD VAULTS

Once companies have established a network barrier in front of network devices and applications, as described above, they store the underlying passwords in a password vault. In this scenario, the user logs into a network barrier with their 2FA and the network barrier accesses a password vault to retrieve the underlying password.

While a password vault is typically secured, consolidating all passwords creates a simple target for hackers. Indeed, there have been several high profile cases where a

TELEGRID

password vault was hacked giving hackers unfettered access to all network devices and applications. Therefore, companies must secure and maintain password vaults, which is an added cost when deploying 2FA. Additionally, the passwords in a password vault must still be changed, based on company policy, requiring the purchase of a password manager. Finally, since the passwords are unknown, if a password vault fails then an administrator may be required to perform a factory reset to access the underlying network device or application.

SMRTe

TELEGRID's SMRTe was designed specifically to overcome the 3 expenses from 2FA for Privileged Access. The SMRTe sits seamlessly between users employing a 2FA solution (e.g., RSA SecurID, Smartcard, etc.) and network devices or applications.

The SMRTe does not require the installation of 2FA client software on network devices and applications. Additionally, TELEGRID's patent pending technology provides secure authentication without the use of a firewall, a gateway, a jump server or a reverse proxy. After users are authenticated and authorized by the SMRTe, they access the network device or application directly thereby removing the potential for any bottlenecks or latency. Even though devices and applications do not "sit behind" the SMRTe, its revolutionary design ensures that hackers cannot perform a brute force password attack thereby eliminating the need for password vaults.

The SMRTe is a scalable virtual machine which can be configured for small, medium and large organizations.

TELEGRID Technologies Inc.
23 Vreeland Road
Florham Park, NJ 07039
973-994-4440
sales@telegrid.com
www.telegrid.com