

Excalibur

no more passwords, no more usernames

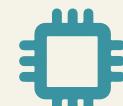
Strong password-less multi-factor authentication



Precise geolocation verification.



On-device biometry.

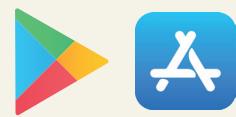


Device ownership factor
(on-device secure element
cryptography).



PIN code fallback.

Excalibur mobile application
available on Play Store and
App Store.



Additional configurable factors
include:

- peer verification
- IP range
- day / time
- PC status (online / offline)
- mobile status (online / offline)

Dynamic passwords

Users do not interact with passwords anymore

Passwords are automatically changed by Excalibur before each authentication and subsequently injected into authentication process.

Random password
G6Ht_3RP=_@wdPjvL3E3C*PKaEVrzuq



No password expiration or regular manual changes required.

Complete legacy compatibility with every system you use today, if Excalibur does not directly integrate the given system user is able to temporarily show password on his token after authentication factor verification. Password gets automatically changed after a short time period.

Excalibur Dashboard

Full visibility into user activity

Complete auditability

no action / event is ever deleted, every action is cryptographically signed creating indisputable cryptographic proof of every user action (login, authorization, registration, configuration changes etc).

User: John Doe

Account	Computer	Location	Start	End
EXCALIBUR\jdoe	177_managed_creds	EMEA	19.6.09:48:17	19.6.09:51:11
EXCALIBUR\jdoe	177_managed_creds	EMEA	19.6.08:48:07	19.6.09:19:49
EXCALIBUR\jdoe	177_managed_creds	EMEA	18.6.23:39:46	19.6.00:36:28
Static Credentials	230	EMEA	15.6.10:03:55	15.6.10:21:18
Static Credentials	192_47	EMEA	14.6.01:50:12	14.6.01:52:29
Static Credentials	192_47	EMEA	14.6.01:45:18	14.6.01:47:45
Static Credentials	rdp	EMEA	14.6.01:45:11	14.6.01:45:11
Static Credentials	192_47	EMEA	14.6.01:30:18	14.6.01:31:02
EXCALIBUR\jdoe	177_managed_creds	EMEA	14.6.01:29:23	14.6.01:31:02
EXCALIBUR\jdoe	220_managed_creds	EMEA	11.6.09:44:08	11.6.09:44:41
Static Credentials	192_47	EMEA	11.6.09:43:51	11.6.10:46:09
EXCALIBUR\jdoe	220_managed_creds	EMEA	11.6.08:43:23	11.6.08:44:16
EXCALIBUR\jdoe	192_47_managed_creds	EMEA	11.6.08:41:41	11.6.10:48:32
Static Credentials	tresk-vm_d2	EMEA	11.6.08:41:28	12.6.10:56:12
Static Credentials	230	EMEA	11.6.08:41:20	12.6.10:56:12
Static Credentials	tresk-vm_dusan	EMEA	11.6.08:41:15	12.6.10:56:12

Timeline Locations

A timeline visualization showing session activity from June 9 to June 19. Each bar represents a session, with its color indicating the session type (Online, Manual, OTP, Tokenless, Locked). The length of the bar indicates the duration of the session. Below the timeline is a map of Poprad, Slovakia, showing the precise geographic location of each session as a green dot. A legend at the bottom right provides details about the session types and their colors.

What system did user login to, when, from where, how long was he active etc...

Precise geographic location of every user interaction.

Group management for users / computers / policies.

Excalibur Client

Passwordless OS login

Seamless passwordless VPN and WiFi logins.

Integration with Cisco AnyConnect.



SSO using Kerberos tickets.



Your
logo
here

Local / remote (RDP) login.

Secure online / offline login.

Web SSO on any browser.

Request colleague with sufficient privilege for login approval in case of forgotten phone, out of battery etc.

Peer verification

4-eye principle anywhere you need it



Require confirmation by additional individual on any action such as login to a sensitive system, registration of a new user etc.

Fully configurable - the action can be verified by any colleague or a manager of the given user or service desk.

Any Excalibur authenticated action can be configured to use 4-eye verification aka peer verification.

Micro-granular geolocation

Excalibur as a home-office enabler

Sensor fusion geolocation used as another authentication factor.

Self-service home geofence registration - powered by peer verification.

Excalibur enables precise micro-granular geolocation. Micro-granular means a unique home address(es) for each employee.

Secure work from home! Location access controlled per user down to building level precision.

Remote peer verification

No more human element risks

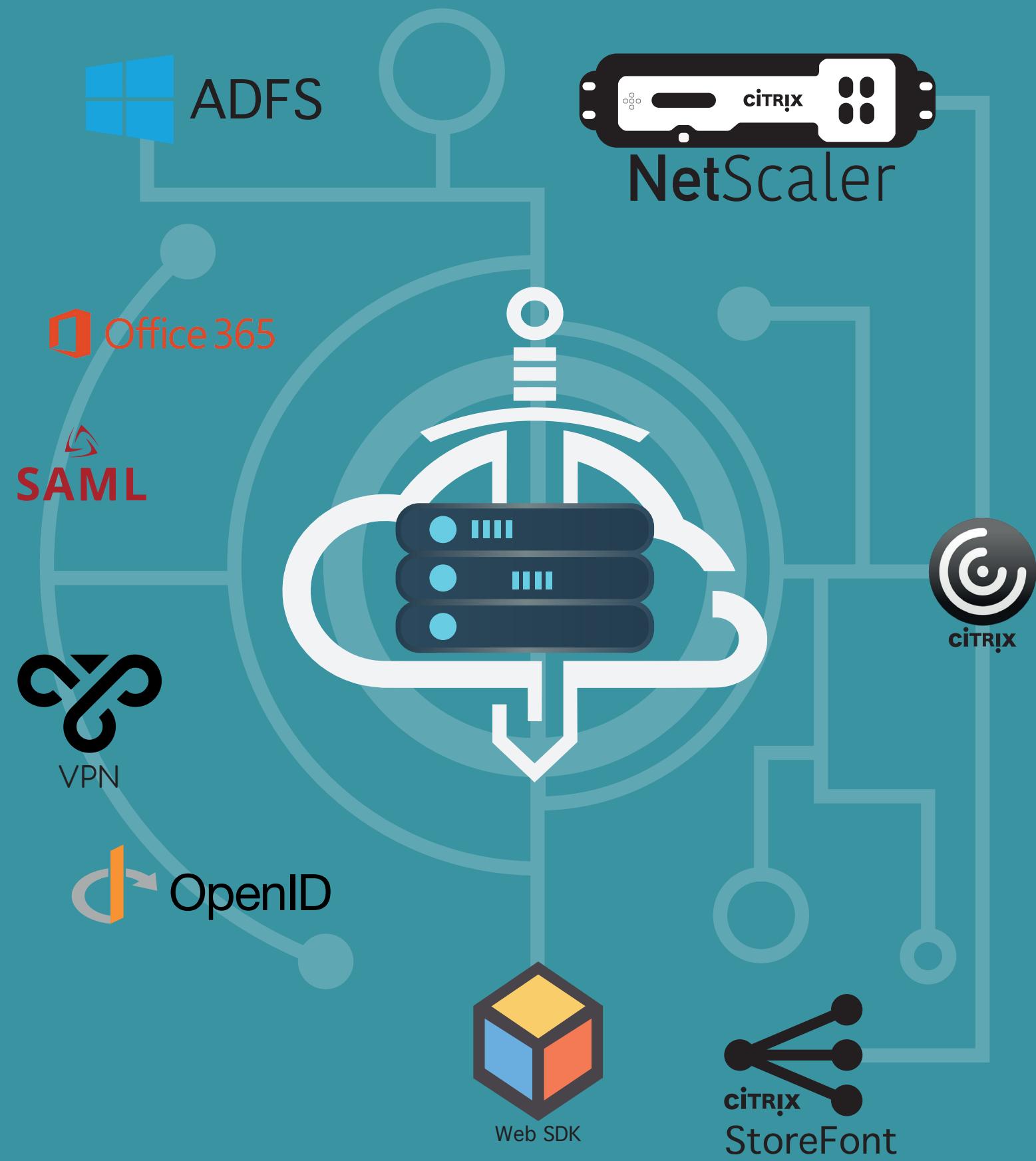
Peer verification supports also remote scenarios. User requesting access (peer verification) and the user confirming access can be on physically different locations.



Every verification is logged - it is clear who confirmed what request, thus managers and/or the security operation center can keep track of them.

Integrations with other systems

Standard protocols, custom integrations,
from cloud to legacy apps - we make it happen



SAM - Streamed access management

Just like Privileged Access Management but for ALL access!

All user activity is monitored, recorded and indexed, fully searchable with zero deniability of actions.



Access resources behind any firewall / NAT via tunnel

SSH tunnel

Resources are no longer exposed, no way to attack protected resources

HTTP / HTTPS, RDP, SSH, VNC, TELNET

Access to resources is streamed directly to web browser



Cybersecurity is rocket science

just hop on and enjoy the ride