# How to Protect Your Data from Unauthorized Access

June 15, 2020 By Cypress Data Defense In Technical

Data protection is one of the primary concerns of organizations around the world today. Information security (InfoSec), which is primarily about prohibiting unauthorized access to information, is what makes data protection possible.

By 2020, security services such as security information and event management (SIEM) and other managed services are estimated to account for nearly 50% of cyber security budgets. This implies that enterprises are increasingly prioritizing cyber security and implementing better and more robust security practices to prevent unauthorized access by attackers or malicious insiders.

Is your data secure enough to prevent unauthorized access? In this article, let's take a look at what you can do to boost your security.

## Prevent Unauthorized Data Access: 9 Tips to Help You Boost Your Cybersecurity

There are several high-level security best practices that every enterprise should adopt to protect their data from unauthorized access. Here are our recommendations to help you prevent unauthorized data access:

### 1. Keep Current on all Security Patches

The first step for any organization to prevent unauthorized data access is to keep current on all the security patches.

Here's why:

Security patches address vulnerabilities in software, operating systems, drivers, etc., that attackers might use to gain access to your

CATEGORIES

Technical

Podcasts

Podcast Clips

Education & training

META

Login

ARCHIVES

September 2020

August 2020

July 2020

June 2020

May 2020

April 2020

March 2020

October 2019

September 2019

May 2019

March 2018

The WannaCry virus that took down more than 400,000 computer systems across 150 countries was one of the most severe attacks in recent years. It attacked the vulnerability in the SMB V1 (Server Message Block) protocol of Windows and was launched by using the EternalBlue exploit.

What's interesting is that security patches for these vulnerabilities were available long before the attack was launched. But there were thousands of users who had not updated their security patches and thus, became victims of the attack.

With the use of updated security patches, users could have prevented giving unauthorized access for the system attacks.

It is important to ensure that you download the latest security patches and updates for your operating systems and other software to protect it against cyberattacks. You can also enable automatic updates so that whenever a security patch or update is released, the system automatically installs it.

By staying prepared and updated, you can protect your data from those trying to get unauthorized access to it.

## 2. Detect and Respond to Intrusions Quickly

Of course, you'd want to stay vigilant and be prepared to prevent hackers from unauthorized data access.

But what if you couldn't detect an intrusion?

What's the way forward?

The earlier you detect an intrusion, the earlier you can respond to it. Prevention is undoubtedly important, but monitoring user activity, login attempts, logs, and other activities can also provide insights into how secure your system is.

There are several ways you can detect and respond to intrusions quickly:

**IDS/IPS (Intrusion Detection System/Intrusion Prevention System)**

policies.

On the other hand, an IPS complements an IDS by proactively monitoring a system's incoming traffic to identify malicious requests. An IPS prevents intrusion attacks by blocking unauthorized or offending IPs, prohibiting malicious data, and alerting security personnel to potential security threats.

**SIEM (Security Incident Event Manager)**

A Security Incident Event Manager, or SIEM, is a security management approach that enables security professionals to get insights into the activities within an IT environment. SIEM software collects and analyzes log data generated by the company's technology infrastructure, from applications, host systems, networks, to security devices.

The software then detects and categorizes events and incidents, as well as analyzes them. Primarily, there are two main objectives of SIEM:

- Track records and provide reports on security-related events and incidents, such as failed and successful login attempts, malware activity or any other suspicious activity.
- Notify security personnel if any suspicious activity is detected that indicates a security threat.

**Implement User and Event Behavioral Analytics (UEBA)**

To prevent unauthorized data access, you need to be on top of your analytics game.

User and event behavioral analytics helps detect any anomalous behavior or instances if there are deviations from a users' "normal" behavioral patterns. For instance, if a user regularly downloads files of 10MB size every day but suddenly downloads gigabytes of files, the system would detect this anomaly and alert the administrator immediately.

Such analytics focuses on users and entities within your system, especially insider threats like employees who could misuse their privileges to carry out targeted attacks or fraud attempts.

## 3. Implement Principle of Least Privilege (Minimize Data Access)

Least privilege is the practice of restricting access rights for accounts, users, and computing processes to only those specific resources required to perform legitimate, routine activities. The 2019 Global Data Risk Report says that, on average, an employee has access to 17 million files.

Implementing least privilege can help you secure your data from providing unauthorized access. The principle of least privilege (POLP) enforces a minimal level of user rights which allows the user to access specific resources needed only to perform his/her role. It reduces the risk of exploitation by unauthorized users, applications, or systems without impacting the overall productivity of the organization.

While least privilege helps provide authority for only specific resources required to complete the job at hand, it also enforces better security practices and reduces the likelihood of your organization becoming a victim to a cyber attack.

## 4. Use Multi-Factor Authentication

It is essential for companies to use strong authentication by implementing robust password policies in addition to multi-factor authentication. That can go a long way in preventing unauthorized data access.

As the name suggests, multi-factor authentication requires multiple pieces of information to be presented by the user and validated by the system before they are granted access to the system. This makes it difficult for attackers to compromise users' accounts as it takes more effort than simply cracking the password.

compromise the second factor as well. This makes breaking authentication much more difficult for the attacker.

Want a pro tip to prevent unauthorized access to your data?

Leverage passphrases.

While multifactor authentication should definitely be used, you can also move towards the use of passphrases instead of passwords. A passphrase is a series of random words or a sentence that can also contain spaces in between words such as, “Ten herds of elephants bowl frequently in Tanzania!!”

A passphrase doesn’t have to be grammatically correct; it can be any combination of random words and also contain symbols. It can be easier to remember a complex passphrase than a complex password. Care must still be taken to generate strong passphrases. Simple passphrases that use only everyday vocabulary words may still be easily cracked.

## 5. Implement IP Whitelisting

Another way to prevent unauthorized data access is through IP whitelisting.

IP whitelisting helps limit and control access to only trusted users. It allows you to create a list of trusted and authorized IP addresses from which users can access your network. Typically a company uses the internet via a defined set of IP addresses, so they can add a list of all the trusted IP addresses that are allowed access.

By whitelisting IP addresses, you can grant permission to only trusted users within a specific IP address range to access specific network resources such as URLs, applications, emails, or more.

If someone with an untrusted IP address tries to access your network, they will be denied access. IP whitelisting also enables organizations to secure remote access to the network including Bring Your Own Device (BYOD) that allows employees to use their own devices.

However, network traffic in server-to-server communications and inside data centers is often not encrypted. If an attacker gains access to such a network, they could intercept data in transit between servers in a multi-machine cluster.

To prevent attackers from snooping on data with unauthorized access, organizations are increasingly monitoring their own network traffic to detect intrusions. Companies might store copies of network traffic for long periods of time in their monitoring systems.

It's crucial for all networks to use encryption if they store privacy-protected data. This applies to both the connections made by authorized users from outside the data center to access the system and network links between nodes in a multi-server system.

You can use a VPN layer between the users and the system or implement an SSL/TLS to encrypt network traffic. Inside the system, communications can be secured using IPsec, SSL/TLS, or some other VPN technology.

## 7. Encrypt Data-at-Rest

Encryption of data at rest ensures that data is stored securely and not as plain text. As data is written to the disk, it is encrypted via a set of secret keys which is known only to authorized administrators of the system.

The access to these secret keys is limited and controlled to ensure that only privileged users can access the encrypted data and use it. This technique safeguards the data from attackers who might attempt to gain remote access to the system and protect the data from being compromised.

It's an effective way of shielding your data from anyone trying to get unauthorized access. Encryption-at-rest requires proper auditing of all places where data might be stored, such as caching servers or temporary storage devices.

## 8. Ensure Anti-Malware Protection/Application Whitelisting

without the user's consent or authorized access. Trojan horses, computer viruses, worms, scareware, and spyware are some of the most common types of malware attacks. They can be present on emails and websites, or hidden in attachments, videos, and photos.

Such malware can give hackers unauthorized data access easily.

Anti-malware protection is very important as it builds the foundation of security for your devices. Run good antivirus programs, avoid clicking on suspicious emails or downloading attachments from an unknown source, and do regular scans for spyware.

Alternatively, a stronger control is to utilize application whitelisting. It can be very effective in preventing unauthorized data access.

Doing this, you identify the known and trusted applications that are allowed to run on your computer systems and reject all others. Even if someone gets unauthorized access, they won't be able to run the malware on your systems if the application has not already been approved as a whitelisted application.

### 9. Track and Manage Your Risks

A risk could be anything that potentially impacts your project's performance, budget, or timeline. If these risks become substantial, they become vulnerabilities that must be addressed to avoid cybersecurity attacks.

It is critical that organizations identify, categorize, prioritize, and mitigate risks in an effective and timely manner. By tracking risks before they escalate, you can prevent them from becoming issues. Additionally, you should develop a response plan to tackle risks immediately.

## Final Thoughts

Data protection isn't a linear process or a one-time activity. You need to continuously invest resources, time, and effort into ensuring security from unauthorized data access.

that each and every employee makes cybersecurity a top priority.

If you want to run a quick security audit on your existing security practices, let us know and we'll help you ensure that you are well-protected from unauthorized data access and other cyber threats.

## ABOUT

Cypress Data Defense was founded in 2013 and is headquartered in Denver, Colorado with offices across the United States. Our goal is to help organizations secure their IT development and operations using a pragmatic, risk-based approach. The diverse background of our founders allows us to apply security controls to governance, networks, and applications across the enterprise.

Learn More

Share page on:

## LATEST POSTS

How to Integrate Security Into a DevOps Cycle

However, DevOps processes aren't restricted to...

Secure SDLC and Best Practices for Outsourcing

A secure software development life cycle (SDLC...

10 Best Practices for Application Security in the Cloud

According to Gartner, the global cloud market will...

## CONTACT

Cypress Data Defense
14143 Denver West Pkwy
Suite 100
Golden, CO 80401

PH: 720.588.8133

Email: info@cypressdatadefens

## SOCIAL



Privacy Policy