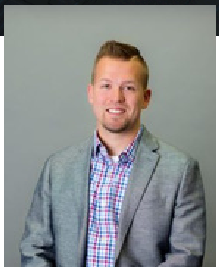
Virtual DataWorks

TECH BYTES

January 2025

Stay up-to-date and protected with our monthly tech and cybersecurity updates. Discover the latest innovations, get valuable tips, and much more!



Keep up with the newest advancements and trends in technology.

Matthew DeWees

-President

Did you know your data could be lurking in the shadows of the internet? Dark web monitoring promises to shine a light on hidden threats, but is it really worth the hype?

There are many cybersecurity tools out there, but dark web monitoring stands out as a hands-free way to protect your identity.

The truth is, what you don't know can hurt you. Your personal information could be up for grabs without you knowing, leaving you open to identity theft, financial fraud, and more.

Want to learn more about dark web monitoring? Reach out to us at everythingit@virtualdataworks.com to schedule a chat.

Until then, stay safe,

Matthew DeWees

President - Virtual DataWorks

WHAT'S INSIDE?

DID YOU KNOW?

Did you know that the term "bug" for a software glitch comes from an actual insect? In 1947, engineers found a moth causing a malfunction in the Harvard Mark II computer.

Virtual DataWorks

475 Wolf Ledges Parkway
Akron, Ohio 44311

virtualdataworks.com

(330) 800-2186

02 WHAT IS THREAT EXPOSURE MANAGEMENT (TEM) AND WHY YOU NEED IT?

Threat Exposure Management (TEM) is an important cybersecurity tool. It helps organizations find and fix weak spots in their digital systems. TEM outsmarts hackers before they break into your network.

Importance of TEM

Cyber attacks keep getting worse. Hackers always find new ways to break in. TEM helps businesses spot problems before they become big issues.

TEM allows you to:

- Find weak points in your network
- Fix issues quickly
- Reduce your risk of cyber attacks

How TEM Works

TEM uses special software to scan your entire network. It finds places hackers could attack and helps you fix these weak spots.

Continuous Monitoring

TEM keeps looking all the time. This way, you can find new problems as soon as they appear.

Risk Assessment

TEM finds which weak spots are the most dangerous. This helps you fix the most important ones first.

Main Parts of a TEM Program

Asset Discovery

This finds all devices and software on your network. You can't protect what you don't know about!

Vulnerability Scanning

This looks for open weak spots in your system. It's like checking for unlocked doors in your house.

Threat Intelligence

This provides insights into new hacker techniques, helping you stay informed about what to watch out for.

Remediation Planning

Once you find the vulnerabilities, you need a plan to fix them. TEM helps you make good choices on how to patch these spots.

Benefits of TEM for Your Business

Better Security

Finding and fixing weak spots makes your whole system much safer and more resilient.

Cost Savings

Stopping an attack before it happens can save you a lot of money. Dealing with the aftermaths of cyberattacks often comes with expensive costs.

Peace of Mind

With TEM, continuous monitoring ensures your system is always under watch. This can help you worry less about cyber attacks.

What to Look for in a TEM Solution

A good TEM tool should:

- Be user-friendly, ensuring that all team members, regardless of their technical expertise, can easily navigate and utilize the tool.
- Provide immediate results, enabling quick and effective decision-making to address potential threats as soon as they are detected.
- Integrate seamlessly with your existing security infrastructure, enhancing overall protection by working in harmony with other security tools and systems.
- Generate clear and comprehensible reports, presenting findings in an easily digestible format that facilitates understanding and action by all stakeholders.

Getting Started with TEM

- Check your current security setup to understand your existing vulnerabilities and areas for improvement.
- Find a TEM tool that fits your needs, ensuring it aligns with your security goals and integrates well with your current systems.
- Set up the tool and start scanning your environment.
- Make a plan to fix the weak spots you find, prioritizing the most critical issues.
- Keep scanning and improve your security continuously, regularly updating your strategies and tools to stay ahead of emerging threats.

Want to learn more about how TEM can help your company? Contact us today for help staying safe in the digital world.

Next-Gen Cybersecurity: Secure Your Digital Horizon

With Virtual DataWorks as your Managed Services Provider, you can leverage your technology through a customized program that allows us to:

- Monitor and maintain every device on your network.
- Have a team of technicians watching your network's every move.
- Give your employees access to our help desk. We are available 24/7.

FIND OUT NOW

03

DO YOU REALLY NEED DARK WEB MONITORING?

The dark web is a hidden part of the internet. You can't find it with Google. You need special software to access it.
Criminals use the dark web for many bad things. If your data ends up there, you should be the first to know.
This is where dark web monitoring services come in.

Why Is Dark Web Monitoring Important?

Dark web monitoring looks for your information on the dark web. It can find stolen passwords or credit card numbers. This helps you know if someone stole your data.

It Protects Your Identity

Thieves might sell your information on the dark web. Monitoring can catch this early. You can then change passwords and protect yourself.

It Helps Businesses
Businesses use dark web monitoring too. It shows them if someone hacked their data. They can act quickly to stop more damage.

How Does Dark Web Monitoring Work?

Dark web monitoring uses special tools. These tools search the dark web in real time. They look for specific information, like email addresses or credit card numbers.

It Uses AI
Many monitoring tools use artificial intelligence. AI helps them search faster and better. It can spot patterns that people might miss.

It Sends Alerts
The tools send an alert when they find your information. This tells you right away if someone stole your data.

What Can Dark Web Monitoring Find?
Dark web monitoring can find many things:
- Passwords
- Credit Card Numbers
- Social Security Numbers

Is Dark Web Monitoring Enough?

Dark web monitoring is important, but it has limits. You still need to be careful online.

Here are other things you can do:

- Use Strong Passwords: Make long, hard-to-guess passwords. Use different ones for each account.

- Be Careful What You Share: Don't put too much personal info online. Be careful on social media.

- Keep Software Updated: Always update your computer and phone. This helps keep hackers out.

How Can You Get Dark Web Monitoring?

You can get dark web monitoring in many ways:
- Free Options: Some banks offer it for free. Check with your bank or credit card company.

- Paid Services: Some companies focus just on dark web monitoring. They often have more features than free options.

How Often Should You Check Dark Web Monitoring?

Check your dark web monitoring often. Once a week is good.

If your info shows up on the dark web, don't panic. Do these things:

1. Change Passwords: Change the password for any account that was found. Use a new, strong password.
2. Check Your Accounts: Look at your bank and credit card statements. Make sure nothing looks wrong.
3. Freeze Your Credit: This makes it harder for someone to open accounts in your name.

Is Dark Web Monitoring Worth It?

Dark web monitoring is very useful. It tells you when someone steals your information. You can then act fast to protect yourself.

Dark web monitoring is an easy way to protect your information. It watches when you can't. If you want to stay safe online, it's a good tool to have.

04

HOW PASSWORD MANAGERS PROTECT YOUR ACCOUNTS

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

You only need to remember one password, the master password. This master password lets you access all your other passwords.

Types of Password Managers

- Apps you download on your phone or computer
- Tools that work in your web browser
- Some offer both options

Why Use a Password Manager?

- It Helps You Create Strong Passwords. Password managers generate long, random passwords that are hard to crack.
- It Remembers Your Passwords. With a password manager, you don't need to memorize many passwords. The tool does this for you.
- It Keeps Your Passwords Safe. Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

- Password Generation: Good password managers can create tough, unique passwords for you.
- Auto-Fill: Many password managers can fill in your login information on websites. This saves time and avoids typos.
- Secure Notes: Some password managers let you store credit card numbers or important documents.
- Password Sharing: Some tools let you share passwords safely with family or coworkers.

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Make sure it works on all your devices.
- Research the features you want and the price you can afford.

Consider using a password manager today to improve your online security. If you need help choosing or setting up a password manager, contact us today.

05

INNOVATIVE SOLUTIONS TO IOT DEVICE SECURITY

The Internet of Things is growing day by day. More devices are connecting to the internet. And with that growth comes new security risks.

Here are some new ways to keep your IoT devices safe.

1. Use Strong Passwords: Always change the default passwords on your devices to strong, unique ones.
2. Regular Software Updates: Keep your device software up to date. Manufacturers release updates to patch security vulnerabilities, so regular updates are crucial for maintaining security.
3. Data Encryption: Encrypt your data to ensure that even if it is intercepted, it cannot be read by unauthorized parties.
4. Develop an IoT Security Policy: Establish a comprehensive security policy for the use and management of IoT devices.
5. Network Segmentation: Implement network segmentation to isolate IoT devices from other parts of your network.
6. Research Before Buying: Before purchasing IoT devices, research the manufacturers' security practices.
7. Secure Your Home Network: Enable network encryption, such as WPA3 for Wi-Fi, to protect your home network from unauthorized access.
8. Be Selective About Connections: Only connect devices that you truly need. Each connected device is a potential entry point for attackers, so minimizing the number of connected devices can reduce your risk.

- **Improve your passwords.**
Think of passwords as the keys to your online home. Use strong, unique passwords for each account to prevent unauthorized access.

- **Update your software.**
Keeping your software up to date is like getting a flu shot. Regular updates patch security vulnerabilities and protect your devices from new threats.

- **Implement two factor authentication.**
It's like putting two locks on your door.

- **Be careful on public Wi-Fi.**
It's like yelling in a crowded place.

- **Identify phishing scams.**
Phishing scams are like fake fishermen trying to catch you. Be cautious of suspicious emails or messages asking for personal information, and verify the sender's identity before responding.

- **Back up your data.**
It's like making copies of your important papers.

- **Review privacy settings.**
Your privacy settings are like curtains on your windows.

- **Teach your family about cybersecurity.**
Cybersecurity is important for everyone in your family. Educate them about safe online practices, just like teaching kids to look both ways before crossing the street.

By following these tips, you can significantly improve your cybersecurity and protect your personal information from potential threats.

READ MORE

Virtual DataWorks

Unlock Exclusive Knowledge Today!

Sign up now to **gain access** to our latest security emails, tailored just for you. Don't miss out on cyber security tips, and insights that can help elevate and protect your business.