Multifactor Authentication: The Missing Piece in Your Cybersecurity Strategy

Nikolaos Vanas – Technical Engineer

data.ally WatchGuard®

Table of contents

01

Passwords

The Weak Link

02

Case Studies

Real-World Examples

03

AuthPoint Solution

MFA That’s Really Easy

04

Centralized Managed MFA Solution

Implement a Zero-Trust Architecture

01

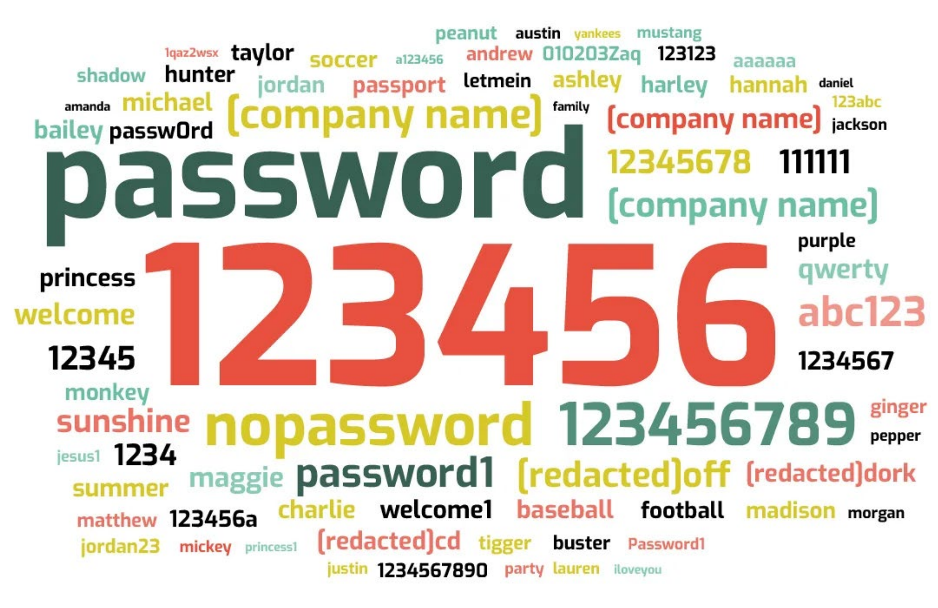
Passwords

The Weak Link

Password Security

Password’s Vulnerabilities

- Brute-Force attacks
- Keylogger Attack
- Dictionary Attack
- Man-in-the-middle
- Phishing
- Password Spraying



Passwords = Problems

#1

Top action used in breaches is **stolen credentials**

81%

Total number of breaches that leveraged either **stolen** and/or **weak passwords**

65%

Of the users, use the **same password** in all of their account

Verizon Data Breach Investigations Report 2020

Google Online Security Survey

02

Case Studies

Real-World Examples

SMS OTP? Really?

- Reddit Breach(2018) due to SMS-only for 2FA.
- Vulnerable to SIM swap attacks
- Rated by Gartner as “Low” security
- Just Google it!

Using SMS in addition to your password is better than nothing, but it’s not the most reliable approach.

Accounts Breached

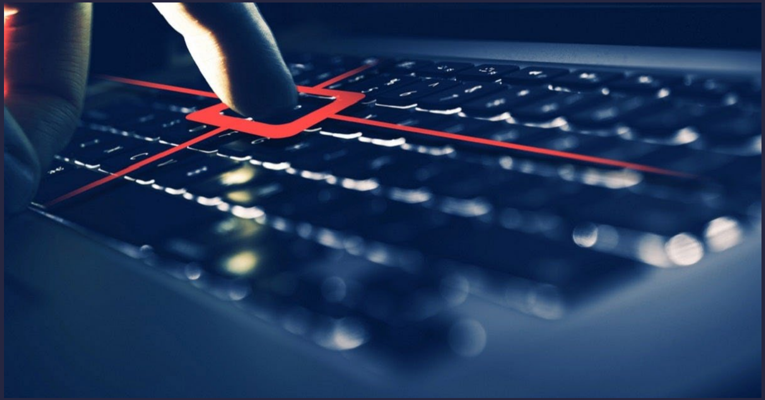
- Close to 35,000 users impacted on Paypal
- More than 500.000 Zoom accounts sold in dark web
- Its EASY getting credentials database from the Dark WEB.

Paypal adviced users to use unique and long passwords and to activate 2FA.

LastPass Breach

- Attack targeted encrypted Amazon S3 buckets
- LastPass's luckless developer got keylogged
- Attack on home computer via 3rd party software

Lack of proper patching and use of MFA.

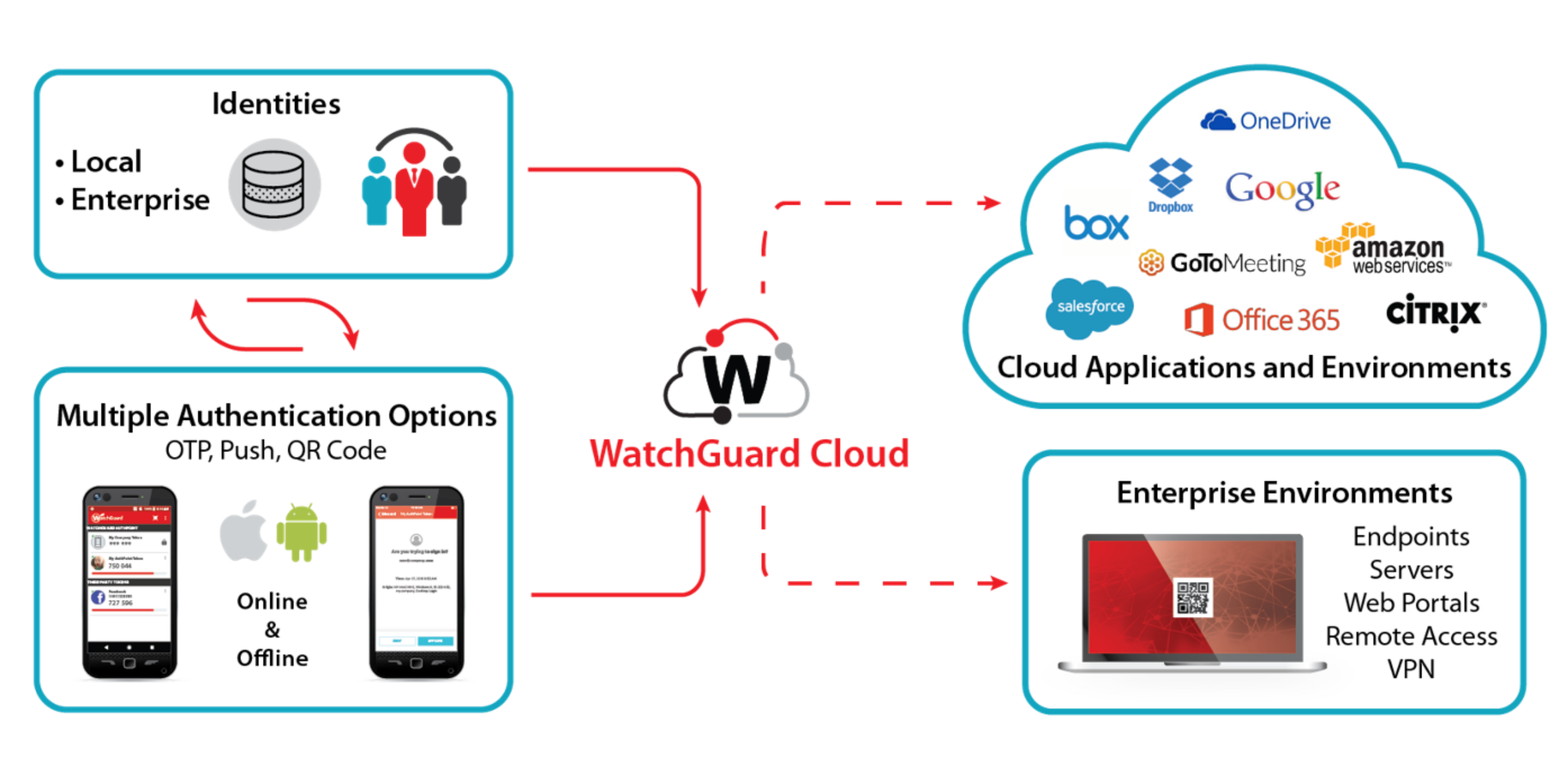


03

AuthPoint Solution

MFA That’s Really Easy

AuthPoint Overview



Identities

- Local
- Enterprise

Multiple Authentication Options

OTP, Push, QR Code

Online
&
Offline

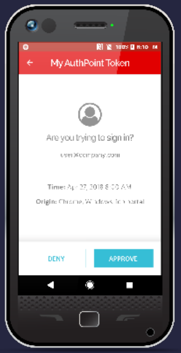
WatchGuard Cloud

Cloud Applications and Environments

Enterprise Environments

Endpoints
Servers
Web Portals
Remote Access
VPN

MFA Authentication Options



Push

QR Code

One-Time Password

MFA Use Cases

PCs & Server Logon

SSO to Cloud Apps

Remote Access

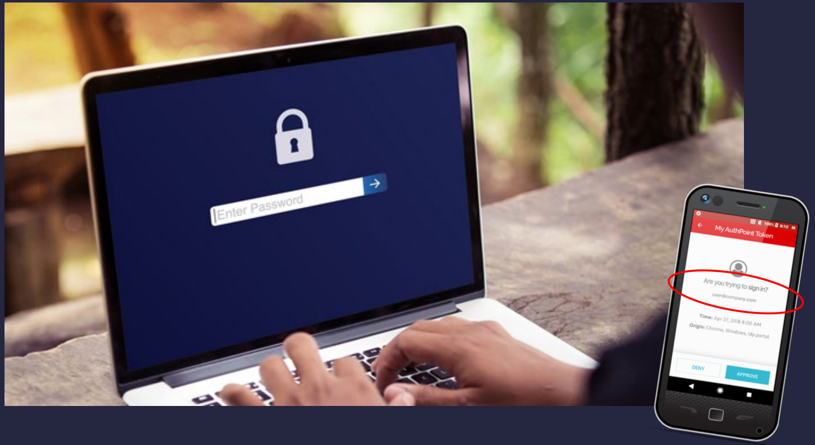
Privileged User Access

PCs & Server Logon

- Protect user login to their local or remote computers and servers using MFA, enabling both online or offline protection.

- Remote connection to a computer(like RDP) can be the 1st step for a hacker.

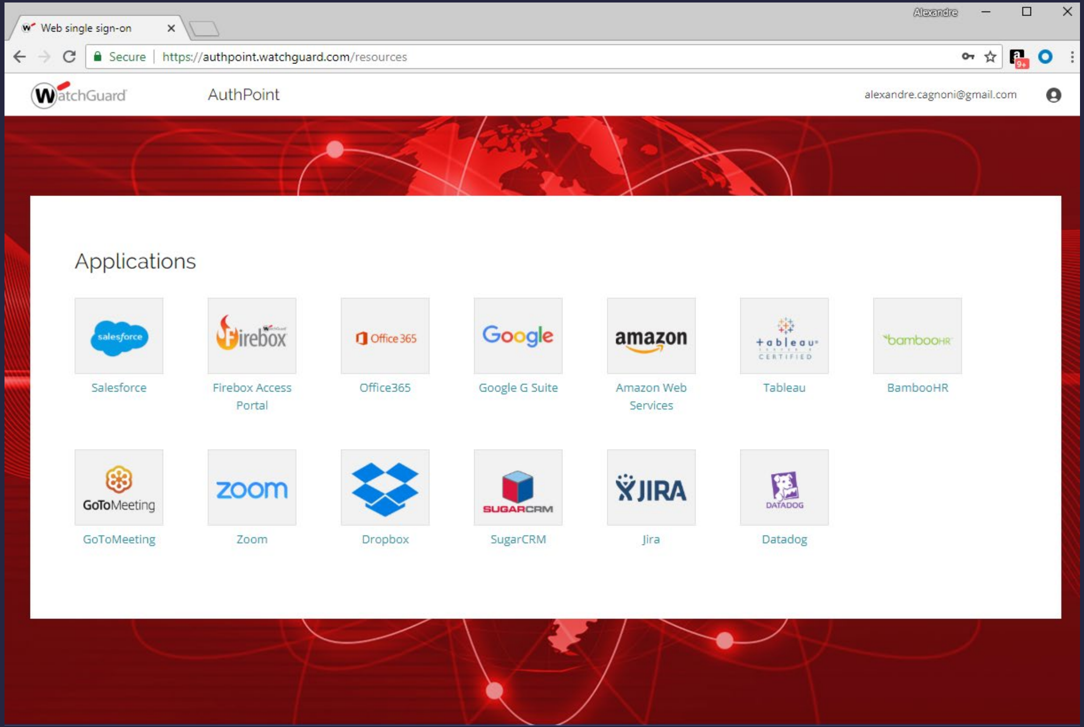
- Key employees might carry critical and confidential information on their laptops.

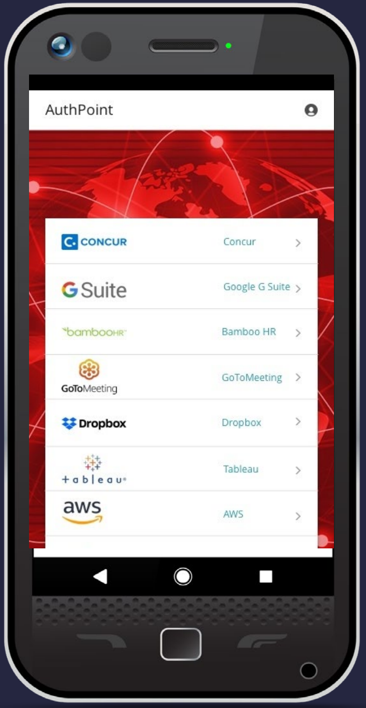


SSO to Cloud Apps

- Protect cloud applications that are outside of your network with MFA.
- Secure employees’ credentials and allow admins to define who has access to which application.
- Sign-in once with MFA and get Web SSO access to your cloud applications.

Web Single Sign-On(SSO)





Remote Access

You may have the best remote access and firewall.
Still, it takes for a hacker to gain entry is **one** of the following:

One User

With bad Password

One User

With Keylogger

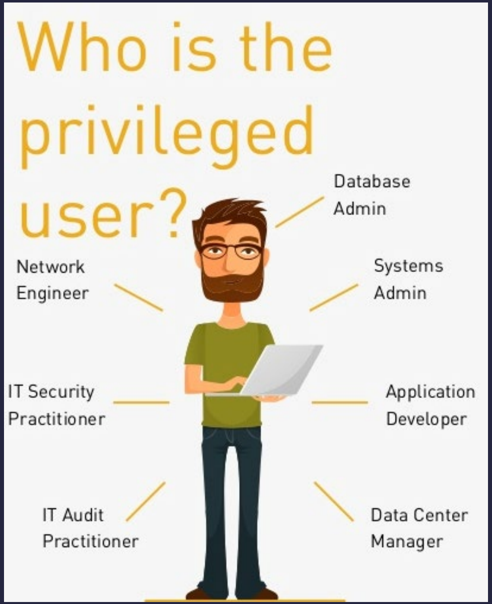
One User

Sharing Password or OTP

Any Remote Access, VPN application, no matter the vendor,
SHOULD have MFA to protect the network.

Privileged User Access

- Additional layer of security.
- Protects against malicious employees.
- Examples are Root access to Linux machines or critical apps or systems (e.g CyberArk)

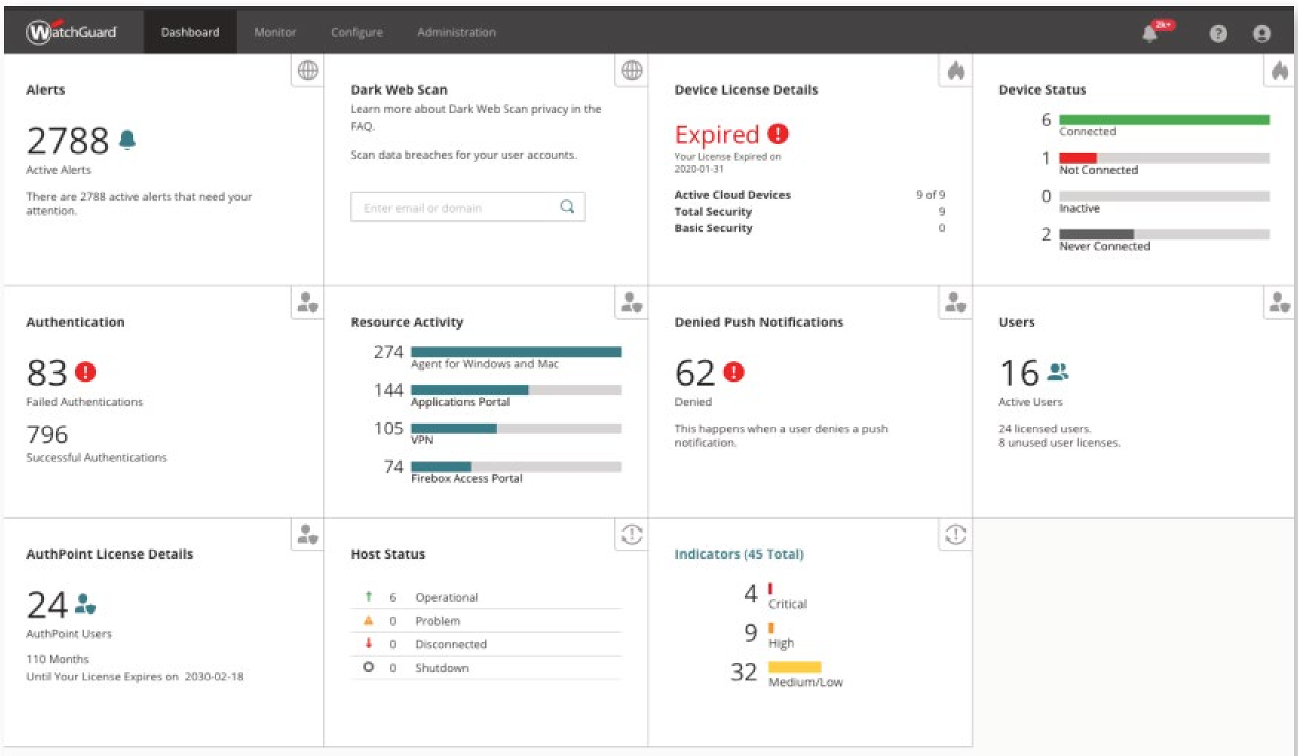


04

Centralized Managed MFA Solution

Implement a Zero-Trust Architecture

Comprehensive MFA Dashboard



Alerts

2788

Active Alerts

There are 2788 active alerts that need your attention.

Dark Web Scan

Learn more about Dark Web Scan privacy in the FAQ.

Scan data breaches for your user accounts.

Enter email or domain

Device License Details

Expired

Your License Expired on 2020-01-31

Active Cloud Devices	9 of 9
Total Security	9
Basic Security	0

Device Status

6 Connected

1 Not Connected

0 Inactive

2 Never Connected

Authentication

83

Failed Authentications

796

Successful Authentications

Resource Activity

274 Agent for Windows and Mac

144 Applications Portal

105 VPN

74 Firebox Access Portal

Denied Push Notifications

62

Denied

This happens when a user denies a push notification.

Users

16

Active Users

24 licensed users.
8 unused user licenses.

AuthPoint License Details

24

AuthPoint Users

110 Months
Until Your License Expires on 2030-02-18

Host Status

↑ 6 Operational

▲ 0 Problem

↓ 0 Disconnected

○ 0 Shutdown

Indicators (45 Total)

4 Critical

9 High

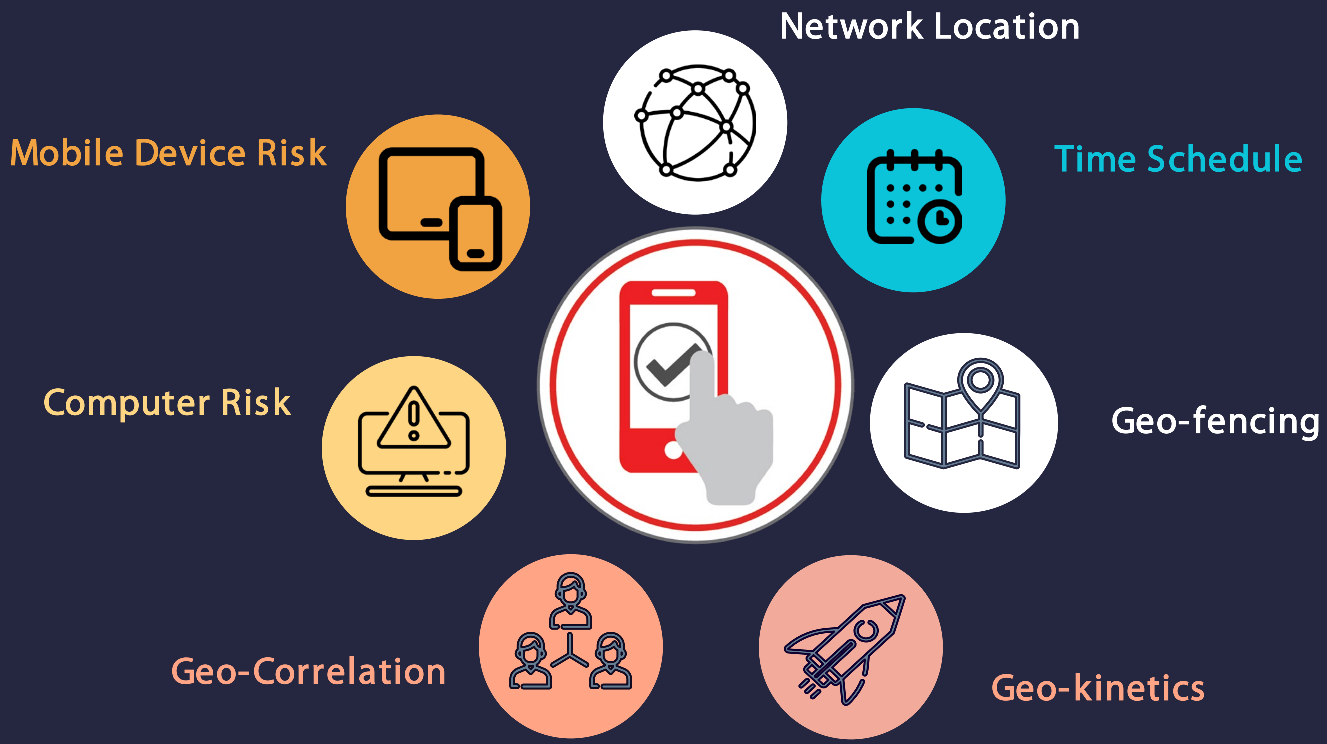
32 Medium/Low

Gartner

Recommendations

- ✓ Adopt risk-based framework
- ✓ Provide end users with choice while satisfying the trust requirements
- ✓ Prioritize mobile push and mobile OTP

Risk Framework



Network Location

Mobile Device Risk

Time Schedule

Computer Risk

Geo-fencing

Geo-Correlation

Geo-kinetics

Conclusions

- ✓ AuthPoint is a cloud-based MFA solution, managed in WatchGuard Cloud
- ✓ Provides Push-Based authentication, for the best security and user experience.
- ✓ Facilitates the Zero-Trust implementation rules.
- ✓ MFA deployment with Risk-based policies.
- ✓ Using MFA for Web SSO also brings better UX for end users.

Thanks!

Nikolaos Vanas

data.ally