Biotechnology

ISSQUARED

Case Study

# CYBER RESILIENCE

## USING IDENTITY MANAGEMENT

## ABOUT THE CLIENT

A leading biopharma/biotech company with a global presence having compliance requirements for protecting PII, IP, and GxP processes.

## OBJECTIVES

The client wanted to reduce the attack exposure for lateral movements as well as privileged escalations.

Also, reduce voluntary/involuntary credentials leakage by employees that would lead to disruption or compromise of manufacturing processes.

The client sought for a solution that enables ease of use for non-IT users and provides sufficient tools for self-service.

## APPROACH

ISSQUARED® conducted various workshops with the client to discuss the most reliable options and strategies. As an outcome, we decided that the best approach would be to keep the user from using the same password across multiple accounts across different untrusted Active Directory domains (Each individual has at least two). The following were the drivers for the solution design:

a) Restrict privileged credentials' exposure in the Enterprise network.

b) Strict credentials policy for privileged accounts.

c) Non-disruptive for non-IT staff to perform their daily functions.

d) Self-service options and notifications for users for any remediation actions assigned.

e) Automated onboarding and provisioning for migrated users with self-service enablement.

f) Metrics to assess efficacy.

ISSQUARED

## SOLUTION

### ADMINISTRATOR/PRIVILEGED USER ACCOUNTS

An industry-leading password vaulting (PI) solution was deployed at all locations. The ISSQUARED® team has implemented daily password change and check-in/check-out process. These passwords were generated randomly by the system ensuring no clash with other accounts belonging to the same user.

Self-service was provided on the password vaulting platform for the admin users to unlock their admin accounts in case of an account lockout.

A log management and event notification tool was also configured to track and flag frequent password changes requests, maintain an audit trail of all account checkouts

Exposure to privileged accounts in the business network was further reduced by setting up new bastion hosts with access to regular accounts only.

### REGULAR USER ACCOUNTS

Provisioning for migrated users was done automatically by ORSUS™ Identity Access & Governance.

Access to all migrated applications was restored automatically.

A self-service option in the form of ORSUS™ Identity Access & Governance was provided for end-users to actively respond to password change requests and manage their regular account in general.

Static password vaults were provisioned for users on the BeyondTrust solution to manage regular accounts' passwords.

Since most of the non-admin users were non-IT staff, it was decided to rely on an escalation process through email notifications to respective managers in case of non-conforming passwords.

Metrics are shared monthly with leadership for further escalation on defaulters.

## RESULTS

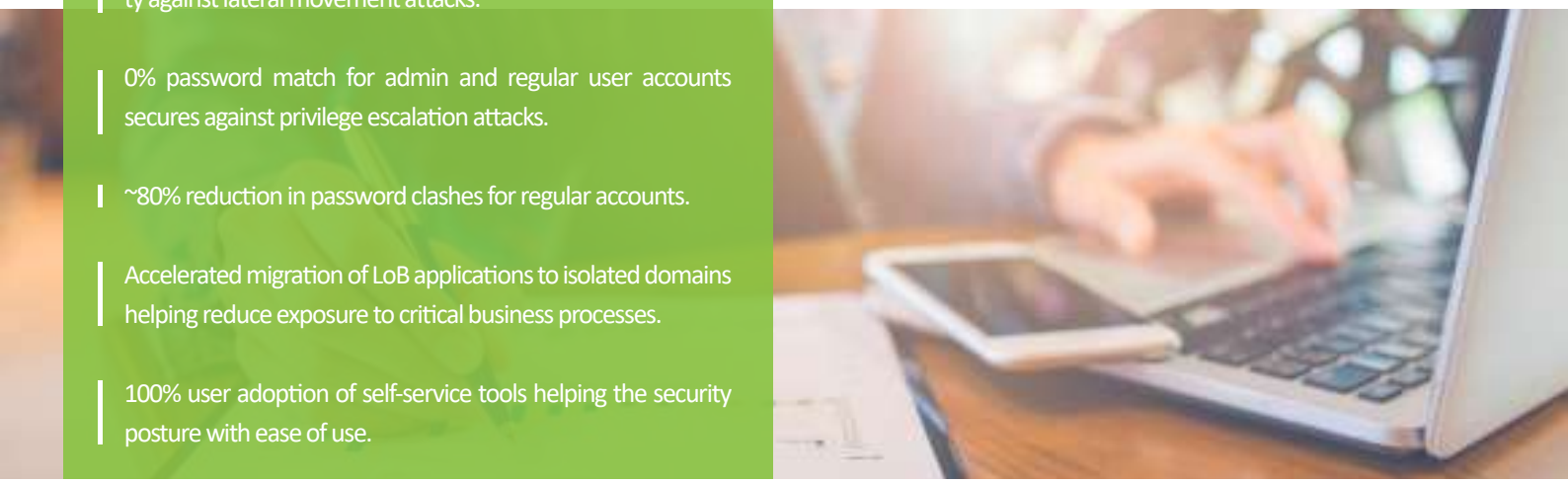
0% exposure of untrusted privileged accounts hardens security against lateral movement attacks.

0% password match for admin and regular user accounts secures against privilege escalation attacks.

~80% reduction in password clashes for regular accounts.

Accelerated migration of LoB applications to isolated domains helping reduce exposure to critical business processes.

100% user adoption of self-service tools helping the security posture with ease of use.



ISSQUARED®

HQ: 2659 Townsgate Rd, Suite 227
Westlake Village CA 91361 USA

+1 805 371 0585
+1 800 779 0587

support@issquaredinc.com
www.issquaredinc.com