MICRO FOCUS

Flash Point Paper

Security

The Right Level of Authentication:

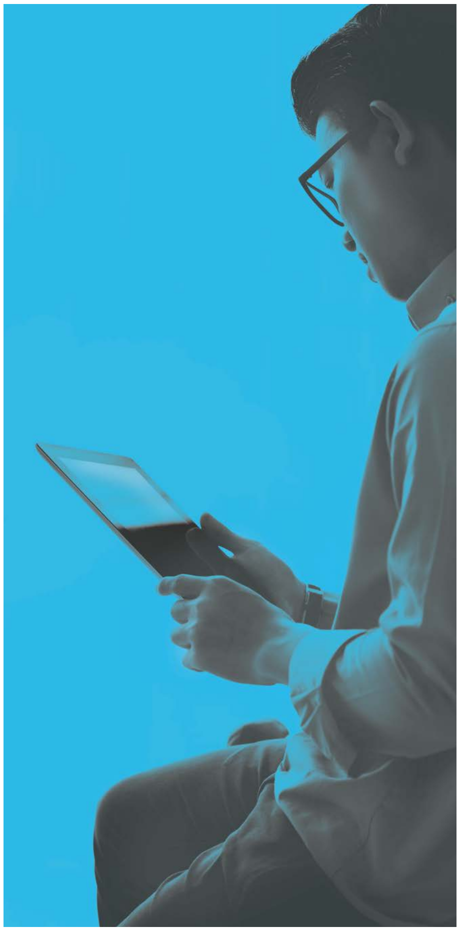
Stolen Credentials Are the Most Common Weapon Used in a Breach

It doesn't take a rocket scientist to observe that stolen credentials is the single most common way that outsiders gain access to your private information. In fact a simple Google of the words "stolen credentials" brings up quite a long list of both an interesting and scary list of breaches. It also brings up some of the biggest.

Anthem lost private information for 80 million of its customers. Those records were accessed from stolen credentials of a privileged user who had access to that information.

Both Target and Home Depot's point of sale breaches were also due to stolen credentials. It's noteworthy to point out that in these cases, the breach wasn't through an internal user's account but, rather, through the accounts of privileged users located at third-party service providers whose credentials were stolen.

Although outsiders gain access to insider credentials through various means, phishing is the most popular method. It requires relatively little investment and is highly effective. Other credential-related vulnerabilities include weak passwords and credentials shared across multiple systems. Weak passwords are a challenge. Managing against them requires a balance of establishing the ultimate password and allowing users to choose something that they can actually remember, especially for environments where no single sign-on is used.



A broader view of credential usage reveals that it's not unusual for people to use a common set of credentials across all the services they use, both internal and cloud based. Consequently, if any of the systems that shared credentials reside on are compromised, all of the other systems are vulnerable as well. The unfortunate truth is that months often go by before individuals are notified that their credentials were stolen.

Why Risk-Based Authentication May Be Right for You:

- *Stolen or compromised credentials is a major tools used by information thieves*
- *The protection from passwords aren't always secure for what's at stake*
- *Maintain convenience by invoking step-up authentication only when the risk level warrant it*

Whether You're Big or Small, Your Risk Is Big

Why should small businesses worry about risks posed to them from data breaches? After all, many owners think computer hackers and identity thieves only target big corporations. But, based on a survey conducted by Ponemon Institute, more than half of you have already been hacked. The reality is that the thieves know that small businesses (SMB) have valuable information just like the large ones. While it's true that, relatively speaking, SMB insider information (often customer and employee lists) is a small trophy, easily compromised weak security makes it a good return on the hacker's investment. It's not uncommon for an online SMB retailer to lose 5k to 20k from stolen credit card records. Not bad for a day's work.

For enterprise-level businesses, the risks are even more noteworthy, almost larger than life. Scarcely a week goes by without a household name or high profile organization being headlined with a warning of massive loss of private information. And with the growing list of retail, healthcare, financial and government organizations that have experienced serious breaches, it's not all that surprising to see heads roll.

So whether you're a CEO, CIO, government Director or otherwise responsible for keeping your business safe, the risks created by stolen credentials are real. And risk is more than someone getting a hold of a privileged user's credential; it's also the ability to use it undetected.

Add More Security Than Just What Your Users Know (Passwords)

A recent Ponemon Institute survey claims that almost half of all companies have been breached in the last 12 months. Of course, the cause as well as the seriousness of these breaches vary, but considering that compromised credentials account for over half of these failures, it does beg the question of how heavily you should depend on credentials alone. Based on some key findings from Verizon's breach report, here are a few dominant trends worth noting:

- **About 8 out of 10 breaches are password related.** This is huge. In fact, nearly all of the most costly and highest publicized breaches involved stolen or shared credentials. You're not going to be able to secure your business as long as this barn door is open.
- **About 2 out of 3 companies have at least six different password policies.** Having a complex password environment forces users to write them down to keep them straight, not to mention the need for credential sharing when they are locked out.
- **About 2 out of 3 companies that allow partner access to resources and internal information rely solely on passwords for users to verify their identity.** This is account sharing on steroids. Because updating accounts is a hassle and often a low priority, partners often allow multiple people to use a shared account.

DOMINANT TRENDS WORTH NOTING:

8 out of **10** breaches
are password related ***

2 out of **3** companies
have at least 6 different password policies

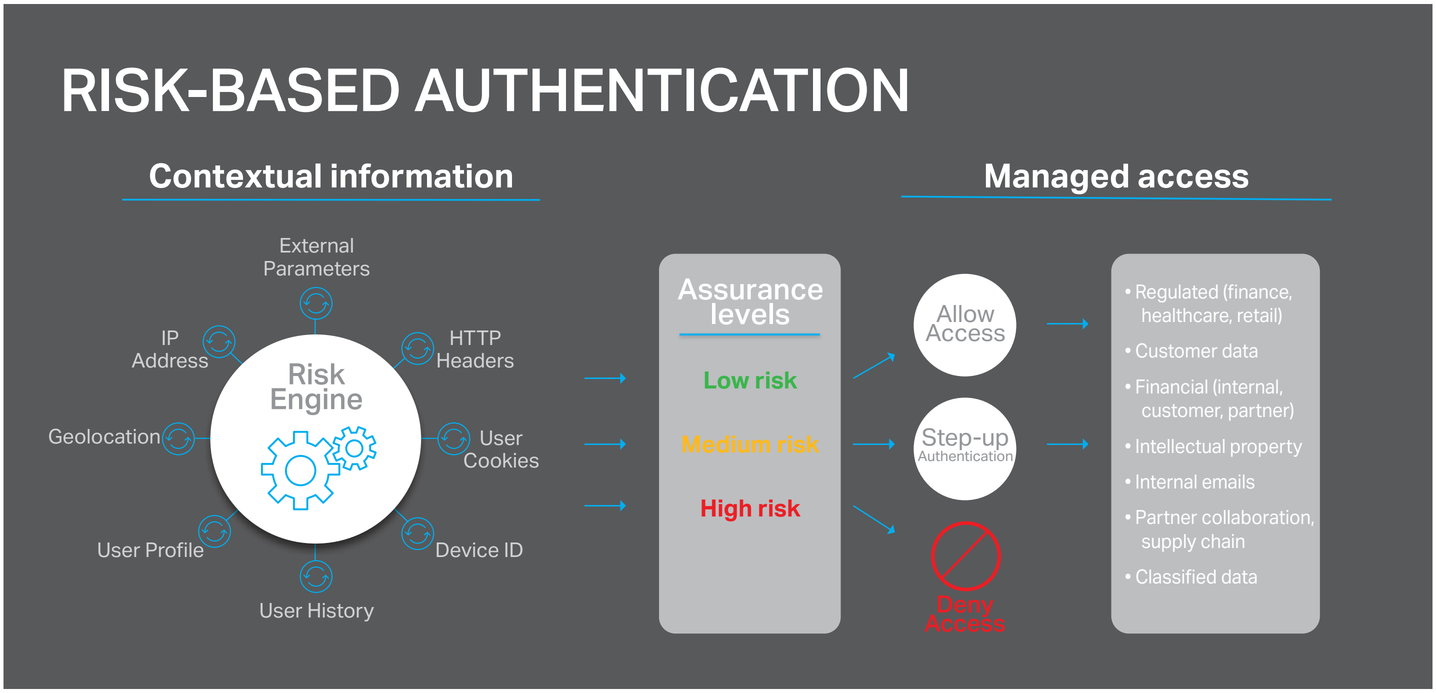
2 out of **3** companies ***
rely solely on passwords

The bottom line is that it's next to impossible to keep passwords away from criminals and other outsiders. Among the most formidable methods that attackers use is phishing, the act of fooling a person to hand over information. These kinds of attacks have been on a rapid rise in recent years, obviously because they are so effective. In fact, a few years ago, Trend Micro reported that more than 9 out of 10 targeted attacks were in the form of phishing. Trend Micro goes on to say, "These targets may either be sufficiently aware of security best practices to avoid ordinary phishing emails or may not have the time to read generic-sounding messages. Spear-phishing significantly raises the chances that targets will read a message that will allow attackers to compromise their networks."

9 out of **10** attacks
were spear phishing

Authentication Needs More Intelligence

Multi-factor authentication provides a robust way to verify a user's identity because it requires more than just what a user knows, such as a password or challenge question. It can be configured to require another method involving something you have, such as a cell phone



or other authentication device. Or, it can be something you are, such as some kind of biometric reader. The catch is that for many environments, you will drive your users crazy if you require them to perform that extra step every time they need to get work done. For these situations, there needs to be a way to limit that extra layer of identity verification to only when the business risk warrants it.

You can think about risk-based authentication as intelligent authentication. It's intelligent because it leverages the user's behavior and activities to decide if another method of authentication is needed to verify the user's identity. Those characteristics include attributes like the user's location, time of access, whether or not the device is known, as well as the type of asset being accessed, etc.; all of which provide context relevant to determining the risk of the request access. That context is processed through a risk engine to determine if another level of user validation is needed.

While you can go wild with sophisticated inference engines, the reality is that even basic metrics provide an effective way determine when another step in the authentication process is in order. Here are a few metrics to consider:

- **The user is accessing some private information for the first time**—this is the perfect time to require a step up authentication.
- **The user is accessing private information from a unique location, using a device that hasn't been seen before**—the best policy might be to deny access altogether.
- **The user is on a known device from an expected location to previously accessed information**—a traditional credential is likely to be secure enough, even for single sign-on environments.

So while thieves have honed their skills at stealing credentials, understanding and impersonating a user's context is dramatically more complicated. Whether you think of this approach to authentication as step-up, adaptive or risk-based, it's essentially the same. More importantly, it's one of the most effective security upgrades you can make.

Using Convenience to Increase Security

MWhen you're able to narrow the use of multifactor authentication to situations where the measured risk warrants it, you have the

Dynamic Authentication can increase both security and convenience.

Contact us at:
www.microfocus.com

Like what you read? Share it.

flexibility to apply it to a broader spectrum of internal information. This means that users will typically enjoy secured yet unfettered access as part of their single sign-on environment, while at the same time they will be required to deliver a step up authentication when the potential risk merits it.

Security Needs More Intelligence

The best strategy against internal threats from privileged users, internal or impersonated, is a layered approach. Micro Focus® offers solutions that enable you to manage what your privileged users have access to, as well as track what they have done.

Getting Risk-Based Authentication Right

As you consider the risks that remote access poses to your organization, take the time to define the right level of identity assurance for each class of information or data. Micro Focus recommends that you go through this exercise for employees, contractors, partners, etc. For each class of information you need to evaluate the level of exposure to potential financial loss and where applicable mandate violations. You also need to consider likely damage to corporate reputation as well as loss of consumer trust.

1. **Catalog the different levels of identity assurance (little, confidence, high confidence, very high confidence) that is appropriate for each type of information you protect.**

2. **Assign the proper type of threat mitigation (user verification) method based on risk rating.**

3. **For information or resources that merit a higher risk rating, avoid static factors where possible. Dynamic factors are significantly harder for hackers to defeat.**

In addition to providing integrations for most any method of user verification desired, Micro Focus is ready to help determine what is right for you.