# THE TOP 5
# Privileged Account Security Reports
# CISOs LIVE FOR

thycotic

# Privileged credentials represent one of your greatest security risks

Hackers today are targeting your privileged account credentials for good reason. Once they gain access, they can advance from an initial breach, escalating their privileges and moving through your network to identify and compromise confidential information. Hijacking the privileged credentials of an authorized user, **an attacker can easily blend in with legitimate traffic and be extremely difficult to detect.**

**62% OF BREACHES RESULT FROM PRIVILEGED ACCOUNT ABUSE**

**ATTACKERS ON NETWORK 240 DAYS BEFORE BEING DETECTED**

**" IF YOU DON'T HAVE GOOD PRIVILEGED ACCOUNT MANAGEMENT, ATTACKERS CAN TAKE YOUR CREDENTIALS AND START ACTING LIKE A TRUSTED USER. "**

- Dave Shackleford, cybersecurity expert at IANS

With Secret Server from Thycotic you can now secure your privileged accounts at a fraction of the cost of alternative approaches—and immediately generate reports to show your results.

See for yourself how valuable these reports in Secret Server can be for improving your company's security posture and helping to demonstrate compliance with policies.

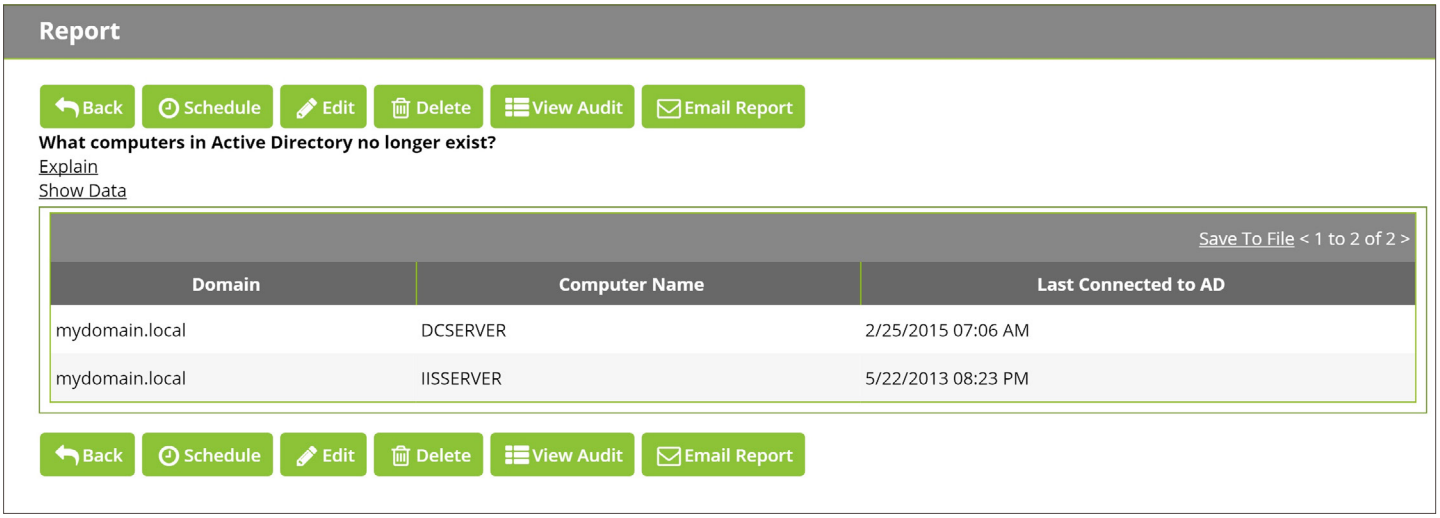
## The Top 5 Privileged Account Security Reports CISOs Live For:

1. **What computers in Active Directory no longer exist?**
2. **Which Privileged Accounts are no longer valid?**
3. **Who hasn't logged in within the last 90 days?**
4. **Privileged Account Password policy compliance statuses**
5. **What Privileged Account passwords are expiring this week?**

REPORT 1

# What computers in Active Directory no longer exist?

The "What computers in Active Directory no longer exist?" report is a precision tool for identifying Windows systems that have not connected to your domain recently. This report allows you to identify systems that may no longer exist or have been decommissioned. This provides a simple way for IT Admins or CISOs to find computers (and thus, the privileged accounts on these computers), that no longer need to be managed. This report can also be sent to Active Directory management personnel to remove these systems from the domain and related asset records. This helps to insure that accurate inventory is being kept and that all valid privileged accounts being managed on target systems are legitimate and within scope of the Privileged Account Management effort.




## What You Gain from this Report

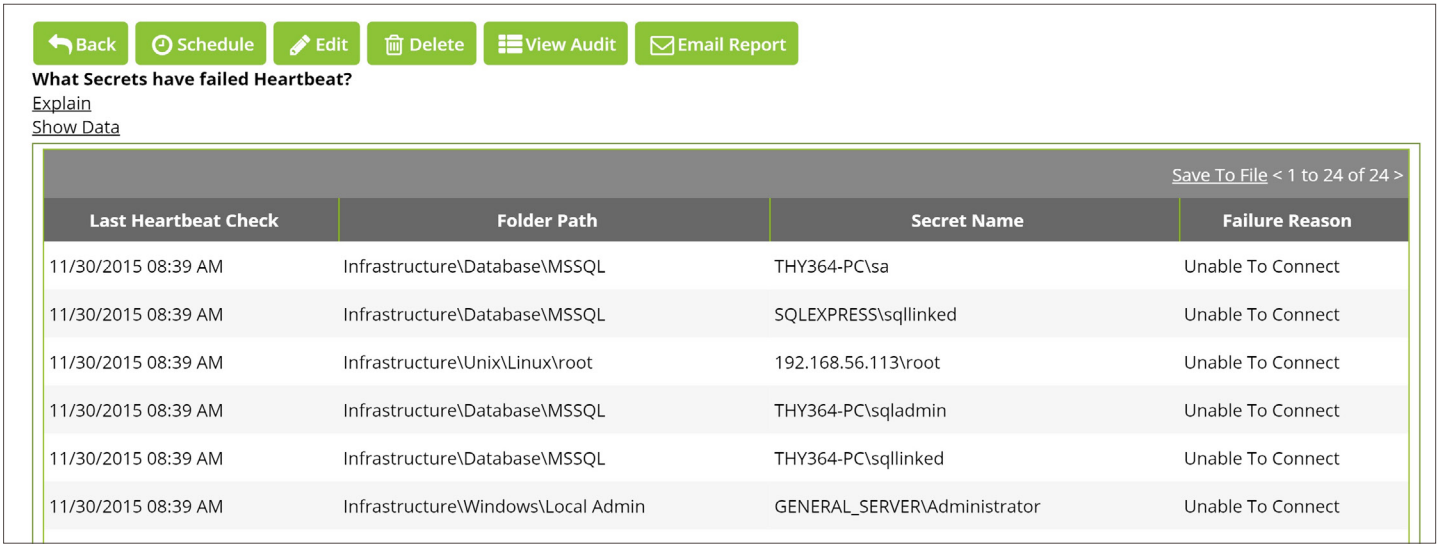
- Quick and simple method to identify computers that no longer exist in your environment
- Exportable list of systems which can be provided to AD Administrators for automated removal or management of these systems
- Gain stronger compliance by verifying that the systems and credentials being managed are not stale or are not within scope of regulatory or policy requirements

REPORT 2

# Which Privileged Accounts are no longer valid?

The “Which Privileged Accounts are no longer valid?” report reveals the credentials kept inside your Privileged Account Management solution that are no longer verifiably correct or accurate via a verification check. Privileged Account Management tools should have the ability to communicate outbound to target systems and verify whether or not the credential being managed within the tool is still the correct username and password that works with the target system. This check is a crucial verification that the credentials stored are accurate and working normally. Without this, credentials could be changed outside the scope of corporate policy by an administrator or worse, by a malicious attacker who has compromised the system.

To help streamline remediation efforts and correct mismatched credentials, this report will also provide the reason for the failure of the verification check allowing for faster correction of credentials which are non-compliant or potentially compromised.




| Last Heartbeat Check | Folder Path | Secret Name | Failure Reason |
|---|---|---|---|
| 11/30/2015 08:39 AM | Infrastructure\Database\MSSQL | THY364-PC\sa | Unable To Connect |
| 11/30/2015 08:39 AM | Infrastructure\Database\MSSQL | SQLEXPRESS\sqllinked | Unable To Connect |
| 11/30/2015 08:39 AM | Infrastructure\Unix\Linux\root | 192.168.56.113\root | Unable To Connect |
| 11/30/2015 08:39 AM | Infrastructure\Database\MSSQL | THY364-PC\sqladmin | Unable To Connect |
| 11/30/2015 08:39 AM | Infrastructure\Database\MSSQL | THY364-PC\sqllinked | Unable To Connect |
| 11/30/2015 08:39 AM | Infrastructure\Windows\Local Admin | GENERAL_SERVER\Administrator | Unable To Connect |

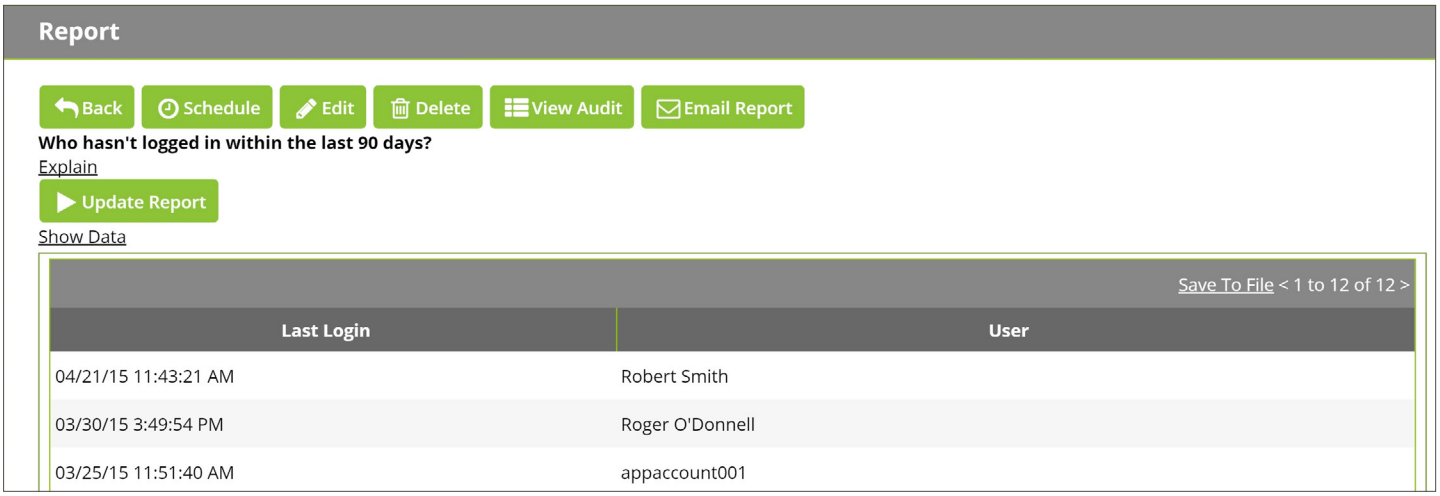
## What You Gain from this Report

- Verification of which credentials stored within your Privileged Account Management tool are still valid and which are not
- Auditable compliance adherence to show that credentials are being managed appropriately and have not fallen out of policy or regulatory compliance
- Insight into why the credential no longer works properly so that administrators or other IT staff can remediate the situation more quickly and efficiently

REPORT 3

# Who hasn't logged in within the last 90 days?

The "Who hasn't logged in within the last 90 days?" report gives a simple view into the Privileged Account Management tool's user logins, which have not been used. This report helps identify staff that may no longer need access to your Privileged Account Management tool and the privileged accounts that it protects. Removing staff who no longer need this level of access conforms to sound "Least Use Privilege" best practices, and adheres to a number of regulatory compliance requirements that mandate only those who need access to restricted accounts are provided this access. Monthly reviews of this report will give CISOs the visibility necessary to make good policy decisions about who will be provided access to privileged credentials within the environment.




## What You Gain from this Report

- Immediate visibility into which Privileged Account Management tool login accounts are not utilizing managed privileged accounts
- Regulatory compliance to verify that access to privileged accounts is only being provided to the proper, active designated users

REPORT 4

# Privileged Account password policy compliance statuses

The “Privileged Account Password policy compliance statuses” report provides a holistic view of all the credentials being managed by your Privileged Account Management tool, and whether they adhere to the assigned policy requirements for password complexity, rotation cycles and other mandated configuration items. It is important to periodically review and verify that these policies have been applied, and that no one has modified the credential itself outside the scope of the applied policies. Privileged accounts that no longer meet their policy requirements may now be out of corporate policy scope or fail to meet regulatory compliance.

By providing an easy-to-read pass/fail type of report, IT Admins and CISOs can quickly identify which accounts are outside of policy compliance and quickly investigate and remediate the situation in order to ensure compliance. This tool can also be used to provide evidence to auditors that privileged accounts within the scope of a particular regulation or policy framework are compliant and adhere to those requirements.

**Secret Password Compliance Statuses**

Explain

▶ Update Report

Show Data

Save To File | Show All < 1 to 30 of 32 >

| Folder Path | Secret Name | Secret Template | Password Requirement | Meets Compliance | Secret ID |
|---|---|---|---|---|---|
| Infrastructure\Cloud\Heroku | heroku.com (benjaminsy@outlook.com) | Web Password | Default | No | 124 |
| Infrastructure\Database\MSSQL | SQLEXPRESS\sqllinked | SQL Server Account | SQL Server | Yes | 118 |
| Infrastructure\Database\MSSQL | THY364-PC\sa | SQL Server Account | SQL Server | Yes | 2 |
| Infrastructure\Database\MSSQL | THY364-PC\sqladmin | SQL Server Account | SQL Server | Yes | 181 |
| Infrastructure\Database\MSSQL | THY364-PC\sqllinked | SQL Server Account | SQL Server | Yes | 119 |
| Infrastructure\Unix\Apache | 192.168.56.113\appaccount | Unix Account (SSH) | Linux | Yes | 113 |

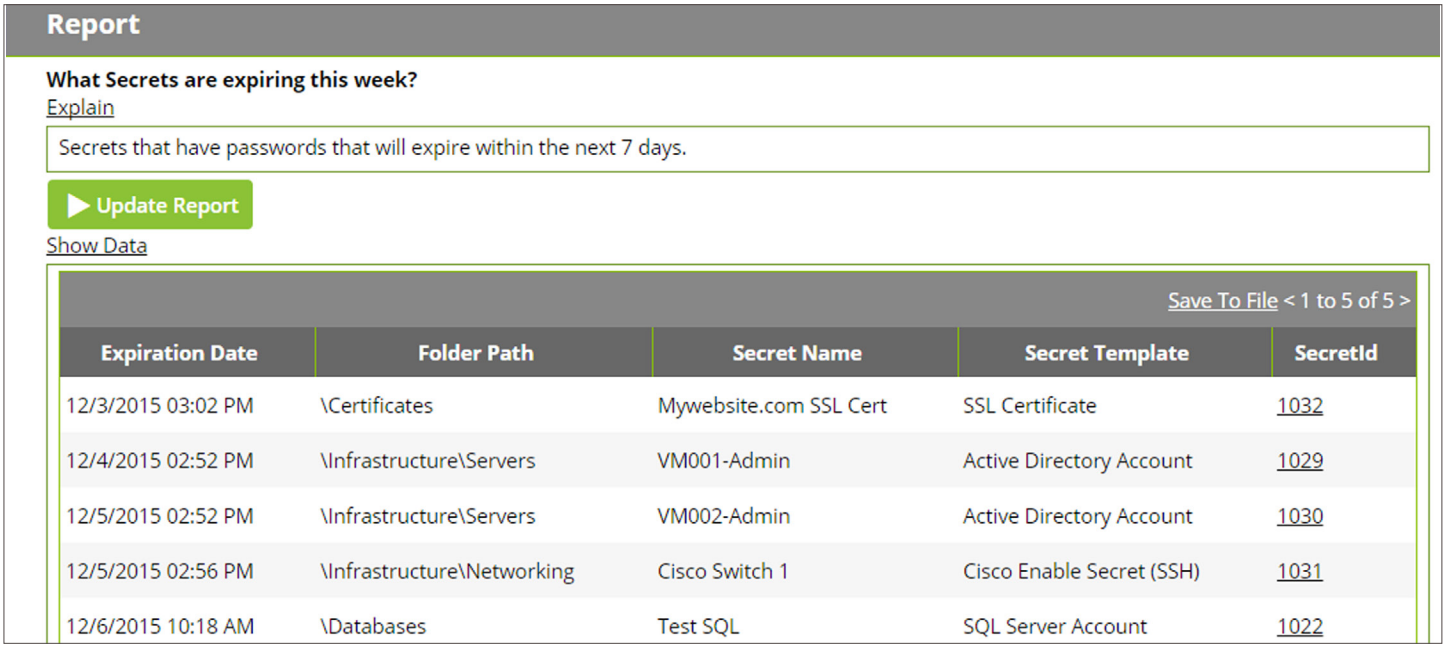
## What You Gain from this Report

- Easy-to-read red/green pass/fail dashboard view of privileged credentials which do not meet their assigned policy configuration requirements
- Demonstrable evidence for auditors and risk managers to show privileged accounts meet regulatory and internal policy requirements
- The designated policy and password requirements are outlined next to the listed privileged accounts to help admins determine if policies or requirements are not assigned properly

REPORT 5

# What Privileged Account passwords are expiring this week?

The "What Privileged Account passwords are expiring this week?" report shows which privileged accounts are due to expire in the coming week. Expiry, in this context, can mean either that the password associated with a credential stored within your Privileged Account Management solution is about to be changed according to an assigned password rotation interval (i.e. once every 30 days). Or, this can mean that any other item stored within the Privileged Account Management tool, such as a web certificate, is reaching the end of its validation period and needs to be renewed. This is an invaluable report to identify which items may need attention or monitoring during their rotation period to ensure related items continue to function normally. This report can also be easily modified to show what passwords are expiring in the next month, 90 days or any other period of time. Additionally, it can be automated to send notifications to relevant parties to alert them to upcoming expirations of credentials, certificates or any other stored item within Secret Sever.



**Report**

**What Secrets are expiring this week?**

Explain

Secrets that have passwords that will expire within the next 7 days.

▶ Update Report

Show Data

Save To File < 1 to 5 of 5 >

| Expiration Date | Folder Path | Secret Name | Secret Template | SecretId |
|---|---|---|---|---|
| 12/3/2015 03:02 PM | \Certificates | Mywebsite.com SSL Cert | SSL Certificate | 1032 |
| 12/4/2015 02:52 PM | \Infrastructure\Servers | VM001-Admin | Active Directory Account | 1029 |
| 12/5/2015 02:52 PM | \Infrastructure\Servers | VM002-Admin | Active Directory Account | 1030 |
| 12/5/2015 02:56 PM | \Infrastructure\Networking | Cisco Switch 1 | Cisco Enable Secret (SSH) | 1031 |
| 12/6/2015 10:18 AM | \Databases | Test SQL | SQL Server Account | 1022 |

## What You Gain from this Report

- Forewarning on the expiration of credentials, certificates or any other stored item within Secret Server to renew items before they are no longer valid and cause disruptions of service
- Automatic notification of items coming due which may require intervention or attention to the administrators or engineers responsible for managing these services
- Provide visibility to management to plan for upcoming reporting periods and outline what accounts or certificates will need attention long before they become due or become a last-minute crisis

# Simply your best value for Privileged Account Management security

Already securing privileged account access for more than 7,500 organizations worldwide, including Fortune 500 enterprises; Thycotic Secret Server is simply your best value for PAM protection.

**You can learn more about these Thycotic enterprise password management solutions by visiting our website at www.thycotic.com.**

## Thycotic Secret Server

Assures a fundamental security layer—managed from a single console—to protect against cyber-attacks that use privileged accounts to strike at the core of the enterprise.

## Password Reset Server

Provides simple, self-service password management to free up IT help desk staff from time-consuming and inefficient processes, and enforces stronger end user password controls.

thycotic

1101 17th Street NW Suite 1102
Washington DC 20036
DC | LONDON | SYDNEY

p: +1 202-802-9399
t: @thycotic
www.thycotic.com