SOLUTION BRIEF

REMOTE WORKFORCE SECURITY CHECKLIST

stealthbits
NOW PART OF netwrix

Our New Reality

The rapid change in technology and physical location of users, along with the necessity to sacrifice security for sake of speed in the wake of the coronavirus pandemic, has resulted in a variety of problems for organizations of all shapes and sizes across the world. If not entirely new concerns, existing challenges aligning to data privacy and security, credential theft, and general IT administration have only been exacerbated with the unanticipated rise in remote workers, leading to the following outcomes from many organizations:

A. Lost control of sensitive or regulated data

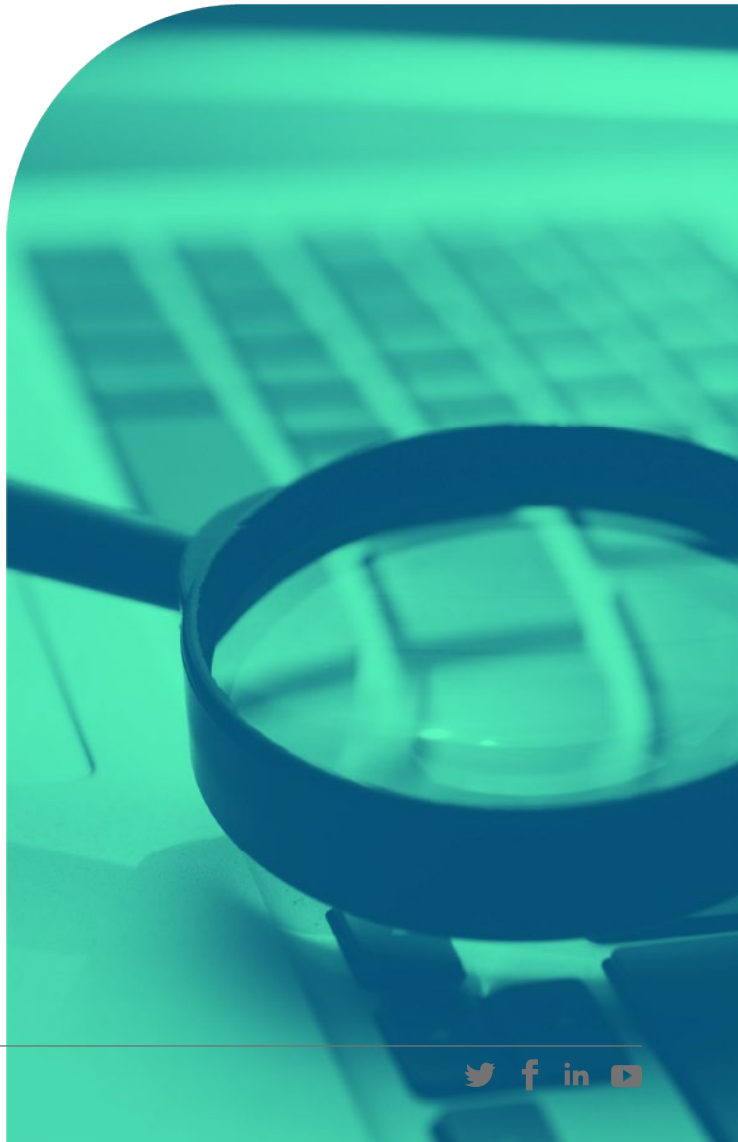
- As a quick fix to the need for network connectivity, many organizations forklifted massive amounts of data to cloud services such as Microsoft 365 and Amazon S3. Was any of that data sensitive? How is it being secured in its new location? Who has access and how? Who is accessing this data? Do unauthorized individuals have access? Is the location of the data compliant with federal, industry, or other regulations?

B. Additional entry points for attackers to your network

- With users logging in from their home networks or perhaps even on personal devices, organizations cannot rely on their enterprise network perimeter to protect critical services like Active Directory from attacks. Are users connecting over insecure protocols? Are system-level settings capable of being exploited? Can user passwords be easily guessed and used to login remotely by anyone?

C. Challenges achieving secure, remote administration

- The way many enterprises have structured their controls were likely not architected for remote administration at the size and scale currently needed. The operational challenges of allowing remote systems administration (e.g. working through firewall zones) may have led to a reduction in restrictions in the vein of enabling remote workforce administrators to do their job. Are privileged users capable of administering systems securely? Given the rise in support cases, have helpdesk admins been given higher level rights to expedite case resolution? Are they leaving administrative account artifacts behind on insecure systems?



Mitigating Remote Workforce Risks

Undoubtedly, there are a wide variety of risks organizations need to address aligning to their new remote workforce. However, the following is a list of some of the top ways to go about mitigating the aforementioned risks both now and when things return to normal.

A: Getting Sensitive Data Under Control

	EFFORT	IMPACT
Identify and classify sensitive information Whether on-premises or in the cloud, understanding which files and/or databases contain sensitive information of virtually any type helps to prioritize risk and provide important context to countless projects, mandates, and questions. **BONUS:** A highly useful and recommended step as part of the identification and classification processes is the identification and assignment of data ownership in all the places sensitive information lives. This allows for and expedites remediation and governance workflows that drastically reduce and even eliminate risk.	HIGH	HIGH
Identify and remediate open access and inappropriate shared access with external parties in the cloud While legitimate in certain scenarios, it is otherwise rare that everyone within an organization would need access to a given resource. Additionally, sharing of content with external entities is often difficult to track, and particularly dangerous when sharing anonymously. Proactively identifying and remediating open access and ensuring externally shared content is configured appropriately and necessary helps to mitigate the risk of more avoidable data breach conditions.	LOW	HIGH
Move and/or Remove Inactive Data Inactive/stale data (especially if sensitive) represents one of the greatest opportunities for risk and cost reduction within any enterprise. Regardless of whether it needs to be retained for compliance purposes, moving or removing stale and inactive data mitigates its exposure and shrinks the attack surface, while also reducing overhead and administrative burden. It's a win for all groups within an enterprise.	MEDIUM	MEDIUM
Monitor user activity for abnormal behavior With the increased variety of ways in which bad actors can compromise accounts due to uncontrollable remote workforce conditions, identifying abnormal data access patterns (particularly against sensitive resources) helps to reduce the opportunity for successful exfiltration of data out of on-premises or cloud environments.	LOW	HIGH

B: Mitigating Threats Caused by New Entry Points

DIRECTORY LAYER CHECKLIST	EFFORT	IMPACT
Enable strong, unique passwords across all accounts In some way, shape, or form, 80% of breaches involve the exploitation weak or already compromised credentials. To mitigate or even eliminate the effectiveness of highly common credential stuffing techniques (e.g. password spraying, kerberoasting) and brute force attacks, ensuring every account continually leverages a strong, unique password helps to drastically reduce the opportunity for easy credential compromise by adversaries.	LOW	HIGH
Monitor for Abnormal Account Activities Whether an initial attempt to compromise an account or the usage of an account already compromised, monitoring for abnormal patterns of behavior indicative of an attacker's presence helps to reduce the opportunity for successful data breach. **Account Takeover Attempts** – Examples include Brute Force, Password Spraying, Kerberoasting, Password Resets **Abnormal Account Usage** – Examples include LDAP Reconnaissance, Lateral Movement, Unusual Logon Activity, LSASS Process Injection	LOW	HIGH
Prevent modification to sensitive security groups, configurations, and policies Attackers not only make changes to obtain higher levels of privilege within an enterprise, but to also achieve persistence within the environment. Preventing modification to sensitive security groups, permissions, configurations, and policies not only reduces the opportunity for attackers to provide themselves back doors into the organization if identified, but also act as an indicator of compromise when alerted upon.	LOW	HIGH
Identify and remediate conditions and configurations attackers look to exploit From accounts set to use reversible encryption to plaintext passwords stored in SYSVOL, delegated permissions to reset passwords or modify group memberships, misconfigured OS-level settings such as LSA Protection or WDigest enablement, and more, attackers look to exploit any weakness in order to move laterally and escalate privileges on their way to complete domain compromise. Proactively identifying and remediating these conditions not only strengthens foundational security controls, but forces attackers to leverage riskier, more visible tactics, techniques, and procedures to execute their attacks, increasing the organization's ability to detect attack signatures and behaviors.	MEDIUM	MEDIUM

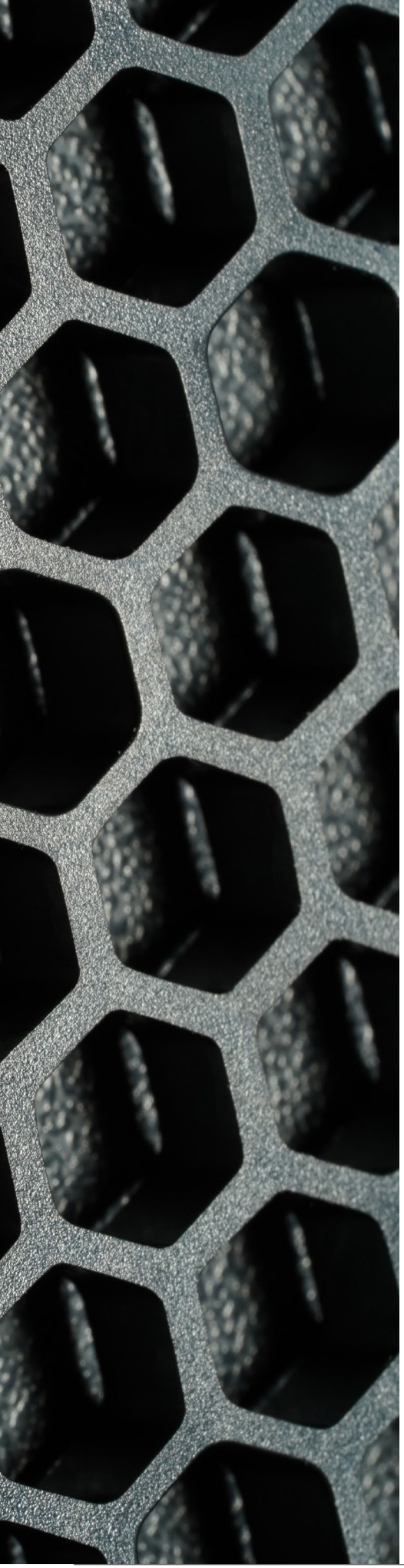
C: Enabling Secure Remote Administration

SYSTEM/SaaS LAYER CHECKLIST	EFFORT	IMPACT
Reduce membership of default privileged groups The theft of "always on" privileges is one of the main vectors attackers use to complete their mission. Reducing (with the goal of eliminating) these privileges is an essential step towards Active Directory security. There should only be one "always on" member of your default privileged groups: the built-in domain administrator user, which is highly protected and only used in emergency situations.	MEDIUM	HIGH
Audit and review privileged accounts granting access to critical infrastructure and applications Proactively identifying and cleaning up privileged accounts across important resources helps to mitigate the risk of privileged account compromise and lateral movement.	HIGH	HIGH
Establish credential boundaries and require multi-factor authentication for privilege use The use of multi-factor authentication and conditional access approaches is necessary to defend privileged access from attackers. Furthermore, establishing credential boundaries -- i.e. not using the same credentials -- across different security classifications is one of the strongest defenses to privilege escalation.	HIGH	HIGH
Use just-in-time activity tokens for member server administrator privileges While using activity tokens at the domain level is predominantly about constraining an adversary's ability to escalate privilege, using them at the member server level is about reducing opportunity for lateral movement (which itself may lead to privilege escalation). Activity tokens on servers can grant access to one or more servers and greatly restrict both the scope and duration of lateral movement risk.	LOW	HIGH

NEED HELP?

Some of the recommendations provided in this checklist may very well be within the grasp of your current capabilities or toolsets. If not, let us know where we can be of assistance – even if it's just advice you seek.

The remote workforce represents a challenge for organizations of all sizes in one way or another. Stealthbits looks forward to tackling the challenge with you.



NEXT STEPS

Schedule a demo
Stealthbits.com/demo

Download a free trial
Stealthbits.com/free-trial

Contact us
info@Stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits