Remediant

REMEDIANT REVEAL

PREPARED FOR “XYZ CORP”

9,859,794*

*INSTANCES OF STANDING PRIVILEGE WITH 24-7-365 ADMINISTRATIVE ACCESS TO SERVERS AND WORKSTATIONS IN YOUR ENVIRONMENT

EXECUTIVE SUMMARY

Remediant would like to thank “XYZ Corp” for the opportunity to collaborate on this assessment in an effort to define privileged access risk and provide recommendations to resolve said risk in the future. This assessment was performed between January XX-XX, 202X and was limited to the “XXXXX” domain, as this is the primary domain for both user accounts and computer objects.

Standing Privilege = Adversary Lateral Movement Risk

TOTAL INSTANCES OF STANDING PRIVILEGE (FROM SYSTEMS SUCCESSFULLY SCANNED)

9,859,794

NUMBER OF UNIQUE ADMIN ACCOUNTS DISCOVERED **40,502**

AVERAGE INSTANCES OF STANDING PRIVILEGE PER SYSTEM	AVERAGE INSTANCES OF STANDING PRIVILEGE PER SERVER	AVERAGE INSTANCES OF STANDING PRIVILEGE PER WORKSTATION
503	**119**	**560**

Any privileged account armed with standing access poses substantial risk as it can be used to move laterally in an organization once authentication has been breached and the credential is in the hands of an adversary. Remediant SecureONE is able to reduce upwards of 99% of standing privileged access records in customer environments, thereby substantially mitigating lateral movement risk.

The data contained herein illuminates the volume and breakdown of persistent “standing” admin risk within the environment scanned and provides recommendations to secure the organization against adversary exploitation of stolen credentials.

ASSESSMENT RESULTS

Infrastructure & Scanning Overview

SecureONE produces continuous discovery and monitoring of your privileged access via daily LDAP sync and continuous enumeration of local admin privilege without the need to deploy any agents. Requiring six network packets of data exchange and 120 milliseconds of time to scan each endpoint on average, SecureONE is purpose-built to scale to the largest of organizational environments and enumerate local admin privilege in unparalleled time. Scan time is critical to ensure changes to access are detected quickly to prevent potential abuse.

"XYZ CORP" Assessment Results

AD COMPUTER OBJECT COUNT	73,357
AD USER COUNT	77,257
AD GROUP COUNT	24,443
AD GROUP CONFERRING PRIVILEGE	19,813
SYSTEMS SUCCESSFULLY SCANNED (WK & SERVER)	19,592
TOTAL TIME TO SCAN ALL COMPUTERS IN DOMAIN (MINUTES)	23.6
AVERAGE TIME TO SCAN EACH HOST (SECONDS)	.0193

Standing Privilege Risk Overview

The first step toward Zero Standing Privilege is quickly and comprehensively illuminating what administrator credentials exist. Within 25 minutes, SecureONE had already cycled through "XYZ Corp's" environment for the first time. SecureONE was allowed to query the environment and gather data for a period of 3 days to minimize the number of offline systems present in the data set.

"XYZ CORP" Standing Privilege Footprint

TOTAL INSTANCES OF STANDING PRIVILEGE (FROM SYSTEMS SUCCESSFULLY SCANNED)	9,859,794
BROKEN DOWN BY SERVER	298,185
AVERAGE NUMBER BY SERVER	119
BROKEN DOWN BY WORKSTATION	956,160
AVERAGE NUMBER BY WORKSTATION	560

Top 10 highest risk accounts via system access

svc.vcac	19,587
adm_aramero	19,587
scom2012	19,587
adm_rarman	19,587
adm_baspen	19,589
adm_tcraft	19,589
dpadmin	19,589
adm_mbjerke	19,565
sccm2012	19,565
srv_ntp	19,560

Top 5 groups with the highest risk of standing privilege exposure

	NUMBER OF ACCOUNTS	SYSTEMS WITH PRESENCE	STANDING PRIVILEGES
INFRASTRUCTURE	59	17,071	1,007,189
DESKTOP SUPPORT	42	17,072	717,024
RDP_USER_ADMINS	25	17,072	426,800
DOMAIN ADMINS	16	19,559	312,944
VMWARE.SERVICEDESK	14	17,074	239,036

Best Practice Violations

SecureONE's unparalleled visibility also enables organizations to identify accounts that violate Microsoft's tiered best practice and expose organizations to risk of adversary privilege elevation. Each of the following datapoints are high-risk violations that should be addressed as quickly as possible and monitored continuously moving forward.

TOTAL NUMBER OF "PRIMARY ACCOUNTS" WITH PRIVILEGED ACCESS (BASED ON CUSTOMER ADM NAMING CONVENTION) **7,373**

TOP 10 "PRIMARY ACCOUNTS" WITH HIGHEST ACCESS

XYZCORP\\PRoberts1	**19,561**
XYZCORP\\PSchutlz	**19,561**
XYZCORP\\AFielder	**17,183**
XYZCORP\\SSweiven	**17,134**
XYZCORP\\JAndrews	**17,134**
XYZCORP\\SPrader	**17,134**
XYZCORP\\TOrvis	**17,120**
XYZCORP\\TBrady	**17,108**
XYZCORP\\DHaas	**17,091**
XYZCORP\\SWolf	**17,088**

NUMBER OF SERVERS WITH DOMAIN ADMIN ACCESS **2,509**

NUMBER OF WORKSTATIONS WITH DOMAIN ADMIN ACCESS **17,083**

*DATA PULLED FROM SECUREONE

POSITIONING “XYZ CORP” FOR SUCCESS

Current State of Privileged Access Security

Breach response data from top firms like Verizon and Mandiant have highlighted a consistent theme over the last decade – privileged credentials are a hot commodity for attackers, being exploited by cyber criminals in 75% of all breaches. The disappointing part, however, is the industry doesn’t appear to be making progress against this statistic as seen over time. In large part, this is because privileged access management solutions are rendered useless once a privileged credential is compromised.

The underlying reason behind this is the *access* the credential provides – specifically, the 24x7x365 always-on, high levels of access that admin credentials allow. When an adversary gains possession of an admin credential, this can be used to move laterally to any system for which the credential has authorization rights, allowing to then modify system configurations, steal sensitive data, deploy ransomware, etc. Unfortunately, the average privileged access management or endpoint privileged management solution was not purpose-built to address the risks associated with this persistent access.

One major gap with traditional solutions is the inability to continuously discover accounts and dynamically monitor the ever-changing authorization rights associated with privileged accounts. Privilege is typically conferred in the form of group memberships or device-level permissions that allow the execution of privileged commands. Even if a user is not explicitly given access to a server or workstation, that user’s domain or group-level permissions often allow access whenever that person needs or wants it. When faced with an IT issue in the workplace, we look for, and expect, the fastest resolution so that we can move forward with our work duties. In the world of permissions, this means access is being provided through groups to IT help desks and server administrators to ensure they can do their job effectively. However, managing these groups at a granular level quickly becomes very complex, so admins always tend to have more access than they need. Lastly, administrator rights change frequently for a multitude of reasons; attackers know this and use it to their benefit. Once authentication has been breached, an adversary may sit for months to wait for the authorization rights associated with the credential to change.

This isn’t the only way the amount of privileged access changes within an ecosystem. For example, old members who leave their teams or the company aren’t always removed in a timely fashion, group memberships change local accounts get added and removed, and the list goes on. In some cases, all of these are traps organizations fall into on a regular basis that ultimately result in an invisible sprawl of administrator access across an enterprise. Not only is 24x7x365 access unnecessary for employees, but, more importantly, it’s available to an attacker using the average employee workstation as the entry point. If an attacker is able to phish their way into an employee’s workstation, that person now has the proverbial “keys to the kingdom.”

Desired Future State – Zero Standing Privilege

In order to effectively reduce the risk of privileged access, we need to continuously answer two simple questions: What admin credentials exist and have standing access? And how do you protect them? Coined by Gartner, Zero Standing Privileges (ZSP) is an emerging, precision approach to privileged access management that addresses both questions.

If we agree that standing privilege is defined as accounts that have persistent privileged access across a set of systems, ZSP is the exact opposite. It is the purest form of just-in-time administrator access, ensuring that the principle of least privilege is enforced by granting authorized users the privileged access they need for the minimum time and only the minimum rights that they need. This elimination of standing privilege through ZSP is really a key inflection point in the understanding of privileged access today.

The first step in a journey toward ZSP is to begin measuring the organization’s standing privilege to understand what administrator credentials exist. This includes discovering and identifying persistent accounts across workstations and servers, as well as mapping out admin access on a system-by-system basis.

Once standing privilege is measured, it can be managed; from there, it is a phased approach to protecting an enterprise environment and achieving ZSP. Start by “stopping the bleeding” by preventing the creation of new rogue administrator accounts. It is critical to have the ability to do this across all types of systems (Windows, Mac, *NIX) and all types of access (local, group, domain). Once the “bleeding” has stopped, it’s time to determine which accounts are authorized and which accounts are not, and to what systems. Unauthorized access should then be revoked, ideally in bulk, to quickly mitigate one of the accounts being compromised.

The last step to achieving ZSP is to shift administrators into just-in-time mode that allows them to gain access to the system when they need to perform required tasks, but only for the right time frame and only to the right system(s). Access should be revoked once the work is complete and only provisioned back (limited to the right system for the right time frame) when needed again.

Required Capabilities

Remediant believes a sound privileged access security strategy shouldn’t take an army of resources to deploy and operationalize. Fast time-to-value and immediate risk reduction is the benchmark we evaluate our company and technology against. One reference customer, Lockheed Martin Corporation, deployed SecureONE to over 150k systems into full ZSP mode in less than 3 months and operationally maintain the solution with 1 FTE. To deliver upon this speed and efficacy, we believe the following capabilities are essential:

Continuous privileged access inventory – To prevent against privileged access accretion and pursue true ZSP, a solution needs to continuously discover and monitor accounts and related access. Periodic interval-based inventory methods can’t effectively manage standing privilege risk.

Agentless architecture - To deliver upon the goals of ZSP and simplify management, an agentless approach across all types of systems (Windows, Mac, *NIX) is of paramount importance. An agentless architecture enables flexibility, scalability and support of zero-time updates.

API-first architecture - Built from the ground up on an API-first architecture via Docker micro services and Mongo DB, SecureONE is purpose-built to simplify integration with other Security, Identity and ITSM technologies.

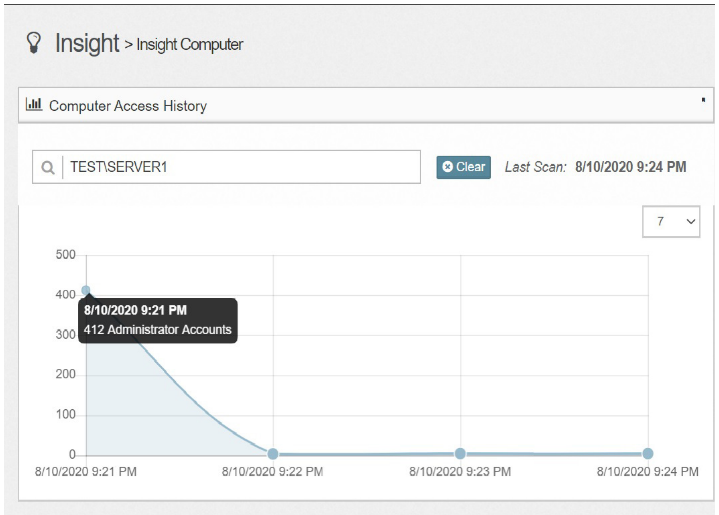
Metrics to Evaluate Success

Historically speaking, evaluating the success of a privileged access management project has been a struggle. With project timelines measured in years with very expensive licensing and deployment expenses, demonstrating quantifiable risk reduction for the business has been hard. A ZSP-based approach, by contrast, enables organizations to easily quantify risk reduction through the maturation of a project. Remediant encourages consideration of the following metrics:

- TIME TO DEPLOY
- NUMBER OF COMPLETE DISCOVERY SCANS PER DAY
- FTE ASSIGNMENT TO OPERATIONALLY SUPPORT SOLUTION.
- NUMBER OF DISCOVERED ACCOUNTS PREVIOUSLY ‘UNKNOWN’
- PERCENT REDUCTION IN STANDING PRIVILEGE RISK
- MEAN TIME TO RESPOND AND REMEDIATE (MTTR) PRIVILEGE RELATED INCIDENTS.

RECOMMENDATION: ZERO STANDING PRIVILEGES

As shown below, SecureONE was successfully tested in ZSP mode by removing 409 standing admin instances from TEST/SERVER1.


Insight > Insight Computer

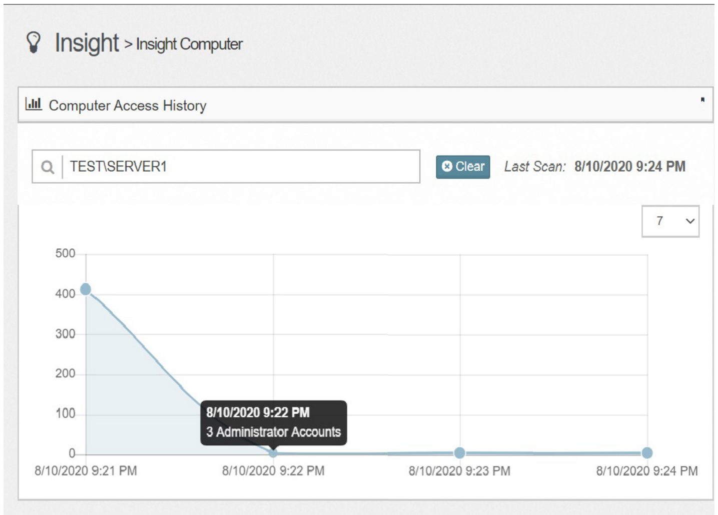
Computer Access History

TEST\SERVER1

Last Scan: **8/10/2020 9:24 PM**

8/10/2020 9:21 PM
412 Administrator Accounts

Figure 1. TEST/SERVER1 pre-ZSP showing 412 admin accounts.


Insight > Insight Computer

Computer Access History

TEST\SERVER1

Last Scan: **8/10/2020 9:24 PM**

8/10/2020 9:22 PM
3 Administrator Accounts

Figure 2. TEST/SERVER1 post-ZSP showing 3 admin accounts, instantaneous attack surface reduction of 99.3%

NEXT STEPS:

1. Limit Domain Admin standing access to domain controllers only (Microsoft best practice).
2. Users and groups with substantial persistent/standing access should be reconfigured to use Just-In-Time access.
3. Eliminate account access that spans workstations and servers –this can enable attackers to cross “tiers” and encounter accounts more likely to have domain-level access, or compromise business-critical server applications.
4. Determine whether each service account requires standing privilege or if JITA provisioned access is possible using automation with SecureONE’s API’s. Evaluate frequency of Service Account usage via AD authentication events.
   - Put Service Accounts into a distinct OU to set specific access controls on the container.
   - Evaluate whether each account needs domain or local account access.
   - Consider which Service Accounts can accommodate dynamic (JITA) access.
   - Grant the remaining Service Accounts persistent access.
5. Quantify standing privilege risk reduction periodically and track over time to reveal trends.
6. Once ZSP is broadly deployed to workstations and servers, engage Red Team or Pen Test to demonstrate efficacy.

Our recommendation is to consider high-risk accounts based on volume and proximity to the adversary. The objective is to evaluate each account from a risk and operational tolerance perspective, to determine a plan for iterating toward ZSP. The visual below represents the deployment process to mature SecureONE within a customer environment.

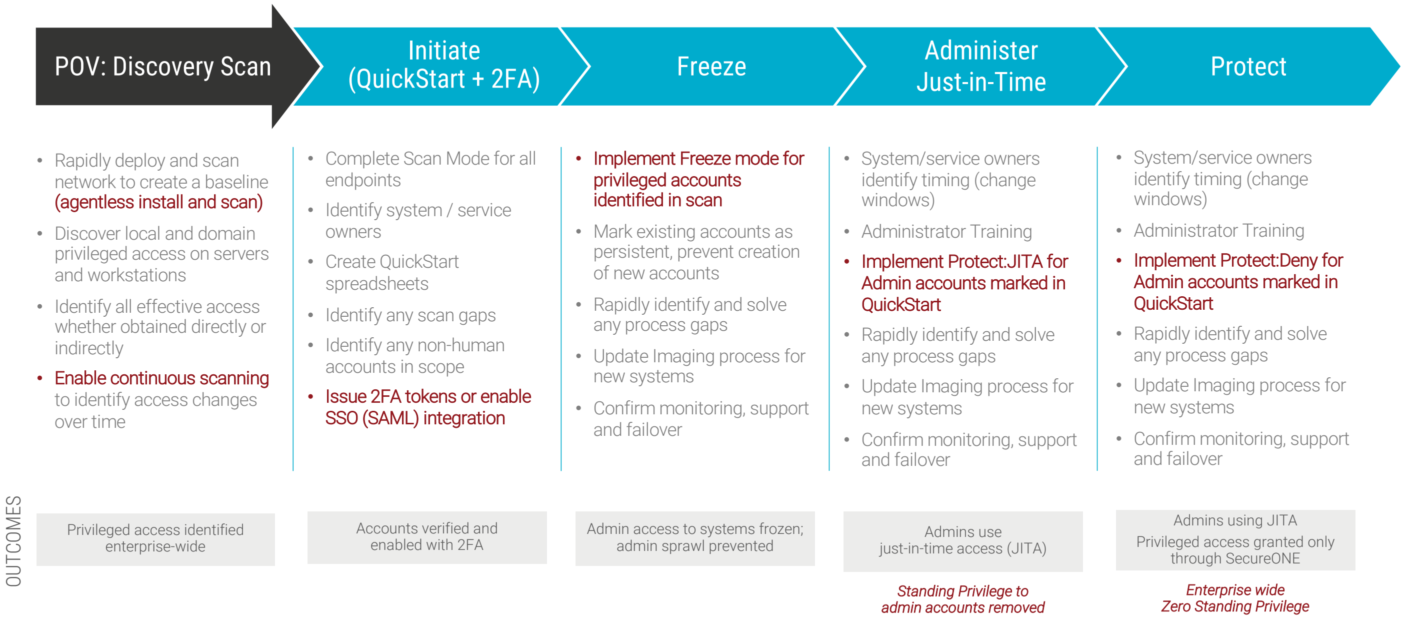

POV: Discovery Scan
Initiate (QuickStart + 2FA)
Freeze
Administer Just-in-Time
Protect
Rapidly deploy and scan network to create a baseline (agentless install and scan)
Discover local and domain privileged access on servers and workstations
Identify all effective access whether obtained directly or indirectly
Enable continuous scanning to identify access changes over time
Complete Scan Mode for all endpoints
Identify system / service owners
Create QuickStart spreadsheets
Identify any scan gaps
Identify any non-human accounts in scope
Issue 2FA tokens or enable SSO (SAML) integration
Implement Freeze mode for privileged accounts identified in scan
Mark existing accounts as persistent, prevent creation of new accounts
Rapidly identify and solve any process gaps
Update Imaging process for new systems
Confirm monitoring, support and failover
System/service owners identify timing (change windows)
Administrator Training
Implement Protect:JITA for Admin accounts marked in QuickStart
Rapidly identify and solve any process gaps
Update Imaging process for new systems
Confirm monitoring, support and failover
System/service owners identify timing (change windows)
Administrator Training
Implement Protect:Deny for Admin accounts marked in QuickStart
Rapidly identify and solve any process gaps
Update Imaging process for new systems
Confirm monitoring, support and failover
OUTCOMES
Privileged access identified enterprise-wide
Accounts verified and enabled with 2FA
Admin access to systems frozen; admin sprawl prevented
Admins use just-in-time access (JITA)
Standing Privilege to admin accounts removed
Admins using JITA
Privileged access granted only through SecureONE
Enterprise wide Zero Standing Privilege

Figure 3. SecureONE deployment process

CONCLUSION

ZSP is an inflection point in privilege management. It is important to recognize standing privileged as a key risk that needs to be addressed and that vaulting secrets and rotating local admin passwords on critical servers are not sufficient. Attackers are targeting workstations as the low-hanging fruit and using the admin access available from those workstations to spread across networks.

With identity as the new network boundary, privileged credentials have become a commodity and will continue to be breached. As a result, the focus must shift toward the access the credentials provide. As an industry, if we do not take a ZSP stance in our environments, stolen credentials will continue as the attacker's low-hanging fruit and continue contributing to 80% of all data breaches today.

Remediant appreciated the opportunity to shine light on “Customer's” standing privilege and welcomes an opportunity to partner together to reduce privilege risk through a Zero Standing Privilege deployment.