ICE Consulting, Inc

IT FOUNDATION CHECKLIST

ICE
TRUSTED IT PARTNER

NO.	SUMMARY	DESCRIPTION OF THE SERVICES	
#1	Deploy SSO (Single Sign-on) & MFA (Multi-factor authentication)	We highly recommend implementing a cloud-based application Single Sign-On (SSO) with industry-standard SAML authentication. This will provide feature-rich dashboards, along with a comprehensive set of security measures to enhance application security. By doing so, you can simplify and streamline the onboarding and offboarding processes, while also bolstering security. Additionally, we will configure multi-factor authentication (MFA) to offer an extra layer of protection.	
#2	Deploy universal directory services as a centralized identity management solution	Implementing Single Sign-On (SSO) necessitates a centralized identity management solution that oversees user management, password security, group organization, and system security. By integrating an Identity Management solution, you can securely regulate access to all resources through centralized permission management, dictating user's resource accessibility.	
#3	Configure secured file sharing	Many startups share information externally or with remote collaborators using public cloud applications, insecure connections, or email, making interception easy. Therefore, it is crucial to establish a secure file-sharing solution protected by your Single Sign-On (SSO) barrier to ensure confidentiality.	
#4	Deploy group policies such as Password Policy	Effectively configure and implement diverse group policies, including password policies, account lockout policies, and more.	
#5	Mobile Device Management (MDM)	MDM enables automated control and robust security of administrative policies on various devices connected to an organization's network, including laptops, smartphones, and tablets. In case of a compromised, lost, or stolen device, quick quarantine measures are implemented to prevent unauthorized access to applications and networks.	
#6	Deploy centralized EDR (endpoint detection and response)	EDR has supplanted antiquated antivirus software, delivering robust protection for company data and users' computers through the implementation of continuous, centralized, AI-driven detection and response endpoint security. This cutting-edge solution not only identifies breaches but also promptly takes measures to nullify the threat.	
#7	Deploy notebook encryption	Endpoint encryption involves utilizing advanced mathematical functions to encrypt data stored on a hard drive. Data within an encrypted hard drive remains unreadable to individuals lacking the necessary key or password. This robust approach shields your systems from unauthorized physical access to the data residing on such devices.	
#8	Deploy centralized, managed endpoint backup	Safeguarding your data from potential loss is paramount, with an enterprise-grade endpoint backup system acting as the cornerstone. By implementing a robust backup solution, all your devices can be shielded, enabling swift recovery whenever needed. This solution seamlessly captures and archives every version of each file across all your computers, leaving no data exposed. Whether through continuous or scheduled backups, the system ensures your files' integrity, preventing any corruption or loss. Trust in this reliable solution to consistently fortify the security of your data.	
#9	Implement email security	Ensuring robust email security is crucial for safeguarding your inboxes against malware, phishing, and spam. It is the industry standard for mailbox security. Take proactive measures by implementing and configuring an email protection system to effectively block spam, phishing attempts, and malware from reaching users' inboxes.	