Tech Data | Security Solutions

Making MFA a Vital Part of Your Security Offering

INTRODUCTION

If you ask a service provider if cybersecurity is paramount to today's IT landscape, they might chuckle and say something along the lines of, "is water wet?" The threat landscape is becoming more dangerous and cyberattacks are getting more sophisticated by the day, with hackers constantly introducing new malware variants and finding network vulnerabilities to exploit.

2020 was a banner year for cyberattacks and data lost due to breaches. The COVID-19 pandemic brought about a remote workforce, providing even more inroads and opportunities for cyberattacks. In 2020, breaches proved to be just as insidious and difficult to stop as the pandemic itself. Cyberattacks on healthcare facilities, for example, in the U.S. this year alone have affected 17.3 million people in 436 breaches tracked by the U.S. Department of Health and Human Services (HHS) Breach Portal.

Malicious actors often attack healthcare providers because medical records are best-sellers on the Dark Web, are challenging to track and can sell for up to $1,000 each. State-sponsored cyberattacks discovered at the beginning of 2021 add a new dimension to the cybersecurity arms race that is accelerating.

A single cyberattack can deliver a serious setback to any company's plans and operations, forcing it to spend money, sometimes a crippling amount, and effort on remediation. This soundly thwarts productivity, to say the least, and forces companies to utilize resources that would otherwise be allocated to driving revenue and meeting strategic goals.

"External risk [was] top of mind for security and risk management leaders in 2020, yet COVID-19 has proved how rapidly and how drastically such risks can change," said Jonathan Care, senior research director at Gartner, in a recent press release on the evolving threat landscape. "Bad actors are always looking to take advantage of worldwide events, such as the pandemic, to exploit new vulnerabilities and circumvent even the most advanced security controls."

So, naturally, providers have had to step up the game in terms of building well-rounded security solutions. It is safe to say that the cybersecurity industry has never been more important.

Businesses are looking for ways to protect their assets and data while simultaneously validating their consumer's identities, all while providing the smoothest user experience (UX) possible. This is not an easy feat, so cybersecurity needs to be viewed through a holistic, all-encompassing lens now more than ever.

One of the most important tools to have in your arsenal these days is multi-factor authentication (MFA). MFA is a simple and effective tool that provides another layer of security on top of the login credentials. It enforces additional authentication measures, such as a text message or a fingerprint, before users can access accounts that hold sensitive information or controls.

According to Expert Insights, there are three main types of MFA:

Something you know. This includes passwords and PINs, which can be any phrase or combination of letters, numbers and symbols that should be complicated enough to not be guessed. Passwords should utilize upper case, lower case, numbers and symbols. Passwords should never be less than 12 characters and should not include any common terms, specific dates or proper names related to you.

Something you have. This would be a physical object, such as a USB key or RF card, or some other device/object uniquely identifying you and qualifying as one factor of access. A totem if you will. RF cards usually come in the form of ID badges or credit card-sized objects that have small radio transmitters in them that can be read by another nearby device.

Something you are. This could be a fingerprint, retina scan or voice recognition. It factors in biometrics that are unique to you, becoming a unique identifier for authentication. Biometrics is an area that has advanced fairly quickly in the last 10 years. Ocular/Retinal and fingerprint scanners now verify by reading and measuring your blood vessels. More research is already being done on pairing voice and facial patterns with other biometrics.

The common two-factor authentication (2FA) uses two of these to verify and authorize a user's access attempt, whereas multi-factor authentication (MFA) uses two or more instances of these checks. This makes MFA a stronger solution than 2FA, but just as simple to implement.

Essentially, with MFA in place, businesses have an extra layer of security over their accounts. It ensures that everyone who accesses company information and data are really who they say they are, reducing the risk of account compromise. Multi-factor authentication tools typically send users an email or text, or require a biometric check, such as a FaceID check or fingerprint scan, before users can login.

It is common practice to use passwords to gain entry into our apps, email systems, work databases and bank accounts. Not only that, but we are periodically forced to change those passwords in an effort to keep the bad guys at bay. But the truth is that, on their own, passwords no longer provide an appropriate level of security.

Let's repeat that:

Traditional passwords on their own just aren't secure enough anymore.

Multi-factor authentication has become a vital component of a comprehensive security solution, as it makes stealing your information much harder for the average criminal. In March of 2020, Microsoft engineers claimed that 99.9% of the incidents they deal with could have been blocked by a MFA solution.

Unfortunately, MFA isn't getting a seat at the cool kids' table these days. Is it because it's difficult to implement? Is it cost prohibitive? Is it just not on MSP and end user radars?

It is time for MSPs to look beyond the foundational blocks of managed security. All signs on the path forward point to implementing more advanced and comprehensive security offerings. This now must include MFA.

THE MODERN THREAT LANDSCAPE AND THE STATE OF CYBERSECURITY

What makes cybersecurity so intricate, complex and formidable is the nature of the threat landscape. It is constantly evolving and reinventing in unexpected ways - much like Hydra with its many heads, new threats sprout whenever one is cut off. Company networks, those of both large and small companies, are constantly under this threat. On average, a cyberattack occurs every 39 seconds.

To make matters worse, many of these modern attacks are automated, using bots to constantly take a battering ram to a network's defenses. Large enterprises certainly face the challenges that come with fending off ceaseless threats and attempted attacks, but it is even more overwhelming for small-to-medium-sized businesses (SMBs) that may not have the advanced monitoring, detection and investigative tools to deal with these threats, at least not in-house. They also may not have the necessary fast-response mitigation technology and procedures in place.

SMBs need to become more aware that their size does not exempt them from attacks. In fact, hackers prey upon this naive mindset, viewing them as low-hanging fruit. According to Verizon's "2020 Data Breach Investigations Report," 28% of breaches involved small business victims.

Furthermore, these attacks are not cheap. The Ponemon Institute and IBM's 2020 Cost of Data Breach Report stated that the average data breach cost $3.86 million in 2020. That is a devastating number for any size organization, let alone a small business.

Research conducted by the National Cyber Security Alliance reveals even more about SMB awareness and preparedness:

28% of surveyed businesses have experienced an official data breach within the past year (this number ranges from 11% for companies with 1-10 employees to as high as 44% for companies with 251-500 employees)

As a direct result of this, 69% have been offline for a limited time, but 37% have experienced a financial loss, a quarter filed for bankruptcy and 10% went out of business

41% of businesses surveyed back up their business data on a daily basis, but only 21% do it multiple times per day, leaving their data ultimately protected from ransomware or other breaches

Despite all the signs, warnings, and very real high-profile breaches, that state of preparedness for most companies when it comes to cybersecurity is rather dim. An Inc.com report gathered data from CEOs of over 1,300 SMBs. More than 60% of the firms didn't have an up-to-date cybersecurity strategy, or worse, or any strategy at all.

The need for better cyber-hygiene is painfully evident.

A survey by Insight’s Cloud + Data Center Transformation team, titled “Cybersecurity at a Crossroads: The Insight 2021 Report,” found that 78% of participants lack confidence in their company’s IT security stance and believe improvements are necessary.

Less than one-third of respondents expressed confidence in their organization’s security roadmap, security-related technology and tools, and internal teams and skill sets. They reported the highest level of trust in their company’s data management strategy, but even then, less than half (45%) voiced confidence in this aspect of security operations.

MSPs and MSSPs can fill this void by providing managed security services that relieve customers of the burden of maintaining and managing the security environment. Managed security now accounts for a substantial portion of the cybersecurity market.

The security services market, specifically managed security services (MSS), has been one of the fastest-growing areas, experiencing double-digit growth rates over five years, and was estimated by the IDC to reach $28B in 2020.

MSPs have a huge opportunity to offer guidance in the current climate, even among customers who have cybersecurity personnel in-house. In fact, 83% of IT leaders with in-house security teams said they are considering outsourcing security tasks to an MSP in 2021, according to Security Boulevard.

Unfortunately, this is still not a widely offered or adopted tool in most security offerings. Why?

THE MYSTERY OF MFA

According to Jason Ingalls, CEO of Louisiana-based MSSP Ingalls Information Security, the disconnect comes down to the user experience. Quite simply, the user doesn't want to have to learn something new.

“There are so many instances that we’ve seen or dealt with where MFA could have prevented a breach. It often comes down to a hesitancy to implement that extra step,” says Ingalls. “This is especially true with executives - they are the worst offenders. But they are the ones targeted by bad actors who are after their credentials to gain access to their emails.”

What people may not realize is that emails provide an extraordinary amount of insight into what is going on in your company. Email is the lifeblood of most organizations.

“If I, a bad actor, get into your email, I can see who you are working on or have strategic deals with, what your plans are, possibly your financials… I would know all kinds of things about your company,” Ingalls continues. “It’s such great intelligence, sort of a window or direct line to your company’s dealings, both internally and externally. People don’t think about this. It’s not just email. Further, it’s a trusted communication mechanism that you own. It’s so easy for hackers to impersonate people these days, recipients often don’t think twice.”

It is clear that some are still not connecting the dots when it comes to how sophisticated cyber-attacks and breaches have become, and what measures the bad guys will go to in order to steal valuable information and data. According to Ingalls, in his experience, some view it as a frivolity, a tedious extra step, without realizing that those two extra strokes could make all the difference.

CASE STUDIES

It is frustrating indeed to hear after a data breach that the violation could have been prevented with multifactor authentication. Here are examples of major security breaches that could have been prevented had the simple solution of multifactor authentication been in place.

Timehop, 2018
Lost 21 million records

Timehop is an application that lets people see past photos and posts from social media. In December 2017, the app was breached, unbeknownst to anyone. The breach wasn't discovered until July 2018, when the hacker used that access to steal personally identifiable data that had recently been added to the system.

"At 2:04 US Eastern Time in the afternoon of the 4th of July 2018, Timehop observed a network intrusion," the company said in a blog post. "The breach occurred because an access credential to our cloud computing environment was compromised. That cloud computing account had not been protected by multifactor authentication."

Names, email addresses, dates of birth, gender, country codes and some phone numbers were made potentially public. Access "tokens," which social media platforms share with the Timehop application to enable it to gain access to the content, were also stolen. This could have allowed a hacker to view customers' social media posts.

After this was revealed, Timehop took security steps — including multifactor authentication — to secure authorization and access controls on all accounts. There have been no reported break-ins since.

Equifax, 2017
Unknown number of records affected

Back in 2017, Equifax experienced a breach that put at least 145 million records at risk of being made public. Before that, there was another breach that put employee records at risk, and at least 750 were used to file false tax returns to the Internal Revenue Service (IRS).

Hackers gained access to a website using default login information based on personal information such as social security numbers and dates of birth. They then had access to employees' W-2 forms to file tax returns in their names to claim a refund.

"Equifax should have known better than to rely on a simple PIN for a password," says Avivah Litan, a fraud analyst with Gartner Inc. "That's so 1990s. It's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN."

Motherboard reported that Equifax was warned about security holes months before the infamous 2017 data breach occurred. In fact, former employees specifically called out a lack of multifactor authentication.

Deloitte, 2017
350 clients affected

Accounting and professional services company Deloitte was another instance where a breach occurred, but wasn't discovered until later. A hacker broke into the firm's global email server through an administrator's account that was gated only by a single password. It is estimated that the breach may have occurred in October or November of 2016, but it wasn't discovered until March of 2017.

The hacker potentially had access to usernames, passwords, IP addresses, architectural diagrams for businesses, health information and as many as five million email messages to and from 244,000 Deloitte employees. Some email messages had attachments with sensitive security and design details. If the administrator's email account had been protected with multifactor authentication, this sensitive material would have been much more difficult to steal.

For each of these scenarios, not having MFA in place was the root cause of the problem. If large enterprises such as these cannot protect against breaches without MFA, it's unreasonable for SMBs to expect their current security measures are enough.

While these are high-profile examples impacting hundreds of millions of users that partners can reference when stressing the importance of MFA to their clients, MSPs should also stress to their SMB clients that dozens of similar breaches are happening at smaller organizations every day. At a time when these data breaches - both minor and massive - are growing in frequency, multifactor authentication may be the last line of defense for both your internal processes and external customers. Otherwise, you risk being a target for a small or large-scale hack.

> ***And make no mistake, if you are a company and you have data, you are a target, no matter your size.***

Security breaches can effectively cripple companies, but there is also the reputation of your brand to consider. It also comes down to trust. If a company suffers a breach of any kind, it can destroy trust and increase the likelihood of customer churn. And let's not forget the loss of revenue.

So what is a modern day security provider to do?

SUCCESSFUL MANAGED SECURITY SERVICE OFFERING

We've established that it often comes down to companies needing, but not necessarily wanting, to proactively implement MFA due to that extra step. Today's connected customers want the seamless and well-rounded multi-channel experience, but also want security and convenience all wrapped up with a bow.

It is a similar balancing act when it comes to employees. Security practices that they consider a hassle can often lead to decreased productivity, which usually means revenue will take a hit. According to a Dell-sponsored survey on the impact of security on business users, "91% said their productivity is negatively impacted by employer security measures."

In order to stay competitive in 2021 and beyond, in terms of both your business and your customers' businesses, MSPs should consider adjusting their offerings and repackaging their services to provide this as-seamless-as-possible experience. MSPs and their end users can benefit from having a single, easy-to-deploy solution that provides comprehensive protection internally and externally.

"From an end user perspective, it's important to emphasize that data is currency," says Frank Corda, business development manager at Tech Data. "If your data is currency, then why do you not want to protect it? The other side to this is that computing where your employees work is no longer inside the office. Especially post-COVID. So now it's somewhere else. Protecting that information is extremely important, so it comes down to the question, 'What is your information worth to you?'

Balancing security with convenience and productivity has always been a daunting hurdle for most companies. But today's authentication solutions have found a way to leap over these obstacles, leveraging contextual factors about users and their devices in near real-time. This ability is disrupting the age-old balancing act, meaning you no longer have to pick and choose.

When presenting your recommended stack to customers, the key is to highlight that while MFA is indeed an extra step, it actually provides a more seamless UX in the long run.

Of course, no security strategy is 100% foolproof. However, MSPs can help manage risk and prevent a threat that could seriously cripple a business, or even put it out of commission completely. Some clients, especially SMBs, may not fully grasp the seriousness of cyber risks. They may think they are not at risk due to their smaller size.

This means that MSPs must put extra effort into making a strong business case for developing a robust cybersecurity strategy. This entails educating customers about the realities of cyber-attacks such as those we've outlined here and offering them a robust, all-encompassing security bundle. Here, again, we must stress making MFA a part of this blended offering.

So, what does that offering look like?

Authentication Protocols

For the sake of this topic, this element comes in at number one. When bad actors attempt to access your business data, authentication solutions stop these unauthorized users in their tracks.

Authentication is a simple and incredibly effective way of preventing breaches, but again, is too often not taken seriously or overlooked completely by companies. Therefore, it is left out of a high number of security policies.

Here's where MFA comes in. Since it requires the use of a secondary device or methods to authenticate a user, it has proven especially useful in preventing breaches. A security solutions offering that includes this is capable of protecting every app or software service you utilize, not to mention aiding companies in meeting ever-shifting compliance standards.

Likewise, automated password management solutions mean that you can ensure your employees are consistently staying up-to-date with strong passwords.

Perimeter Security

These security solutions provide a protective layer around data between a private internal network and an external public-facing network.

Perimeter security has historically been the be-all and end-all of cybersecurity in terms of network protection. Think perimeter firewall solutions. This is most certainly not the case anymore, as these solutions by themselves aren't enough.

Perimeter security still plays an important role in protecting internal data, however. There are several solutions that can achieve this, the most popular of which are unified threat management and a web application firewall.

Unified threat management includes antivirus, firewall, intrusion detection, spam filtering, content filtering and in some cases, VPN support for encrypted communications.

Endpoint Protection

Endpoint protection is important because of the increased prevalence of the cloud and the Internet of Things (IoT), which has caused the number of devices businesses need to protect to shoot up.

Endpoints are everywhere. Think smart TVs, mobile devices, and printers/copiers.

According to Impact Networking, in 2015, there were 15 billion Internet-connected IoT devices worldwide. In 2020, that figure doubled to 30 billion, and by 2025 it will be 75 billion.

To protect your endpoints, businesses should look into domain name system (DNS) protection. Essentially, DNS understands and translates IP addresses rather than human language.

Of course, there are a countless number of malicious sites out there. DNS protection stops access to these, and can be extended to all devices under the network.

According to Cisco, over 90% of attacks are done over DNS and only two-thirds of organizations monitor their DNS records.

There is also managed detection and response (MDR), which is an endpoint protection service that detects, prevents, and responds to attacks across all vectors.

MDR doesn't search for the characteristics of malware, which can be masked or changed to something unrecognizable, MDR monitors every endpoint, recognizes blips and responds to them.

Then there is persistence detection. This type of detection is pointed at a fairly new hacking process, where cybercriminals gain entry into your systems and lie in wait, waiting to strike at the most opportune time.

Persistence detection acts as a drug-sniffing dog, using advanced technology to sniff out would-be attackers by collecting information associated with persistent mechanisms that evade other cybersecurity technologies.

Backup and Disaster Recovery

In case the worst does indeed happen, businesses need to be able to retrieve lost information, and quickly. Backup and disaster recovery (BDR) is a solution that backs up and restores vulnerable information on internal servers, external cloud data, or website data.

BDR is a method that effectively battens down the hatches in the event of a storm, which can be incredibly damaging and costly - particularly to SMBs.

BDR is an essential part of any cybersecurity strategy, but like some of these other elements, is not widely implemented. This, plus software-as-a-service backup (which protects the data within cloud apps) and website backup are vital tools for securing your business in the event of an attack.

Information Security

This element is designed to prevent data leakage and other forms of accidental data loss.

Information security is aimed at stopping inadvertent data loss. Data loss prevention (DLP), for example, prevents data leakage, which is the unauthorized transfer of data from inside your organization to outside. Again, often accidental.

DLP essentially establishes clear standards for your data to prevent this from happening. It designates where certain data should be stored, who has access to it, and where/how it can be shared.

This helps organizations avoid data leakage and all the issues - both large and small - that it can bring to a business.

Email protection, another essential element, operates on the same premise. This comes into play with phishing attempts and spam.

Monitoring

Last but certainly not least, a key component of a well-rounded cybersecurity tech stack is monitoring.

Monitoring tools provide total visibility into your network and find vulnerabilities. These can include scanning for vulnerabilities, security information and event management (SIEM), and network detection and response (NDR).

Vulnerability scanners use machine learning to automatically assess risks. If vulnerabilities are found, they are prioritized depending on threat level and patched immediately.

A SIEM is a monitoring and event management solution that will send out an alert if it recognizes a suspicious login or excessive failed login attempts, for example. And in general, it just recognizes any abnormal behavior in your network.

Network detection and response (NDR) is similar to SIEM, but is more focused on network traffic analysis (NTA). It ferrets out any anomalies and provides more up-close data on any suspicious security events. This gives you total visibility into your network profile.

BOTTOM LINE

These are some of the elements that are vital to what a comprehensive cybersecurity tech stack looks like for a modern business. It cannot be stressed enough that a multi-layered approach to business security is essential to having all your bases covered.

Look at your organization and your clients' organizations inside and out, assess any weaknesses in your security stack, and then build a strategy to address them.

It comes down to this: MFA is easy to implement, is not cost prohibitive (most apps/tools are free) and is that vital second layer between you and the constant barrage of attacks. There are many options out there, one of them being receiving a code via text message or a specialized smartphone app simply called an "authenticator."

Once linked to your accounts, the app displays a constantly rotating set of codes to input when needed. There are also several others, including some from Microsoft and Google, who have free apps for both major mobile platforms. Others such as Twilio Authy, Duo Mobile, and LastPass Authenticator all do the same thing with password management and other features. For more details, read The Best Authenticator Apps for 2021 by PCMag.

In order to protect yourself and your customers, it is now essential to have a well-designed, marketable security stack. An effective security stack incorporates multiple components such as email security, web filtering, sandboxing, endpoint protection and MFA. Once this has been implemented, it is important to annually review your stack, evaluate your vendor relationships and stay abreast of new solutions that are constantly coming on the market in order to provide the best possible protection to your clients.

Tech Data | Security Solutions

For more information or advice on implementing MFA in your own or your clients' environments, please contact the Tech Data security team at securityservices@techdata.com

We're always here to help connect you with the appropriate solutions and sales enablement materials you need to best position your offerings to prospects and customers.