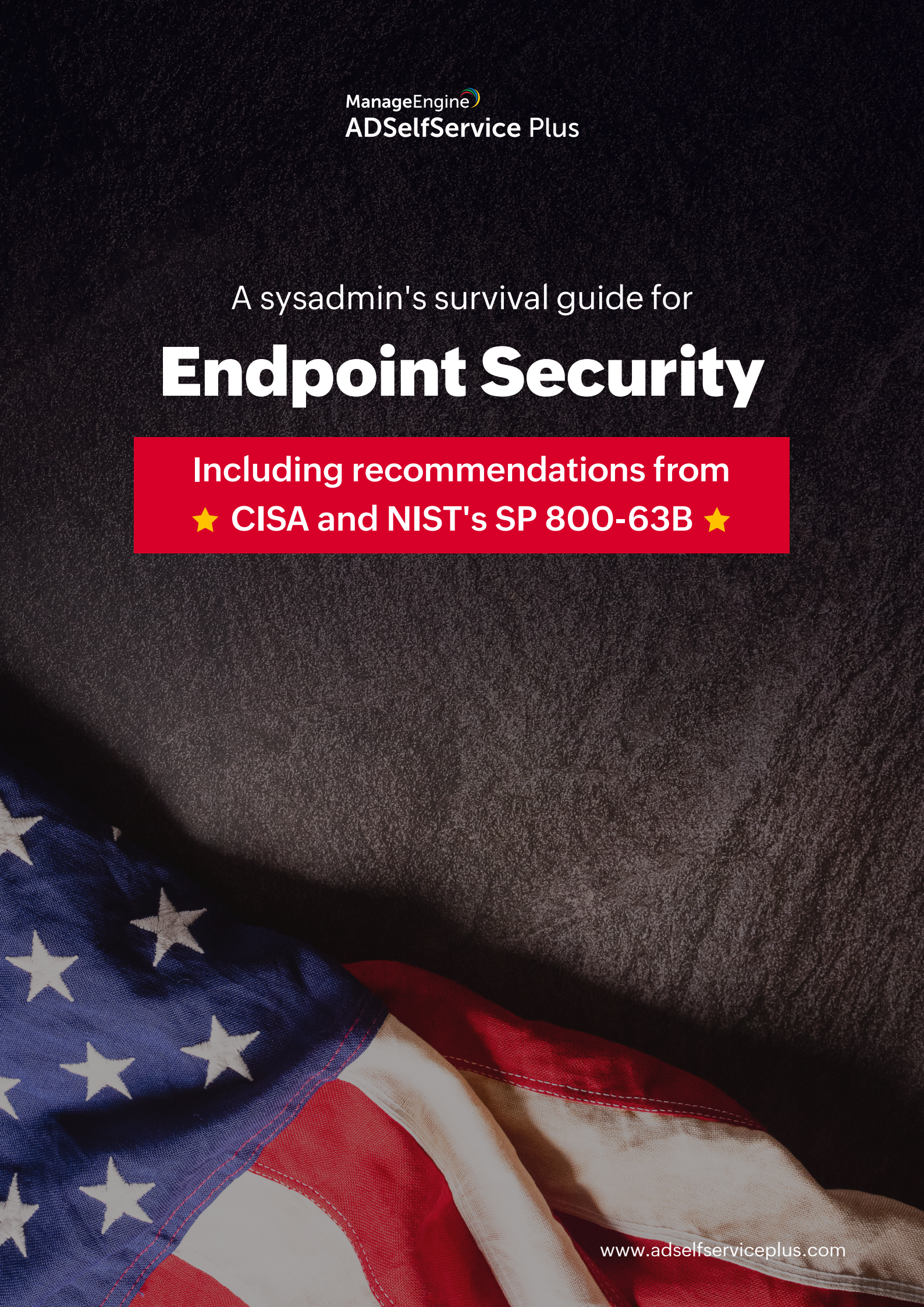
ManageEngine
ADSelfService Plus

A sysadmin's survival guide for

Endpoint Security

Including recommendations from ★ CISA and NIST's SP 800-63B ★



www.adselfserviceplus.com

Table of contents

Introduction

A constantly expanding attack surface is one of the biggest security concerns.

In the past, organizations were required to safeguard their physical location and a small number of devices within it, such as servers, desktops, network devices, and printers. Today, as organizations continue to adapt to the pandemic and implement BYOD and remote work policies, the attack surface is expanding to encompass employees' home networks and personal devices that can access company data, increasing the number of vulnerable endpoints.

All of these are possible entry points for hackers, and when employees work from home, the organization has less visibility over its endpoints, which increases the cyber risks. Thus, endpoints are the weakest link in every business network today, making them susceptible to a range of cyberthreats, such as ransomware and data leaks. Cyberthreats of this nature can cause significant financial losses and severe reputational damage for businesses. Centralized solutions are becoming ineffective, and establishing smart, powerful endpoint security is of the utmost importance to defend an organization and its entire network from cyberthreats.

This e-book discusses how organizations can mitigate risks to their endpoint security by implementing the recommendations of the United States' Cybersecurity and Infrastructure Security Agency (CISA). The e-book also explains how these recommendations can be easily implemented in your organization with ADSelfService Plus, ManageEngine's integrated, self-service solution for password management, MFA, and SSO.

Endpoint security risks in your organization

1. Unsecured Wi-Fi connections

Employees working remotely may find it convenient to send an urgent email to a client, attend a meeting, or access sensitive information while connected to a free Wi-Fi network in a public place. However, public networks are not secure. Because they are open and accessible, hackers can exploit them. Using an unsecured Wi-Fi connection, an attacker can access sensitive information (such as login credentials), install malware, and perform MitM attacks.

2. Unsecured personal devices

Nowadays, employees are transferring sensitive business data to their personal devices and either sharing it via unsecured channels or storing it in applications with inadequate security. Unsecured personal devices can also be stolen or lost, leading to a loss of company data and an increased risk of data breaches.

3. Weak password policies

Weak passwords provide attackers with a greater opportunity to attack an organization and thus pose a massive security threat; using the same password across different accounts and using the manufacturers' default credentials for devices can also pave the way for sensitive or financial data compromise. APT groups target healthcare, academic, and local government organizations to steal sensitive research data and intellectual property designed for commercial and state benefit. A joint advisory by CISA and the United Kingdom's National Cyber Security Centre highlights how APT groups use password spraying and brute-force attacks to gain access to accounts lacking strong, unique passwords. Such attacks also result in user lockouts, causing a denial of service.

4. Single-factor authentication

Using only a single form of authentication increases the risks of unauthorized access and account takeover. Users often fail to store passwords in a secure manner and do not recognize social engineering attacks that aim to trick them into disclosing their passwords. Single-factor authentication can be particularly dangerous for remote desktop users. According to IBM's Cost of a Data Breach Report 2023, 19% of breaches in 2023 were facilitated by compromised credentials. This indicates that using single-factor authentication puts your business at risk for these attacks due to how easy it is for attackers to bypass this security process.

5. Misconfigured cloud services

Application suites that use the cloud, such as Microsoft 365 or Google Workspace, do not have adequate security measures, making them vulnerable to hacking attempts and data breaches. According to Gartner, "through 2025, 99% of cloud security failures will be the customer's fault," with security misconfigurations being a common cause. The most common misconfiguration is the failure to enable MFA. When a user logs in to any cloud application, they should verify their identity by setting up an additional authentication factor (like fingerprints or OTPs). If no additional authentication methods are enabled, and they access the app just by giving their credentials, the account is at greater risk of being hacked. A lack of MFA leaves cloud accounts susceptible to brute-force attacks. Brute-force or password guessing attacks frequently target Outlook Web Access (OWA) deployments.

6. RDP security vulnerabilities

Weak login credentials make RDP systems vulnerable to attacks. Many companies leave password management to their employees, leading to the reuse of device passwords for remote RDP logins. Reused passwords can be exploited by cybercriminals through credential stuffing or brute-force attacks. Also, it was recently reported that Microsoft's RDP is vulnerable to an MitM attack, allowing anyone to connect to an RDP session and take control of other RDP users' systems.

7. VPNs with weak security

Unsecured VPNs expose the entire network to threats, which can lead to security risks like VPN hijacking, MitM attacks, split tunneling, weak user authentication, and malware infections. Using weak passwords from personal accounts or sharing credentials with coworkers creates entry points into your network for hackers. Additionally, VPN servers grant the vendors access to all the applications and data in your network with no checks on access to resources, making it impossible to prove who or what created an issue.

How ADSelfService Plus helps enhance endpoint security

ManageEngine ADSelfService Plus enables Active Directory (AD) password management and SSO for cloud applications. It provides endpoint security through MFA and advanced password policy controls, including biometrics, push notifications, and fingerprint and face ID authentication. MFA is available for Windows, macOS, Linux, VPNs, and endpoints that support RADIUS, including Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway. MFA is also available for OWA, cloud applications, and the Exchange admin center.

To strengthen their network defenses against endpoint exploits, IT admins can use ADSelfService Plus to implement the endpoint security best practices below, which include recommendations from CISA and NIST.

Implement MFA for endpoints

NIST's SP 800-63B recommends that you use two-factor authentication or MFA methods such as TOTPs, Google Authenticator, or RADIUS. CISA also suggests using an additional layer of security beyond the password and username. With ADSelfService Plus' endpoint MFA, admins can ensure that users prove their identities through additional authentication methods for logging in to various systems and applications. ADSelfService Plus supports MFA for the following:

- Machine logins for Windows, macOS, and Linux
- VPN logins
- OWA logins
- User Account Control
- Cloud applications
- Microsoft 365

ADSelfService Plus also offers offline MFA for Windows machines, ensuring the security of offline remote workers during machine logins.

ADSelfService Plus supports 20 different authentication methods for MFA:

1. Security questions and answers
2. SMS verification
3. Microsoft Authenticator
4. Duo Security
5. RADIUS
6. Fingerprint/face ID authentication
7. TOTP authentication
8. AD security questions
9. Zoho OneAuth TOTP authentication
10. Custom TOTP authenticator
11. Email verification
12. Google Authenticator
13. Entra ID MFA
14. RSA SecurID
15. Push notification authentication
16. QR code authentication
17. SAML authentication
18. YubiKey authentication
19. Smart card authentication
20. FIDO2 passkeys

Enforce strong password policies

NIST's SP 800-63B and CISA both provide guidelines for creating stronger passwords that avoid common dictionary words and include eight characters or more, a combination of uppercase and lowercase letters, numbers, and special characters. With ADSelfSerivce Plus' Password Policy Enforcer, admins can customize password policies for users based on their OU, group, or domain membership. Policies can be used to set password controls that are not available in the native policies, like:

- The mandatory inclusion of Unicode characters.
- Restrictions on the repetition of consecutive characters from usernames and old passwords.
- Restrictions on the usage of weak passwords, dictionary words, and palindromes.

Prevent the reuse of stolen credentials

As per CISA guidance, organizations should implement credential hardening measures, such as controls to prevent the use of compromised passwords in the network. Using ADSelfService Plus' integration with the Have I Been Pwned? service, admins can ensure that users do not use stolen passwords during enterprise password resets and changes. The service integration is also enforced on the GINA (Ctrl+Alt+Del) login page and for AD Users and Computers password resets through the Password Sync Agent.

Go passwordless

Admins can enable passwordless authentication for cloud and on-premises enterprise application logins through SSO. ADSelfService Plus' SSO supports SAML, OAuth, OpenID Connect, and custom applications. Implementing ADSelfService Plus' SSO within an enterprise allows users to access all authorized applications by logging in once with one set of credentials. This benefits users by lowering the number of passwords that need to be memorized, thereby reducing password resets and password fatigue and enhancing cybersecurity. Also, IT admins can reduce the number of logins performed by users for applications like Google Workspace, Microsoft 365, and Salesforce.

Enable conditional access rules

CISA recommends that organizations harden their conditional access policies to manage how users connect to the network and cloud services. Using ADSelfService Plus' conditional access rules, admins can restrict which users have access to workstations, applications, and various features (like password changes and directory self-updates) based on risk factors such as the IP address, time of access, device used, and geolocation. Admins can enable specific rules for specific domains, OUs, and groups of users.

Conclusion

Today, it is crucial for an organization to have comprehensive protection that can swiftly detect, evaluate, and stop threats across networks and endpoints to avert business losses. ADSelfService Plus helps in this regard by expanding your protection surface and ensuring that all endpoints, including employee-owned devices, are protected from unauthorized access and potential cyberattacks. This safeguards your organization's vital data and preserves your standing within the industry.

ADSelfService Plus offers the following key capabilities:

1. MFA
2. Conditional access
3. Enterprise SSO
4. Self-service password reset and account unlock
5. Password synchronization
6. Password expiration notifications
7. Password Policy Enforcer
8. Self-service directory update
9. Employee directory search and an organization chart
10. Email group subscriptions

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.
For more information about ADSelfService Plus, visit
https://www.manageengine.com/products/self-service-password.

$ Get Quote Download