

A red-tinted background featuring a stylized globe with white lines representing latitude and longitude. Overlaid on the globe are several white circles and lines, suggesting a network or security theme.

AuthPoint – MFA

Smart Security, Simply Done

Luca Manidi
Channel Account Manager
Watchguard Technology Inc.

LE PASSWORD RUBATE OFFRONO UN ACCESSO VELOCE ALLA VOSTRA RETE

#1

L'azione principalmente utilizzata nei data breaches è il furto di credenziali

Verizon Data Breach Investigations Report 2018

81%

Il numero totale di data breaches avvenuti tramite password rubate o comunque deboli

Verizon Data Breach Investigations Report 2017/2018

1.4B

Numero di passwords rubate trovato su di un file nel dark web

Forbes, December 11, 2017

PASSWORD

* * * * *

I TENTATIVI DI PROTEZIONE DELLE CREDENZIALI FIN QUI VISTI NON SONO SUFFICIENTI

6%

Percentuale degli utenti internet che usano la **stessa password per tutti gli account che possiedono online** in 2017

www.statista.com/statistics/763091/us-use-of-same-online-passwords

>70

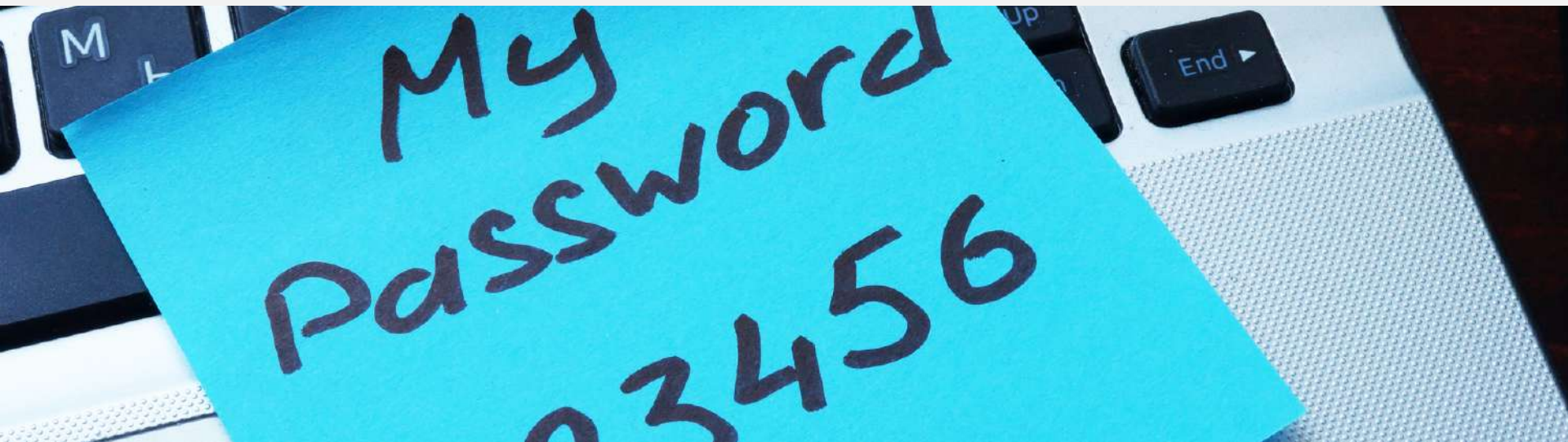
Numero di **accounts online per una persona (media USA)**

Dashlane Survey 2015

37

Numero di account online per i quali una persona media ha dovuto usare un **link per resettare la sua password**

Dashlane Survey 2015



Tra te e un hacker c'è solo una password debole a difenderti...

.... E anche le password più "complicate" che riuscirai a inventarti possono essere violate.

Ormai le password non sono più sufficienti per proteggere le tue risorse, gli account e le informazioni.
Ecco spiegati alcuni dei motivi principali:



L'80% degli utenti
UTILIZZA la stessa password
per più di un account²



Il 6% degli utenti Internet
utilizza la **STESSA** password
per tutti i suoi account online²



Circa il **46%** dei dipendenti
utilizza **password personali** per
gli account aziendali³

Le persone scelgono password deboli

La lista delle 25 password più deboli del 2017¹

- | | | |
|--------------|--------------|--------------|
| 1. 123456 | 10. iloveyou | 19. passw0rd |
| 2. Password | 11. admin | 20. maste |
| 3. 12345678 | 12. welcome | 21. hello |
| 4. qwerty | 13. monkey | 22. freedom |
| 5. 12345 | 14. login | 23. whatever |
| 6. 123456789 | 15. abc123 | 24. qazwsx |
| 7. letmein | 16. starwars | 25. trustno1 |
| 8. 1234567 | 17. 123123 | |
| 9. football | 18. dragon | |

Se un hacker dovesse decidere di violare la tua password invece di comprarla, anche in quel caso non ci metterebbe molto tempo.

In effetti per violare la maggior parte delle password ad un hacker serve meno del tempo che impiegherai a leggere questa

Tipologia	Password	Tempo (HSIMP) How Secure Is My Password?	Tempo (PA) Analizzatore Passfault	Livello di sicurezza
parola comune con 8 caratteri	required	52 secondi	<1 giorno	Inutile
8 caratteri casuali	qkcrmztd	52 secondi	<1 giorno	Inutile
8 caratteri casuali con numeri	kqw8bv832	11 minuti	<1 giorno	Inutile
8 caratteri casuali con maiuscole e minuscole, simboli e numeri	J5bZ>9p!	20 giorni	<1 giorno	A rischio
Tipologia	Password	Tempo (HSIMP)	Tempo (PA)	Livello di sicurezza
Password con 2 parole comuni	orange tea	98 giorni	<1 giorno	A rischio
Password con 3 parole comuni	this is cool	546 anni	<1 giorno	A rischio
Password con 5 parole non comuni	du-bi-du-bi-doo	12 milioni di anni	<1 giorno	A rischio

Le password vengono violate con facilità e offrono una sola linea di difesa. Se un hacker riesce a rubare anche solo una password dei tuoi dipendenti, di solito è poi in grado di accedere all'intera rete. Una volta entrato, sarà libero di fare ciò che vuole. Normalmente un hacker diffonde malware, ruba, modifica o cancella le informazioni importanti.

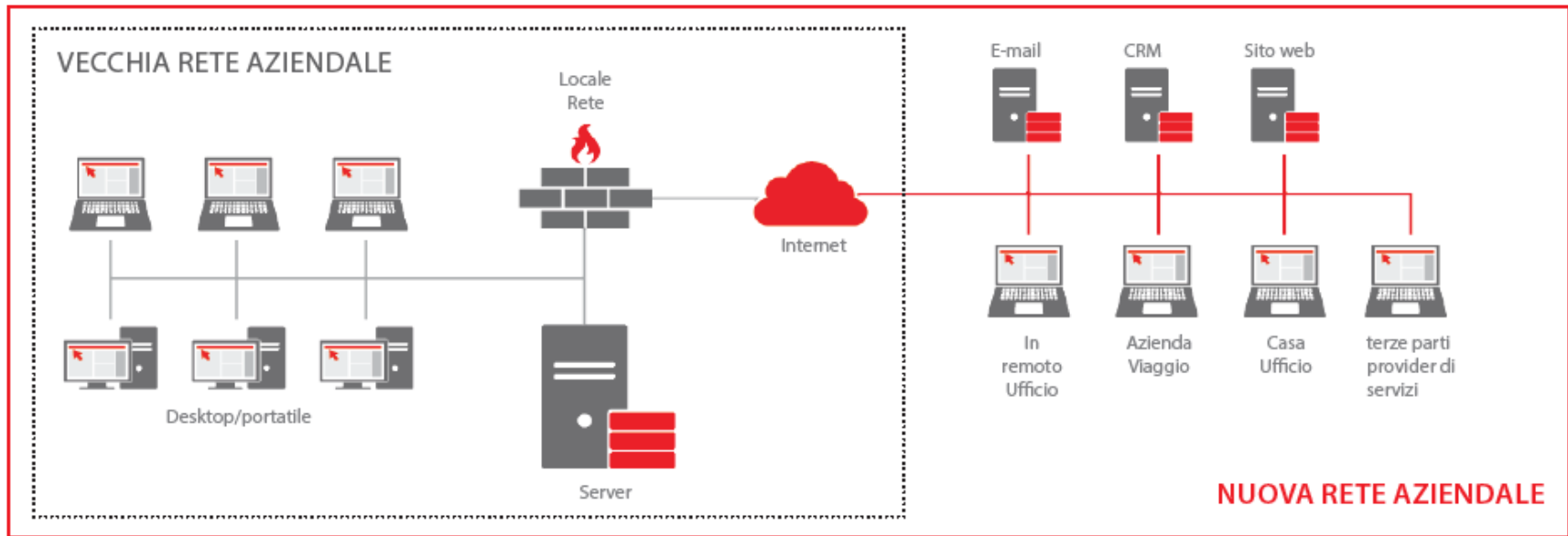
Type	Password	Time (HSIMP)	Time (PA)	Security Level
Passphrase 1	i own 2 dogs and 1 cat	1 sextillion years	330130 centuries	Secure forever
Passphrase 2	I own 2 dogs and 1 cat!	30 octillion years	8594846 centuries	Secure forever
Passphrase 3	#I own 2 dogs and 1 cat!?	285 nonillion years	1220882818 centuries	Secure forever

- **Don't** use common dictionary words - Ex. orange, car, password
- **Don't** use sequential letters or numbers - Ex. 12345, abcde
- **Don't** use repeated letters/numbers or keyboard patterns - Ex. 111, aaa, qwerty, asdfgh
- **Don't** use the same passphrase for every site if you can help it. Something you could do would be to make a passphrase saying "I am accessing Facebook!" for Facebook, or "I am accessing YouTube!" for YouTube, etc.



84% IT Managers che preferirebbero avere una tecnologia efficiente in atto piuttosto che basarsi su politiche applicate a password forti e complesse

L'EVOLUZIONE DELL'AUTENTICAZIONE : COME SIAMO ARRIVATI FIN QUI



L'accesso veloce a Internet, permette ai dipendenti di lavorare da qualsiasi luogo. Le informazioni aziendali non sono più concentrate in una sala server o in data center aziendali. Si trovano ormai nei cloud e sono accessibili tramite CRM, server e-mail e portali web.

Ogni giorno un dipendente cercherà di autenticarsi per accedere a questi servizi. In primo luogo dal computer. In secondo luogo da un server e-mail e forse anche da un'applicazione cloud.



Le previsioni dicono che **entro il 2023 Il mercato globale MFA raggiungerà un valore di \$17.76 bilioni di dollari**, con una crescita media annua prevista del **15.07%**

MFA protegge con piu' di una semplice password



Multi-Factor Authentication e' Protezione Essenziale

By requiring additional proof of identity beyond a simple password, **multi-factor authentication (MFA) is the most important safeguard** to protect your business



Cosa rende AuthPoint speciale?

MFA deve essere senza problemi !

Difficolta' legate ai token HW

- Oggetti da ricordare
- Costosi
- Difficili da distribuire
- Richiedono installazione driver
- Richiedono USB connection



Limiti di copertura

- Remote network access
- VPN
- Cloud applications
- Computer login

Software costosi da acquistare/mantenere

- Infrastrutture costose
- Conoscenze tecniche staff



Le organizzazioni hanno bisogno di un servizio MFA che sia semplice da configurare e utilizzare (meglio se Cloud)

I Benefici con AuthPoint

Management Semplice dal Cloud – Low TCO

Lightweight, Full-Featured, Mobile App Intuitiva

miglior esperienza utente Con Push Authentication

VPN, Cloud and PC Login Protection – Tutto incluso

Web Single Sign-On (SSO) grazie ad un portale semolice ed usabile

Online and Offline Authentication

Distribuzione veloce con guide d'integrazione

Tecnologia con piu' di 10 anni di esperienza



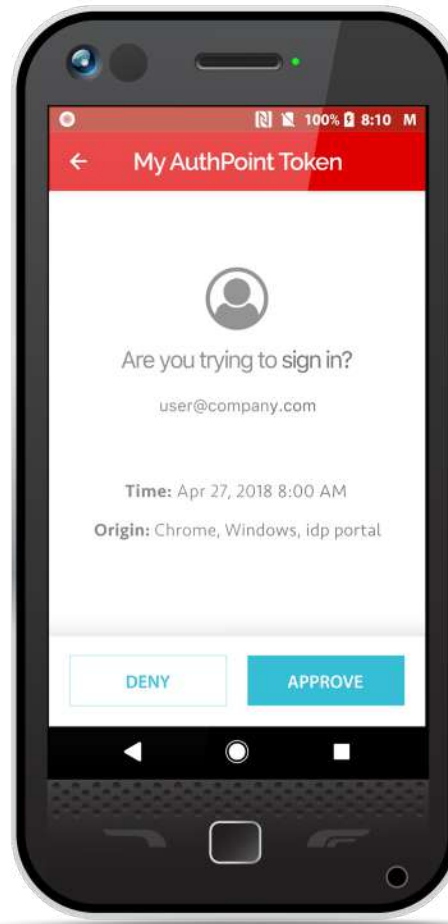
Che cosa e' l'autenticazione multi fattore?

Use of 2 or more authentication factors, from:

- **Something you know**
(password, PIN)
- **Something you have**
(token, mobile phone)
- **Something you are**
(fingerprint, face)

Password

• • • • •

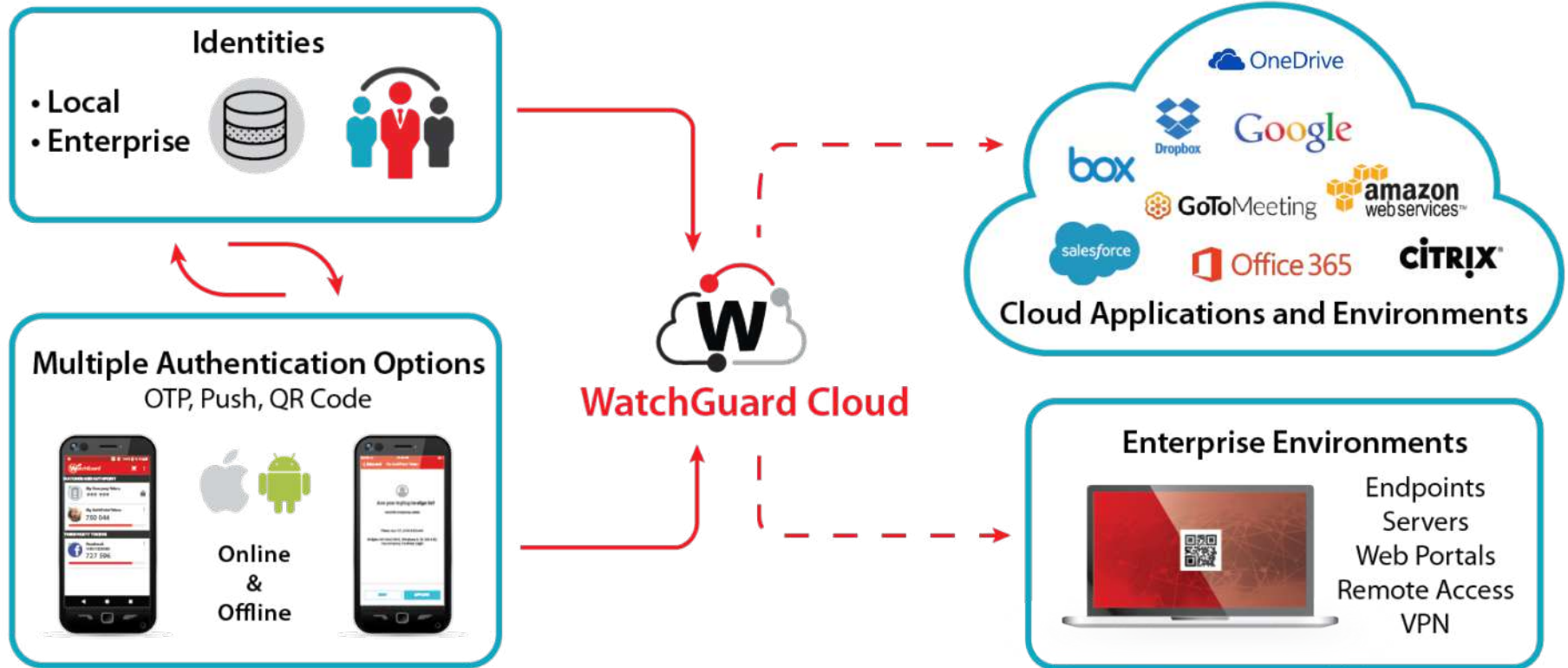


AuthPoint factors:

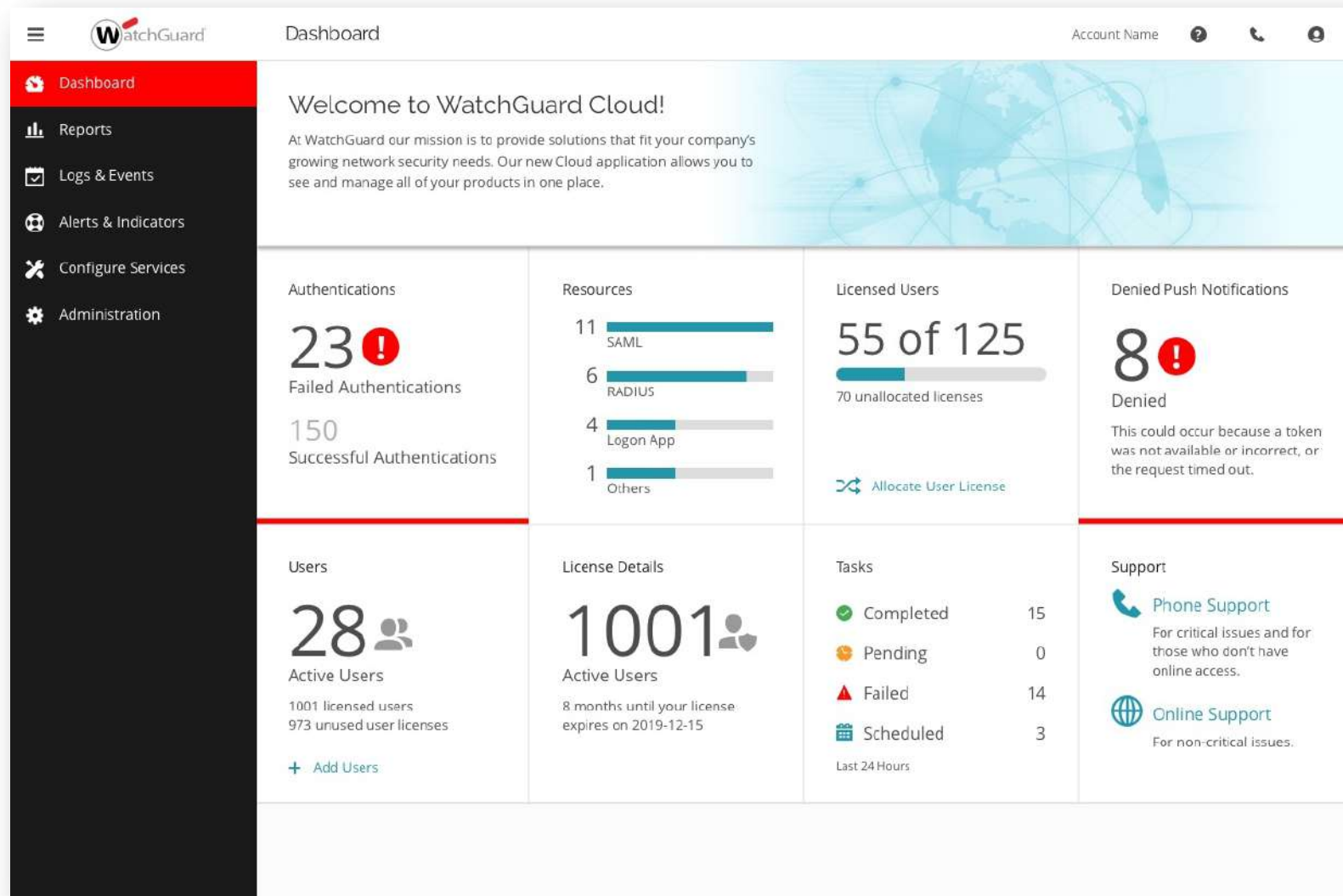
1. Your password
2. Approval on your mobile authenticator
3. Correct mobile phone DNA
4. A fingerprint to access
(with certain phone models)



Protegge VPNs, Web Apps, PC Login...



WatchGuard Cloud – Manage from Anywhere



WatchGuard Cloud – Configure

The screenshot shows the WatchGuard Cloud 'Configure Services' dashboard. The left sidebar contains navigation links: Dashboard, Reports, Logs & Events, Alerts & Indicators, **Configure Services** (highlighted), and Administration. The main content area is titled 'Configure Services' and features a banner for 'Introducing AuthPoint' with a 'CONFIGURE AUTHPOINT' button. Below the banner, there are four summary cards: 'Users' (28 Active Users, 1001 licensed, 973 unused), 'Groups' (3 Groups Added, largest group has 6 users), 'Resources' (11 SAML, 6 RADIUS, 4 Logon App, 1 Others), and 'Configurations' (4 Providers, 25 Gateways). Each card has an '+ Add' button.

WatchGuard Configure Services Account Name ? ☎ ?

Introducing AuthPoint

AuthPoint is at the forefront of technologies that are specifically designed to prevent unauthorized access and fraud while also enabling business growth. With an unmatched combination of protection and ease of use, AuthPoint products are uniquely simple, yet powerfully secure.

[CONFIGURE AUTHPOINT](#)

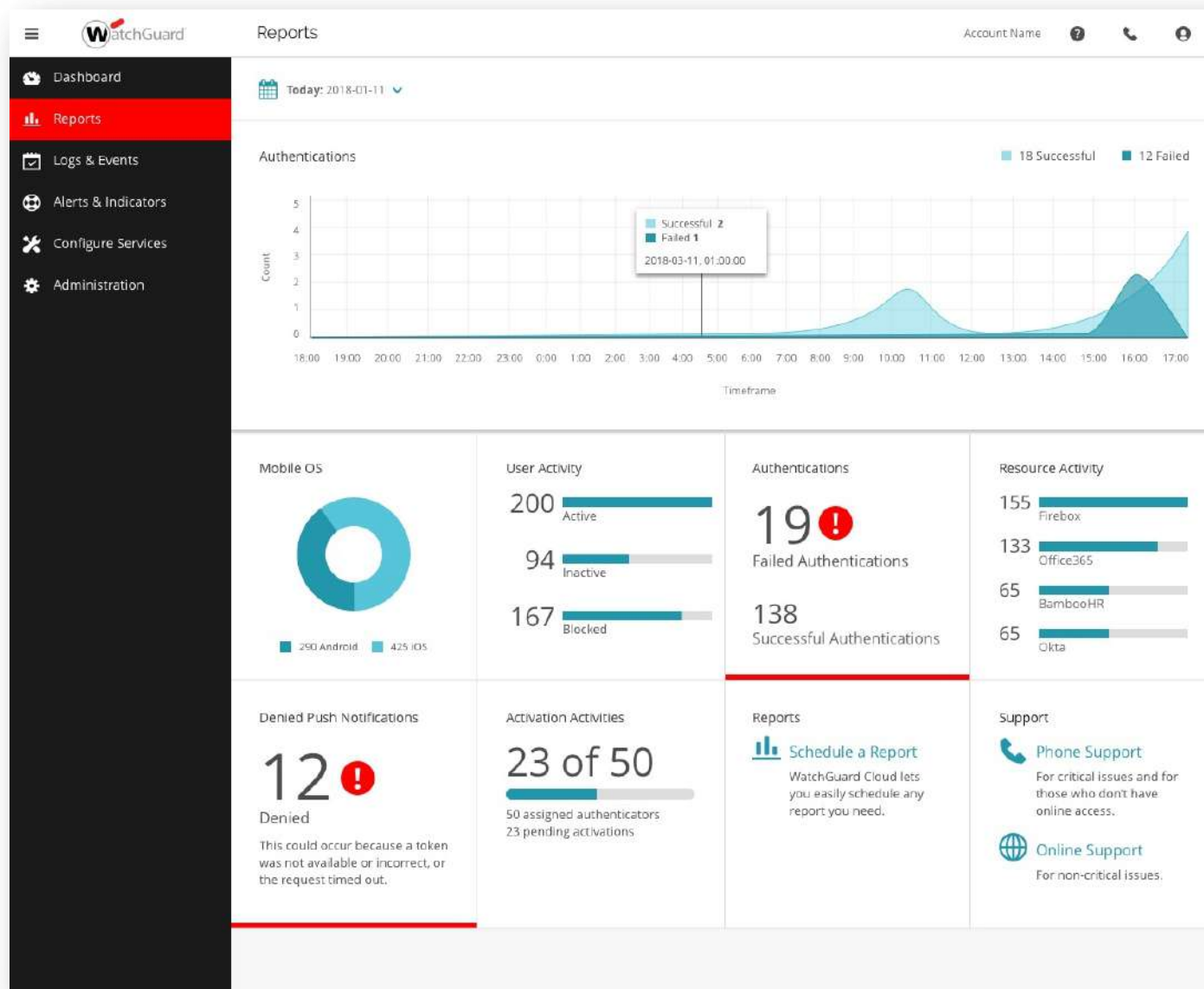
Users	Groups	Resources	Configurations
28 Active Users 1001 licensed users 973 unused user licenses + Add Users	3 Groups Added Your largest group has 6 users. + Add Groups	11 SAML 6 RADIUS 4 Logon App 1 Others	4 Providers 25 Gateways

WatchGuard Cloud – Sync to LDAP or AD and Allocate Tokens Automatically

The screenshot displays the WatchGuard Cloud 'Users' management page. The left sidebar contains navigation options: AuthPoint (selected), MANAGEMENT (Resources, Groups, Users, External Identities, Gateways), and GENERAL (Download, Settings). The main content area shows a table of users with the following columns: USER NAME, NAME, EMAIL, GROUP, and AUTHENTICATION. Each user entry includes a status indicator (red or green dot) and a token ID.

USER NAME	NAME	EMAIL	GROUP	AUTHENTICATION
ssmith	Sean Smith	sean.smith@email.com	AWS local RADIUS	WG-9473E
jmonroe	Juan Monroe (LDAP)	juan.monroe@email.com	AWS local RADIUS	WG-9473D
tsplater	Tom Splater (LDAP)	tom.splater@email.com	AWS local RADIUS	WG-9473F
mcrumb	Malcomb Crumb	malcomb.crumb@email.com	AWS local RADIUS and LDAP	WG-9473A
cconnor	Carl Connor	carl.connor@email.com	AWS local RADIUS and LDAP	WG-9473B
smoran	Shaine Moran (LDAP)	shaine.moran@email.com	AWS local RADIUS	WG-9473C
mwright	Megan Wright	megan.wright@email.com	AWS local RADIUS	WG-9473G
tjuarez	Thomas Juarez	thomas.juarez@email.com	AWS local RADIUS	WG-9473H
kwest	Kyle West (LDAP)	kyle.west@email.com	AWS local RADIUS	WG-9473I
rmcreed	Rex McReed	rex.mcreed@email.com	AWS local RADIUS and LDAP	WG-9473J
rmankowski	Ray Mankowski	ray.mankowski@email.com	AWS local RADIUS and LDAP	WG-9473K
lsmith	Larry Smith	larry.smith@email.com	AWS local RADIUS	WG-9473L

WatchGuard Cloud – View Reports



Online and Offline Multi-Factor Authentication

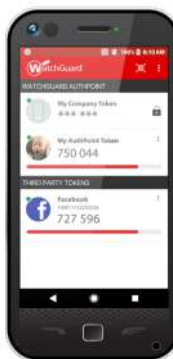


Push-Based Authentication

Secure authentication with one-touch approval. You see who's trying to authenticate, and where, and can block unauthorized access to your resources.

QR Code-Based Authentication

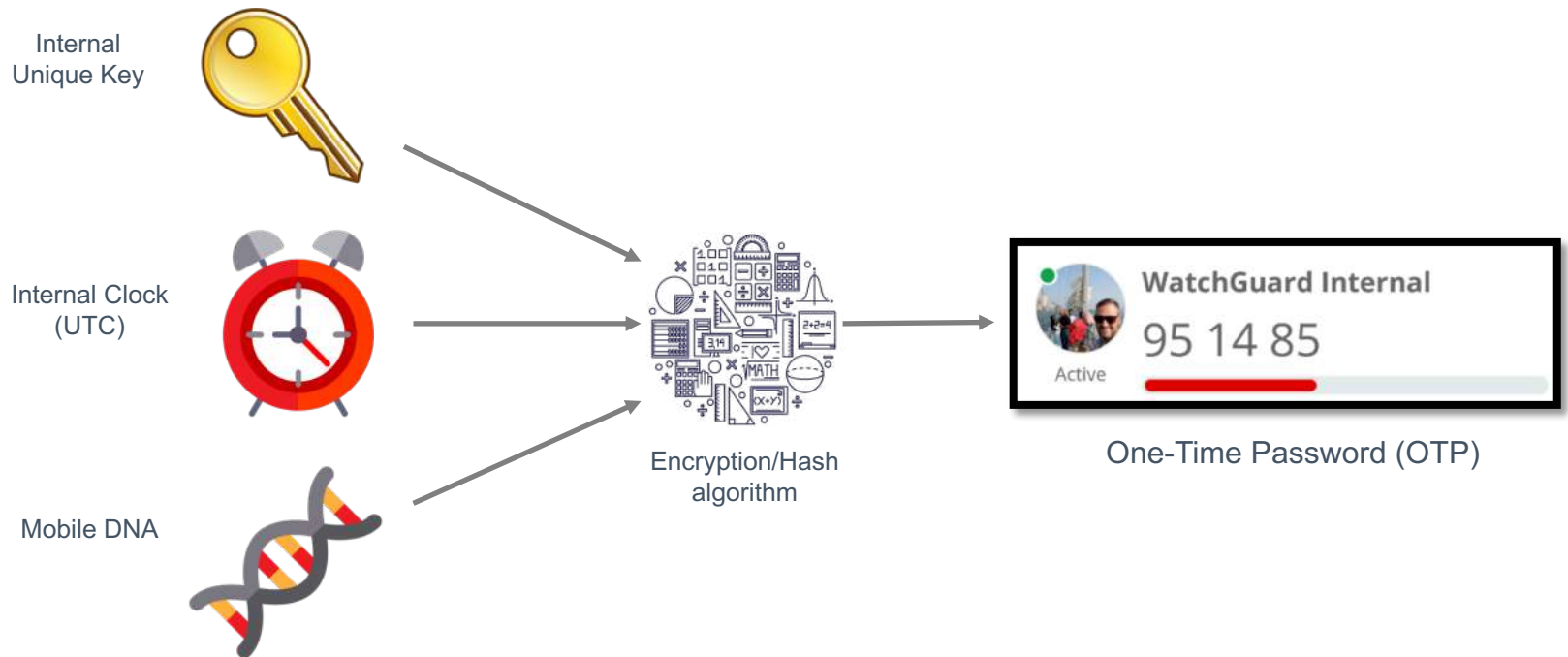
Use your camera to read a unique, encrypted QR code with a challenge that can only be read with the app. The response is typed in, to finalize the authentication.



Time-Based One-Time Password (OTP)

Retrieve your dynamic, time-based, one-time password as displayed, and enter it during login.

Added Security from Mobile Phone DNA



Makes the authenticator even more unique!

MFA Come servizio: ROI altissimo

9,350

Media dati rubati per Data Breach
2017 Ponemon State of SMB Cybersecurity Report

\$1.3M

Media del costo di un Data Breach (\$141 per data record)
2017 Ponemon Institute Cost of Data Breach Study

\$0

Costo per nuova infrastruttura, hardware tokens, e software maintenance with a Cloud MFA service



Un mese di questa **protezione essenziale** per utente costa meno del nostro cappuccino mattutino.

Essential Security for the Modern Business

THE WATCHGUARD SECURITY PORTFOLIO



Network Security



Secure Wi-Fi



*Multi-Factor
Authentication*

Costruisci la tua offerta di sicurezza

Contact a WatchGuard authorized partner to get started
or visit www.watchguard.com