IDENTITY

Identity is the new perimeter. Identity management stands at the forefront of today's cybersecurity challenges. The traditional notion of a physical perimeter has become obsolete has become obsolete with the proliferation of interconnected systems, cloud computing, and remote access. Effective identity management is essential for safeguarding sensitive data, protecting against unauthorized access, and ensuring compliance with regulatory requirements such as GDPR and HIPAA.

WHY IDENTITY MANAGEMENT IS CRITICAL FOR YOUR CYBERSECURITY STRATEGY

Control Access

Ensures that only authorized individuals, devices, or applications have access to appropriate resources, systems, or data within an organization's network.

Mitigate Risk

Assign the appropriate access privileges based on users' roles and responsibilities to reduce the likelihood of insider threats, data leaks, and unauthorized activities. Additionally, facilitate the implementation of security policies like password complexity requirements to strengthen security posture and mitigates outsider threats.

Gain Compliance

Identity management plays a crucial role in ensuring compliance with various regulatory frameworks and industry standards, such as GDPR, HIPAA, PCI DSS, and SOX. Maintain audit trails, uphold data protection obligations, and avoiding regulatory penalties and reputational damage by implementing robust identity and access management practices.

Identity Governance

Establish policies and procedures to ensure proper oversight and accountability of identity-related processes, enhancing security and compliance.

Identity Access Management (IAM

Streamline access control and authentication processes to ensure only authorized users can access resources.

Compromised Account Discovery

Proactively identify compromised accounts and mitigate security risks before they escalate.

EntraiD Best Practices

Implement industry-leading best practices to migrate to and managed EntraID (Azure AD).

Privileged Account Management (PAM)

Secure and monitor privileged accounts to prevent insider threats and unauthorized access to critical systems.

Multi-Factor Authentication (MFA)

Enhance security with layered authentication mechanisms, reducing the risk of unauthorized access even with compromised credentials.

ID Validation

Verify the identity of users through robust validation techniques, minimizing the risk of impersonation, social engineering and fraud.

Brite

Brite.com
1.800.333.0498
SalesInfo@Brite.com