SILVERFORT

Why Identity Security Is a Necessity

Identity security has become a top priority for all organizations. Traditional identity controls do not provide complete coverage, leaving critical resources exposed to malicious access and attacks that use compromised credentials, like lateral movement or ransomware. By not taking a proactive approach to identity security, you will always be one step behind malicious actors.

Here are the key foundations of identity security that you should focus on.

Understanding Your Environment

Without a clear understanding of the different users and their activities in your environment, you will not be able to identify any potential risks, identity threats or security gaps. Complete visibility is the first step to understanding what is in your environment. With full visibility, you will be able to view and manage all human users, non-human identities, service accounts and identify security risks associated with each user account – and gain actionable insights from that information. You can detect who is accessing which resources as well as what authentication protocols are being used and what risks they entail. Without full visibility into user and authentication activity, access permissions and risky identities, you could be leaving critical security gaps without even knowing it.

KEY BENEFITS

- Complete visibility enables organizations to have a full understanding of the different types of users (human, machine-to-machine, non-human identities) and resources in their environment
- Empowers organizations to understand the different risks their users pose
- Alerts on the key risks and highlights where you need to mitigate them

Prioritizing Identity Risks

After gaining full visibility into user authentications and activities, you can start mitigating the risks they pose. Security gap prioritization will help you to identify the most critical areas and move down the line. By focusing on privileged users and users authenticating through insecure protocols, you will be able to prioritize these security gaps first. It is important to address these critical areas immediately to protect your organization's environment and prevent any further risks or threats.

KEY BENEFITS

- Prioritization helps to identify the most critical areas to address
- Apply stronger authentication requirements for privileged users and those who use insecure authentication protocols
- Continuous monitoring helps manage access activity and detect malicious activity

Applying Strong Security Controls

Once you have complete visibility into your environment and understand your security risks, it is time to apply security controls. By adding security controls like MFA, deny access policies, and more, you will be able to verify users' identities before approving or restricting their access requests. By implementing identity segmentation to your user base, you can isolate user access based on their roles, ensuring individuals have access to the resources according to their job functions. Additionally, by adopting the least privilege model across your environment, users will have the minimum permissions required to perform their tasks. With the implementation of security measures across all users and resources within your organization, you can ensure your users and resources are secure while strengthening your security posture.

KEY BENEFITS

- Categorizing users and applying security controls to individuals and user groups reduces the risk of unauthorized access
- Limiting user access to necessary resources decreases the potential impact of compromised credentials and prevents privilege escalation
- Security controls like MFA, deny access and more can strengthen your security posture at the identity layer