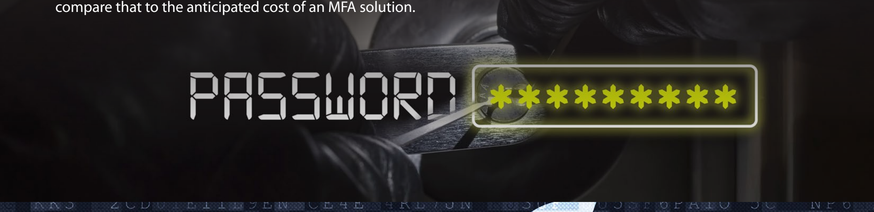
Multi-Factor Authentication ROI

About 1 in 5 people consistently use weak or shared passwords…
How many of them work in your organization?

Given that it takes just one stolen password to compromise your network, you have to ask yourself, how likely is it that one or more of your employees are mishandling their passwords? Even more alarming, the costs associated with a breach can reach millions of dollars with direct fines, investigation and remediation expenses as well as indirect expenses from lost customers and low employee productivity. The following statistics can help to quantify the risks and compare that to the anticipated cost of an MFA solution.



DATA BREACH RISKS/EXPENSES

9,350
Average number of breached records

Quantity of **stolen data** in the average breach is **9,350 records**
2017 Ponemon State of SMB Cybersecurity Report

$1.32M
Average cost of breached records

Average cost of a data breach = **$141** per data record containing sensitive information
2017 Ponemon Institute Cost of Data Breach Study

81%
Percentage of breaches facilitated with weak/stolen passwords

This is the **#1 tactic** used by hackers
Verizon Data Breach Investigations Report 2017

3
Number of users out of 100 with 123456 as a password

10% of people have used at least one of the 25 worst passwords on this year's list, and nearly 3% of people have used the worst password, **123456**
Http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

6
users out of 100 that use the same password for all online logins

6% of 100 U.S Internet users are using the **same password** across all accounts in 2017
(https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/)

1
Number of lost/stolen passwords needed to breach a network without MFA

File with **1.4 Billion** hacked/leaked passwords found on the dark web
"ready for would-be hackers to pump into so-called 'credential stuffing' apps"
(Forbes, Dec 11, 2017)

ESTIMATED INVESTMENTS IN A CLOUD-BASED MFA SOLUTION

$0
Additional infrastructure to host Authentication Mgmt.

All management is available using Cloud computing and **included in the price.** Some features require software on the gateway and agents

$0
Hardware token purchases

The free mobile app is the authenticator on a **smartphone** – requires no additional hardware

$2700
Estimated annual cost of MFA service per 100 employees

Assumes **$2.25/user/mo** – use for reference purposes only. Contact a WatchGuard partner for specific AuthPoint pricing

Minimal
IT staff expenses

Token deployment is **automated,** so recurring IT staff activities are mostly from maintenance and monitoring

CLOUD-BASED MFA BENEFITS FAR OUTWEIGH THE COSTS

Mitigate the risk of a breach resulting from a stolen password by adopting multi-factor authentication (MFA). Cloud-based MFA requires no expenses for additional infrastructure, hardware tokens, software support and maintenance.

WatchGuard AuthPoint

AuthPoint provides multi-factor authentication (MFA) on an easy-to-use Cloud platform. The AuthPoint mobile app makes each login attempt visible, and as a Cloud service, there's no hardware to deploy. It can be managed from anywhere and features integrations with 3rd party applications including popular Cloud applications, web services, VPNs and networks. **Learn more at www.watchguard.com/authpoint**

WatchGuard®