

**Would you bet your
business on the
strength of every
employee's password?**



Because Your Passwords Suck
Approve Yourself, Deny Imposters

Be Authentic
With AuthPoint MFA
WatchGuard Technologies

Table of Contents

You're only one weak password away from a breach 3

Think your passwords are strong? That won't stop hackers 4

Time to crack your password 5

A simplified overview showing how a hacker steals your password 6

Stealing your password is easy 7

Authentication defense: Changing employee behavior around passwords simply doesn't work 8

Since passwords aren't enough, what is? 9

Note of caution: Not all MFA solutions are created equal 10

How does AuthPoint work? 11

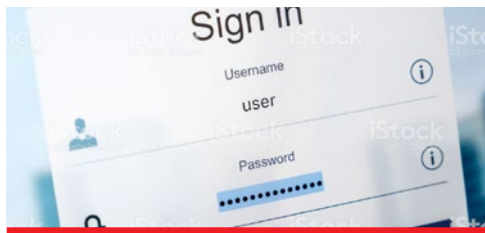
Is AuthPoint right for you? 12



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:



80% of users **REUSE** passwords across accounts²



6% of Internet users use the **SAME** password across all online accounts²



About **46%** of employees use **personal passwords** for company accounts³

People Choose Weak Passwords

The Top 25 Weak Passwords in 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 | |

1. <https://www.teamsid.com/worst-passwords-2017-full-list/>

2. <https://www.csoonline.com/article/3244137/password-security/password-managers-grow-up-target-business-users.html>

3. <http://www.statista.com/statistics/763091/us-use-of-same-online-passwords>

4. <https://www.fastcompany.com/40469838/dashlane-reused-password-hygiene>

Think your passwords are strong? That won't stop hackers.

They can simply purchase credentials on the dark web in a similar way that you'd make a purchase on amazon.com.

Average price of a password on the dark web⁵: **\$160.15**

Average value of a user's identity (credentials across accounts) for a hacker: **\$1,200.**

If your IP, financials, customer information, employee information, or anything else in your network is worth more than \$1,200, it's simple economics that it is profitable for a hacker to purchase access (i.e. your credentials) to that information.

**Think it wouldn't happen to *your* credentials?
Or your colleague's credentials?**

There are billions of credentials available on the dark web, many of which belong to admin users. In late 2017 alone, a single file containing 1.4 billion plain text passwords was discovered.⁶ Chances are, your login information could be purchased within seconds.

Once on the dark web, buying your passwords is as easy as making a purchase on Amazon. At right are some images of dark web credential purchase pages.

This screenshot shows two listings on a dark web marketplace. The first listing is for 'Yahoo | 100K | Email:Pass | Decrypted | Instant Delivery' priced at USD 10.76. The second listing is for 'Gmail | 450K | Email:Pass | Decrypted | Instant Delivery' priced at USD 25.76. Both listings include a 'Buy Now' button and a 'Views' count.

Item	Price (USD)	Views
Yahoo 100K Email:Pass Decrypted Instant Delivery	10.76	975
Gmail 450K Email:Pass Decrypted Instant Delivery	25.76	861

This screenshot shows a listing for 'USA - PERSONAL INFO | 2016 FRESH SSN + DOB FULLZ'. The listing includes a description of the product, a 'Sold by' field, and a 'Features' table.

Features
Product class
Quantity left
Ends in

This screenshot shows a listing for 'Hacked USA Western Union Accounts'. The listing includes a description of the product, a 'Sold by' field, and a 'Features' table.

Features
Product class
Quantity left
Ends in

This screenshot shows a listing for 'W-2 TAX FORMS 2016 ***** \$7.99 ONLY'. The listing includes a description of the product, a 'Sold by' field, and a 'Features' table.

Features
Product class
Quantity left
Ends in

5. <https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366>
6. <https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14>
7. <http://www.cyberinject.com/gmail-yahoo-passwords-on-dark-web/>
8. <https://www.theteneogroup.com/2017/06/08/understanding-deep-web-dark-web-guard-network/>
9. <https://zerohedge.whotrades.com/blog/43790836676>
10. <https://zerohedge.whotrades.com/blog/43790836676>

If a hacker chooses to crack your password instead of buying it, it probably won't take them long to do it.

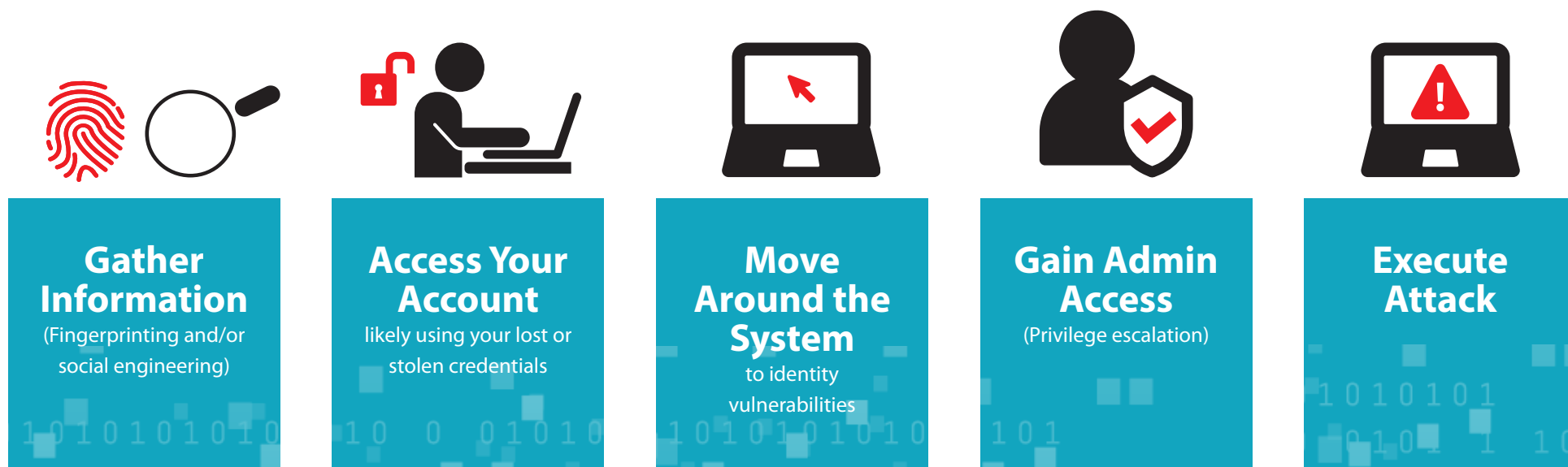
In fact, they could crack most people's passwords in the time it takes for you to read this table¹¹

Type	Password	Time (HSIMP) How Secure Is My Password?	Time (PA) Passfault Analyzer tool	Security Level
8-character common word	required	52 seconds	<1 day	Useless
8 random characters	qkcrmztd	52 seconds	<1 day	Useless
8 random characters w/numbers	kqw8bv32	11 minutes	<1 day	Useless
8 random characters w/mixed case, symbols, & numbers	J5bZ>9p!	20 days	<1 day	Risky
Type	Password	Time (HSIMP)	Time (PA)	Security Level
2 common word password	orange tea	98 days	<1 day	Risky
3 common word password	this is cool	546 years	<1 day	Risky
5 uncommon word password	du-bi-du-bi-doo	12 million years	<1 day	Risky

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.

11. <https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/>

Here's a simplified overview showing how a hacker steals your password, as described in "Hacking the Hacker" by computer security expert and white hat Roger Grimes:



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.



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 using 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.

Authentication Defense:

Changing Employee Behavior Around Passwords Simply Doesn't Work

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).

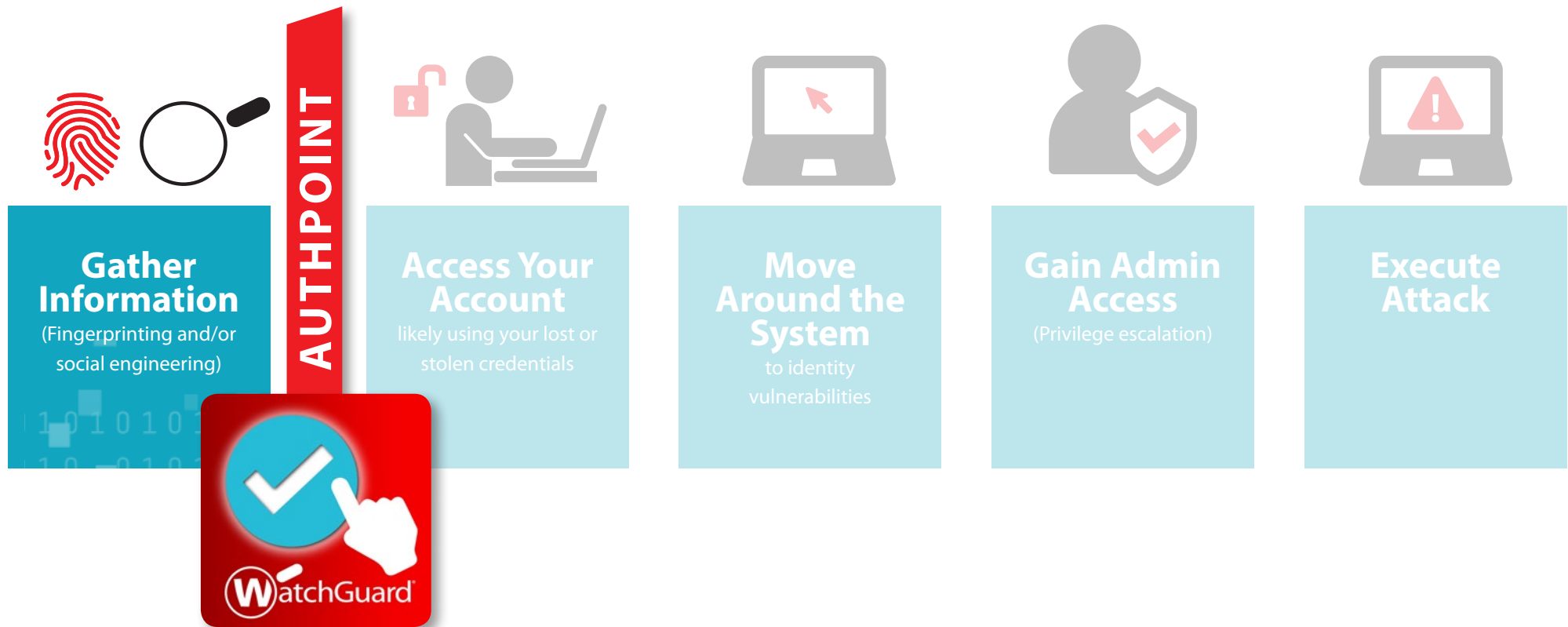
It creates an overly complex user experience

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) is a method of verification that 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.



WatchGuard offers an easy-to-use multi-factor authentication solution that helps companies keep their assets, information, and user identities secure: AuthPoint.

AuthPoint® is easy to deploy, easy to manage, and is available for less than the cost of a cup of coffee per month per user. It's also more secure than two-factor authentication (2FA), more secure than SMS-based solutions, cheaper (lower TCO) than non-Cloud-based solutions, and easier for end users than solutions that require tokens.

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.



How does AuthPoint work?

AuthPoint 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.

These factors are a combination of:

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

Password

••••••

By using **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.

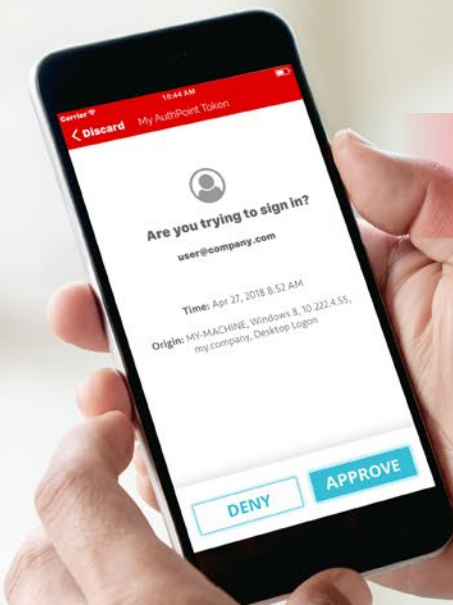
With AuthPoint, this protection is easy. Users approve or deny logins with a single touch on the AuthPoint mobile app. Once they've logged in, users can enjoy single sign-on (SSO) across key accounts.

Since approvals are all done through the user's mobile app, there aren't additional tokens to carry. It's easy!

AuthPoint is based entirely in the Cloud. This means that there's no expensive hardware to deploy and no software to update. It can also be managed from anywhere and, since it's so easy to deploy and manage, it doesn't require an in-house security expert to get started.

Travel for work? AuthPoint functions both online and offline, meaning users can securely log in even if accessing their account from an airplane. By using QR code-based authentication, users can log in anywhere, at any time.

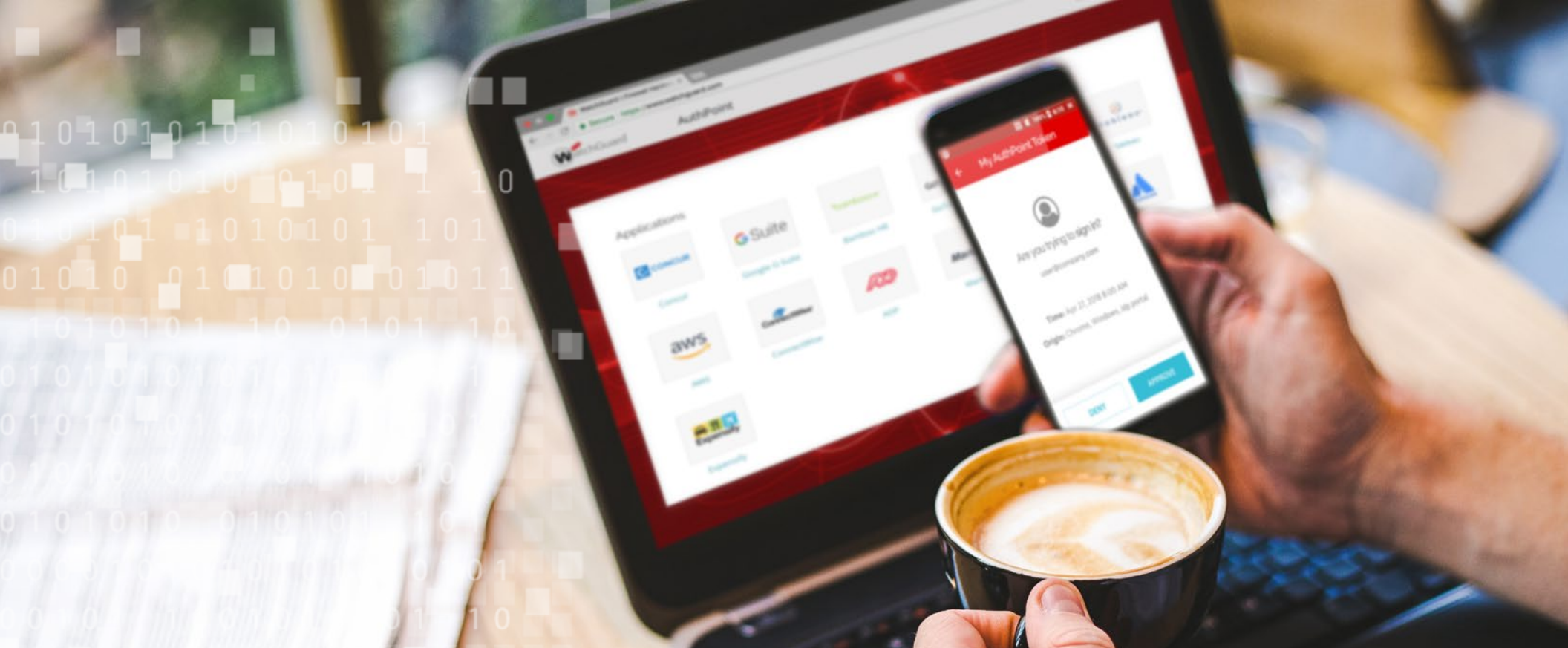
Learn more about how AuthPoint helps keep companies secure:
www.watchguard.com/authpoint





Is AuthPoint right for you?

Since passwords are so easily stolen or cracked, many organizations are adopting multi-factor authentication as a means of keeping their user identities and assets secure. WatchGuard wants to make this protection available to companies of all types and sizes, so it created AuthPoint multi-factor authentication. Multi-factor authentication is one of the most important safeguards needed to protect modern small and midsize businesses and it's now available through your WatchGuard reseller.



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

**So, would you bet your business on the strength of every employee's password?
With AuthPoint, you don't have to. It's affordable, it's powerful, and it's easy to use.**

**Contact your WatchGuard reseller to start your free 1-month AuthPoint trial today.
For more information about AuthPoint, visit www.watchguard.com/authpoint.**

THE WATCHGUARD SECURITY PORTFOLIO



Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing management, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.



Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.



Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit <https://www.watchguard.com>.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit [WatchGuard.com](https://www.watchguard.com).



North America Sales: 1.800.734.9905

• International Sales: 1.206.613.0895

• Web: www.watchguard.com/authpoint

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2019 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and AuthPoint are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67135_022019