How to Protect the New Perimeter – Identity Access Management

Identity Access Management (IAM) is a significant component of any digital security strategy. The IAM framework controls user access to critical data and can regulate role-based user access to systems and networks. IAM is the most vital component of a security plan; it stops the bad actors at the front door. If your security plan doesn't lead with IAM, it is like leaving your keys in the front door.

Understanding the Fundamentals of Identity and Access Management

The critical components of IAM are:

1. Identification - The first step in IAM is identifying who is trying to log in. If you are not using a biometric, you have a tremendous vulnerability.
2. Authentication – The next step is to authenticate that the individual is who they claim to be.
3. Authorization – The final step is to allow and regulate users' access according to their roles and responsibilities and govern the permissions set for access from different infrastructures (cloud, on-premise, or hybrid) and devices (tablets, smartphones, etc.).

IAM authenticates, authorizes, and audits access privileges ensuring only approved users can access critical systems and assets. This is done by establishing a single digital identity for every individual, which can manage multiple accounts.

The ability to control access to an organization's assets and access in and out of the network is vital to securing an environment. In addition, IAM solutions help organizations meet industry compliance requirements and help save costs by minimizing the time needed to deal with user account-related issues. IAM can also automate critical aspects of managing identities, save IT departments time and money, and reduce risks.

Benefits of Using V2verify for IAM

V2 Eliminates Passwords

If you are using passwords, PINs, challenge questions, etc., as part of your IAM or PAM process, you're not improving your current process. Your security is only as good as the weakest link, and keeping passwords in the equation doesn't make sense! Not when 81% of all data breaches resulting from a hack are tied to compromised credentials. Using V2verify to identify and authenticate users removes the vulnerability and inefficiency of passwords, PINS, and Knowledge-Based Authentication (KBA) from the IAM process. Adding V2 improves security and IT efficiencies by eliminating the task and overhead of managing passwords. V2 also provides an SSO with built-in double authentication, significantly improving the user experience.

V2 Regulates Privileged Account Access and Profile Management

Generally, organized attacks target privileged accounts. Once a privileged account is compromised, it increases the chances of a massive security breach. Social engineering and phishing attacks are common ways of tricking privileged users into sharing their credentials. This is where a robust set of controls can significantly reduce the attack surface.

V2 Automates Access Privilege Assignment

It is essential to establish an automated workflow to assign new employee privileges based on roles and rules and automatically revoke privileges once they resign or are terminated, ensuring all privileges will be taken away automatically. This practice helps control access and prevent unnecessary privileges on abandoned or phantom accounts. Access management, when done manually, can take a lot of time. Automating this process can reduce expenses and human errors.

V2 Audits and Controls

In a well-designed IAM system, there is an audit and control process. Organizations need to implement a strategy where they periodically review who has access to what and determine whether they should still have the permissions.

V2 Provides Better Risk Management and Reporting

It is critical for businesses to report on "Who has access to what, from where, when, and how?". V2 provides this functionality and governs data access, so users can only query and report on the data they are responsible for. This is instrumental in meeting data compliance regulations and guarding against data leaks.