Building a Cyber Strong America

PREPARE. DEFEND. STAY SECURE.

#CybersecurityAwarenessMonth

Red River

When we look across public sector, critical data, public works and essential infrastructure systems, and proprietary intellectual proprietary are all protected by logins – which is why password best practices are always the first step in a strong cyber culture.

PASSWORD BEHAVIOR CAN PREVENT CYBER RISK

NIST guidance recommends that a password should be at least 15 characters long. At 100 billion guesses per second, it would take a computer more than five hundred years to guess all the possible combinations of 15 lowercase letters.

It's best to adopt passphrases over passwords, which combines multiple real words together to create something that's easier to invent and remember.

Have fun with it. Make your passphrase funny or an inside joke or a series of words that only make sense to you, it's a chance to be creative and protect yourself and your organization.

Read our latest blog on Cybersecurity Awareness across your organization.

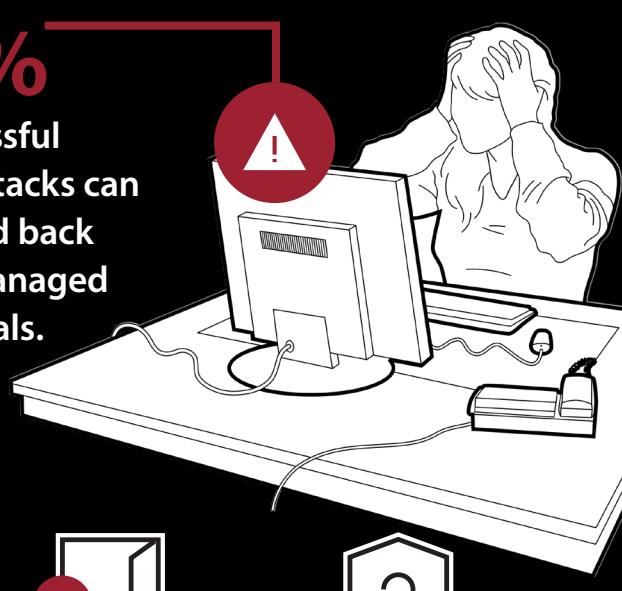
Strengthen Zero Trust Strategies with Privileged Access Management

Up to 50% of successful cyber-attacks can be traced back to mismanaged credentials, and when it comes to privileged accounts, the consequences can be even more devastating. The Zero Trust model is built on identify and access management at its core. Mismanaging privileged accounts can open the door to a wide variety of attacks from insider threats to ransomware.

Up to

50%

of successful cyber-attacks can be traced back to mismanaged credentials.



5 MOST COMMON SECURITY MISTAKES OF PRIVILEGED USERS

Mismanaging Passwords

Disabling or Not Using MFA

Sharing Privileges with Others

Using Admin Accounts Excessively

Ignoring Cybersecurity Policies

Our Zero Trust multi-vendor demo environment is based on the CISA models where we can showcase different solutions working together to enhance security.

Watch our video from the demo lab to explore a real-world example.

Create a Concrete Process for Zero Trust Customized to Your Organization

Integrating with complex legacy systems, managing network segmentation, navigating new policies and regulations, staying ahead of cyber threats, and safely integrating AI technologies – the list of challenges on the Zero Trust journey are many.

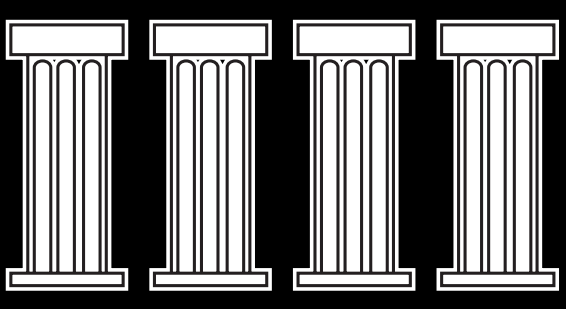
Organizations that engage in a Zero Trust workshop find a concrete process for organizing this complexity including:

- Which existing vendors map to the Zero Trust framework
- Any current gaps in technology
- How to optimize existing or identify new vendors needed to address Zero Trust controls
- The order of priority for addressing each control
- When controls need to be in place and what level of maturity is required to meet federal mandates (for federal agencies and Department of Defense)

Read our latest blog, You Are Here: Finding Your Way on the Zero Trust Roadmap

Meet Federal PQC Policies

Federal migration to Post-Quantum Cryptography (PQC) is now a policy-driven priority. Although today's quantum computers aren't breaking mainstream encryption yet, the "harvest-now, decrypt-later" threat elevates risk to long-lived sensitive data.



AGENCIES SHOULD FOCUS ON FOUR PILLARS IN ALIGNMENT WITH POLICIES:

Inventory-first

OMB M-23-02 tells FCEB agencies to build a prioritized inventory of cryptographic systems and keep updating it.

Crypto-agility by design

NSA's CNSA 2.0 policy and advisories set concrete timelines for moving NSS to quantum-resistant algorithms

Risk-based sequencing

M-23-02 emphasizes a prioritized inventory.

Automation with continuous assurance

M-23-02 tasks CISA to publish a strategy for automated discovery; CISA's ACDI Strategy specifies using ACDI tools and integrating results with federal reporting.

Download our latest guidance on Evaluation Criteria to Meet Post-Quantum Cryptography Policies.

Red River

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing more than 25 years of experience and mission-critical expertise in managed services, AI, cybersecurity, modern infrastructure, collaboration and cloud solutions.

Learn more at redriver.com.

12670