Free Credential Compromise Snapshot: Healthviro

This is a mockup report to demonstrate the format in which we deliver our credential compromise snapshot.

Healthviro – Active Directory Assessment

Executive Summary

At your organizations request, Scapien analyzed credential data taken directly from your live Active Directory environment. This was not a generic scan or a theoretical exercise. The results are based on your actual accounts and configurations, tested using methods an attacker would use if password data were exposed.

This matters because the findings reflect **real exposure in your environment today**.

The outcome shows a **material weakness in credential control** across the organization. This is not driven by a single flaw. It reflects how credentials are being created, reused, and maintained in normal operations.

From a business standpoint, this creates a clear risk condition:
if credential data is obtained, access can be gained quickly, expanded broadly, and maintained longer than expected.

There are positive controls in place — most notably, no Domain Admin passwords were compromised — but those controls are not sufficient to offset the overall exposure.

This is not a hypothetical issue.
This is a **measured condition in the live environment**.

Headline Results

- **Enabled accounts reviewed:** 4,748
- **Accounts compromised during testing:** 1,465
- **Compromise rate:** 30.9%
- **Largest shared-password group:** 530 accounts
- **Compromised accounts with shared passwords:** 1,173
- **Compromised accounts that were non-expiring:** 953
- **Higher-impact accounts compromised:** 160
- **Domain Admin passwords compromised:** 0

What This Means for the Business

The scale of the result indicates a systemic issue. When nearly one-third of active accounts can be compromised, this is not isolated user behavior — it is embedded in how the environment operates.

Password reuse significantly accelerates risk. A single compromised password can unlock large numbers of accounts. In this case, one password provides access to 530 enabled accounts. That changes a breach from a contained event into a rapidly expanding one.

The presence of compromised operational and service accounts increases the impact. These accounts are tied to systems and workflows, meaning access is not limited to data — it can affect how the business runs.

Non-expiring credentials extend that risk over time. Once access is obtained, it may remain valid indefinitely unless it is actively identified and reset. That increases both the likelihood of persistence and the cost of removal.

This combination — scale, concentration, and persistence — is what turns a technical weakness into a business problem.

Financial and Operational Implication

This type of exposure does not degrade gradually — it tends to fail quickly once triggered.

If credential data is obtained through a breach, phishing event, or system compromise, the conditions identified here would allow an attacker to:

- gain immediate access to a meaningful portion of user accounts
- expand access rapidly through shared credentials
- interact with operational systems using service accounts
- maintain access for extended periods due to non-expiring credentials

In practical terms, this increases the likelihood of:

- operational disruption
- extended incident response and recovery cost
- audit and compliance exposure
- downstream financial and reputational impact

The key point is straightforward: this is a preventable condition.

Addressing it now is materially less costly and less disruptive than managing it after an incident.

What Is Working

This is not a worst-case scenario, and that should be recognized.

No Domain Admin passwords were compromised, which prevented a full-environment failure scenario. No basic control failures such as blank passwords were identified. There is clear evidence of stronger password policy intent within the environment.

These controls reduced the severity of the outcome. The issue is that they are not being applied consistently enough to control the overall risk.

Why This Matters Now

This assessment is based on your actual data, not a model or assumption. It reflects how the environment behaves under realistic attack conditions today.

The conditions required for a credential-based incident are already present. The remaining variable is whether and when those conditions are triggered through events such as credential theft, phishing, or system compromise.

Situations like this are typically addressed in one of two ways:

- proactively, through controlled remediation and strengthening of credential practices
- reactively, in response to an incident, where time pressure, operational impact, and cost are significantly higher

The difference between those two paths is not technical — it is operational and financial.

Next Step

This summary is intentionally limited. It is designed to establish whether a real problem exists and whether it warrants action.

The full assessment includes:

- account-level findings
- cracked credential identification
- password reuse mapping
- prioritization of highest-risk exposure
- structured remediation plan
- validation and retesting approach

Scapien can provide the full report along with a detailed review session and outline practical engagement options based on your environment and risk tolerance.

To proceed, you can contact Scapien or visit our website to review available programs and speak with a representative.

Closing

This assessment shows a clear and measurable credential exposure issue in the live environment.

It is fixable.

The decision is whether to address it in a controlled manner now, or under the pressure and cost of an incident later.