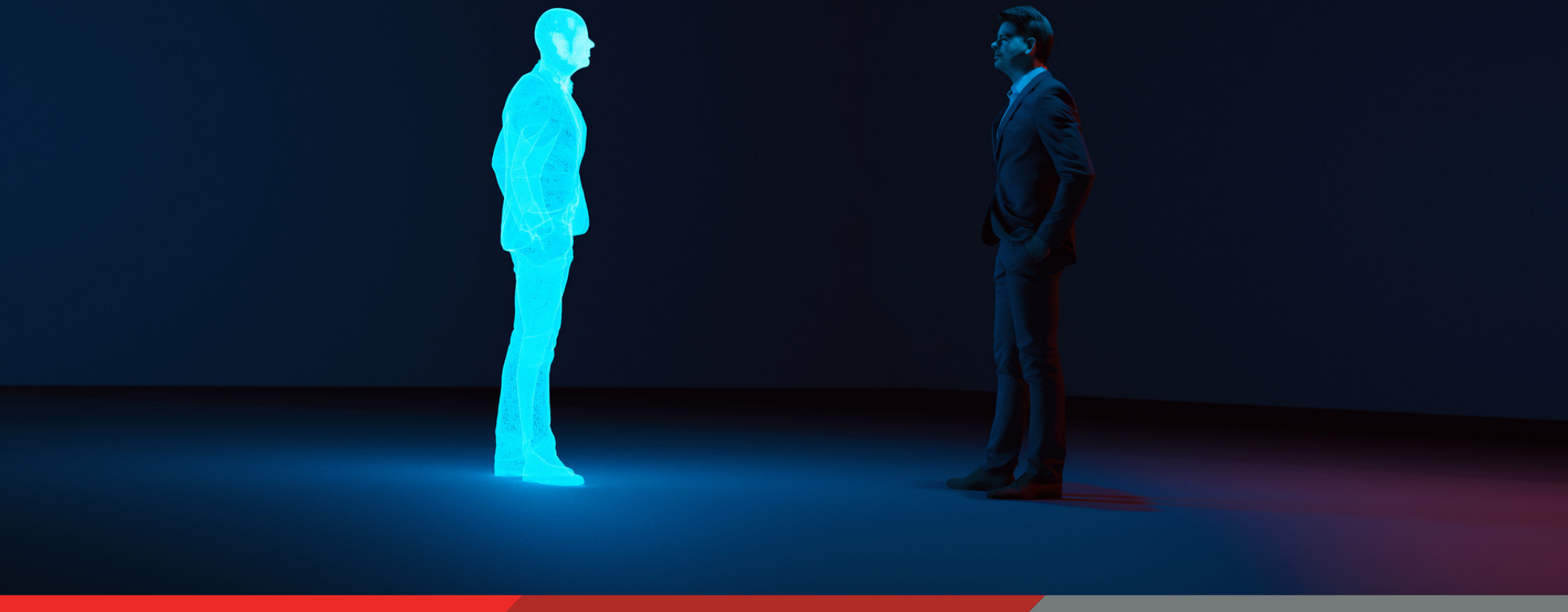
CCS Media

WatchGuard

DON'T WAIT UNTIL IT'S TOO LATE.

ADD SECURITY TO KEEP IDENTITY REAL.



You're Only One Weak Password Away from a BREACH

... And even your "complicated" passwords can be cracked.
Passwords are simply no longer enough to keep your assets, accounts, and information secure.

Here's some evidence as to why:

74% of 2022 breaches involved the human element, including stolen credentials[1]

51% of people use the same password for work and personal accounts[2]

Ultimately, people choose **weak passwords**

Here's a List of the 20 Passwords Most Commonly Found On the Dark Web[3], Due to Data Breaches:

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

It's Not Hard for Passwords to Fall into the Wrong Hands

A full set of credentials can be purchased on the dark web for $8-25,[4] making it both cheap and easy to attempt to breach systems. And if that doesn't work, a skilled cybercriminal could crack most people's passwords in the time it takes for you to read the list of passwords on the previous page.[5]

Passwords are easy to hack and provide only one line of defense. If a hacker can steal just one employee's password, they can usually access your entire network. Once in, they can do whatever they want. This usually means spreading malware or stealing, modifying, or deleting critical information.

WatchGuard

Stealing Your Password Is Easy

The process of stealing a password is shockingly easy (and profitable) for hackers. Their password-guessing tools and technologies have become exponentially more sophisticated and automated to the point that manual password "guessing" is often not required. Even when it is, advanced algorithms, social engineering (e.g. phishing attacks or trojan horses), keylogging, and other methods allow them to efficiently guess and test the most likely passwords, which is very often successful.

Some common password hacking methods include:

Dictionary Attack

Hackers try to guess a password by typing in a common list of words from a password dictionary. More advanced password dictionaries include lists of the most commonly used words in passwords. This is a relatively simple method, but one that is effective in guessing less complex passwords. If you use real words in any of your passwords, your credentials are at risk.

Brute Force Attack

While not as efficient as a dictionary attack, a brute force attack is more effective in eventually guessing a password. With this method, hackers use tools to repeatedly try every possible password combination of letters, numbers, and symbols until the password is cracked. A similar approach is a reverse brute force attack, in which a hacker tries one password against many usernames.

Rainbow Attack

This method uses a resource called a rainbow table to crack password hashes (essentially scrambled up passwords stored in system databases) in a much more efficient and effective way than brute force or dictionary attacks.

Credential Stuffing Attack

Since so many people use the same passwords or variations of passwords across accounts, hackers found a way to automatically run database lists of breached username/password combinations against a target website login. According to Shape Security, 90% of login attempts at online retailers are from this type of attack and this method is effective for hackers about 3% of the time.

Social Engineering

This approach comes in a number of styles, all of which are rooted in the idea of deceiving or manipulating people into divulging their information or taking a certain action. Common social engineering methods used to steal passwords include phishing and using a trojan horse attack. A less common approach is shoulder surfing, in which the hacker simply watches a user type in his or her password.

With the increasing sophistication of hacker technologies and tools, the easiest step of a hack is often cracking the password. In fact, it's so easy that many times it doesn't even involve guessing at all. The scariest part about this is that regardless of how secure your password is, all it takes is one colleague's weak password to put your company's entire system at risk for a breach.

Lost or stolen credentials earn hackers money by enabling data theft or access to your business systems where ransomware or other profitable malware attacks can be executed. Computer security expert and white hat hacker Roger Grimes describes this process in his book *Hacking the Hacker*.

According to Grimes:

> If the hacker has done their homework in the fingerprinting stage, then this stage really isn't hard at all.

That is to say, it's easy for hackers to access your accounts. Some also cover their tracks or create a doorway for future access, although this is not always the case.

How do you ensure that the person with the password is really the person they are claiming to be? How can you keep identity real?

Experts in governments and independent agencies around the world are offering sage advice about protecting business systems from attacks. A recent alert from cybersecurity authorities from the US, New Zealand, Canada, the Netherlands and UK concludes that hardening credentials with the use of MFA and strong password policies are best practices against the growth of cyberattacks.[6] And that's not just any kind of identity and credentials protection, as the criminals become more sophisticated, so do our security solutions. As a case in point, in August 2021, CISA added single-factor authentication to their list of Cybersecurity Bad Practices[7] – a clear message to all those organizations that rely solely on passwords for protection.

Many Organizations Have Attempted to Change Employee Behavior Around Passwords

One method of mitigating the risk of having a password stolen is to train your employees to create stronger passwords and to change those passwords more frequently. However, changing the behavior of every single employee is not only challenging, but in this case ineffective.

Historically, this approach doesn't work

This is evidenced by the millions of companies whose databases have been hacked and the tens of millions of leaked passwords that are available online (note that one can purchase many of these credentials on the dark web).

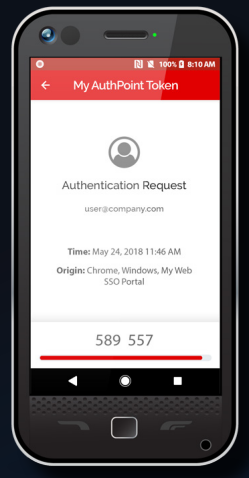
It creates an overly complex user experience

Using unique, completely randomized, 16-character passwords across accounts is complex. The reason people use simple passwords is that passwords are hard to remember. Many people create slightly more complex ones, but compensate for that complexity by reusing that same password (or variations of it) across accounts.

Since passwords aren't enough, what is?

Multi-factor authentication (MFA) adds a security layer to logins beyond just a simple username and password. It helps ensure that hackers cannot access your systems even if one of your employee's passwords becomes compromised. Specifically, a multi-factor approach is preferred over a single-factor authentication because it includes:

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



Note of Caution: Not all MFA Solutions Are Created Equal

SMS-based multi-factor authentication is no longer a trusted, secure method. Users with SMS-based authentication should migrate to other methods immediately. In its 2016 Digital Identity Guidelines, the National Institute of Standards and Technology (NIST) encouraged users to move away from SMS-based authentication:

"Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems should carefully consider alternative authenticators. Out-of-band authentication using [SMS or voice] is deprecated and is being considered for removal in future editions of this guideline."

Harvard Business Review went even further, stating: "It could be argued that SMS authentication became more of an attack vector than a security measure."

The reason SMS-based authentication is risky is that text messages are vulnerable to being intercepted. Reddit was a notable victim of this in 2018. Reddit commented on the attack on its own site, attributing the hack to the weakness of SMS-based authentication: "We learned that SMS-based authentication is not nearly as secure as we would hope, and the main attack was via SMS intercept. We point this out to encourage everyone here to move to token-based 2FA.

While using SMS-based MFA is better than relying on a password and username alone, it still leaves users vulnerable to being hacked. To mitigate this risk, companies should rely on MFA that only uses stronger methods of authentication.

Protecting the Password Is Also Important!

While MFA alone helps a great deal, passwords are still considered for identity validation, which is why the cybersecurity experts also recommend additional credentials hardening and monitoring. In particular, a business-grade password manager product is a win-win proposition for many companies. Not only does it promote the use of unique, complex passwords, but provides a tool to users so that they can access and recall those passwords easily and securely when needed. Even better, the password manager and MFA can be deployed and managed together for an efficient solution built to the specific requirements of businesses.

Given the strong trade in lost/stolen credentials on the dark web, a monitoring service can also offer companies valuable time to become alerted to a breached set of credentials for their domain, before it can be used in a damaging attack.

WatchGuard offers an easy-to-use multi-factor authentication solution with a corporate password manager and dark web monitoring service in our AuthPoint Total Identity Security package.

How Does AuthPoint Total Identity Security Help?

AuthPoint MFA is a multi-factor authentication (MFA) service that helps companies keep their assets, information, and user identities secure. It works by requiring users to use 2+ authentication factors to log in, rather than relying on a password alone. Additionally, Total Identity Security includes our Corporate Password Manager and Dark Web Monitor service. You benefit with:

Multiple layers of authentication

Companies can significantly reduce the risk of having their accounts hacked. If a hacker gets hold of an employee's password, there is still another layer of security to help prevent the hack.

Management from WatchGuard Cloud – one interface for easy administration

The AuthPoint Total Identity Security products are managed entirely in the Cloud. This means that there's no expensive hardware to deploy and no software to update.

Happy users and streamlined adoption

Users approve or deny logins with a single touch on the AuthPoint mobile app. Once they've logged in, users can enjoy single sign-on (SSO) for fast access to their applications and environments. Even better, the Corporate Password Manager is available from the same AuthPoint app and can be used for both business and personal passwords.

A solution built for businesses

Unlike 2FA and password managers built for consumer use, AuthPoint was designed to address corporate use cases. For example, it authenticates users at Windows/macOS startup, including both online and offline access, meaning users can securely log in even if accessing their account from an airplane.

Powerful protection is available to you at less than the price of your morning cappuccino

Would you bet your business on the strength of every employee's password? Keep identity real with AuthPoint. It's affordable, it's powerful, and it's easy to use.

Keep Identity Real with WatchGuard AuthPoint

WatchGuard