SOFTPROM

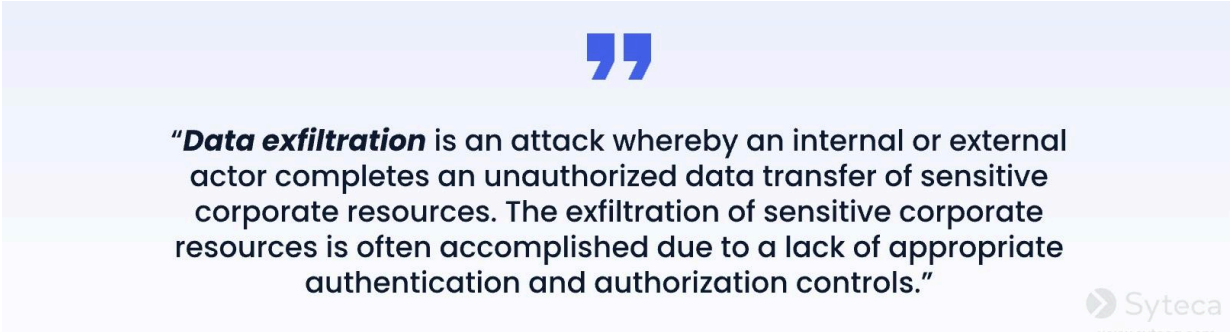
Syteca
formerly Ekran System

Data Exfiltration in Cybersecurity: What It Is, Examples, and Prevention Tips

Data security is vital to your organization's well-being. A single data breach costs $4.88 million on average, according to IMB's Cost of a Data Breach Report 2024. Besides financial losses, data exfiltration may damage a brand's reputation, cause operational disruptions, and result in legal actions. Therefore, giving maximum attention to your cybersecurity measures and constantly enhancing them is a must. In this article, we explain the meaning of data exfiltration and the malicious tactics behind it. We'll also explore recent real-life examples of data exfiltration and offer ten best practices for protecting your data.

What is data exfiltration in cybersecurity?

Data exfiltration is a type of security breach characterized by the unauthorized transfer of data from an organization's systems or devices to an external location. It is also referred to as data theft, data exportation, data leakage, or data extrusion.



Definition of data exfiltration in cybersecurity by Microsoft.
Malicious actors can exfiltrate data through digital transfer, the theft of physical documents or corporate devices, or an automated process as part of a targeted attack on sensitive data.

What data is at risk?

Any information that provides financial, strategic, or operational value is at risk of being exfiltrated. Attackers often target the following types of data:

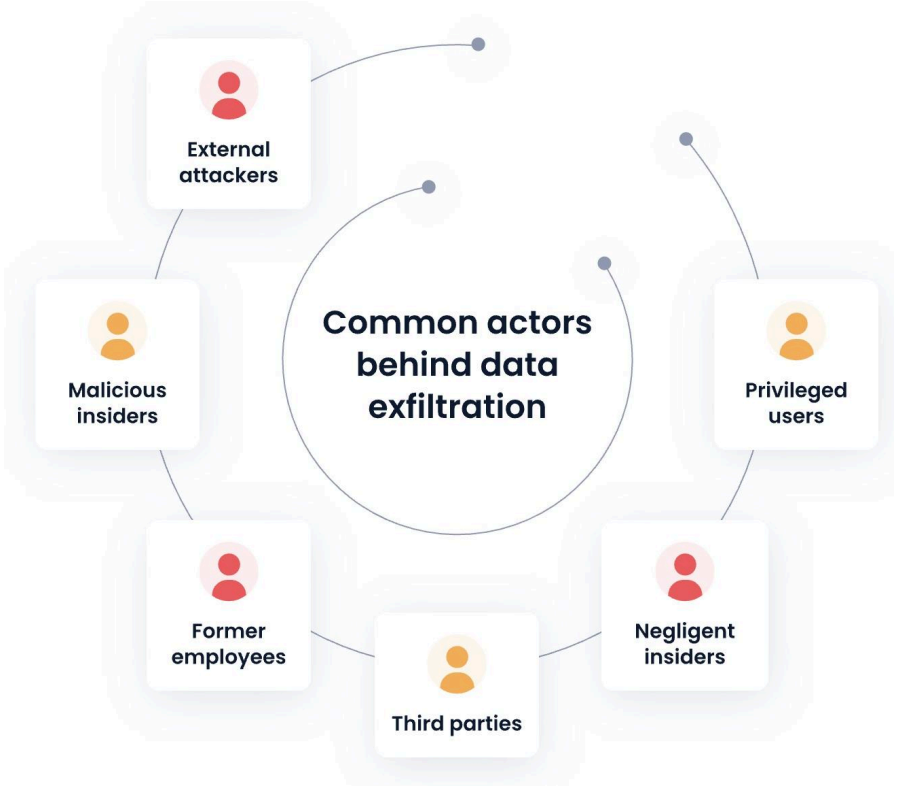
What are the consequences?

Potential consequences of data exfiltration depend on the attacker's goals. Attackers might demand a ransom payment to return stolen data to the organization, sell it to a company's competitor or on the dark web, or use the data to get revenge on a former employer.

To better understand the data exfiltration meaning, we'll now explore some examples.

Where do data exfiltration threats come from?

Malicious actors can exfiltrate data in various ways. First, let's look at some of the most common actors behind the exfiltration of data. Who can potentially exfiltrate data? Data exfiltration can occur due to either external or internal threats. The most common actors behind data exfiltration are:

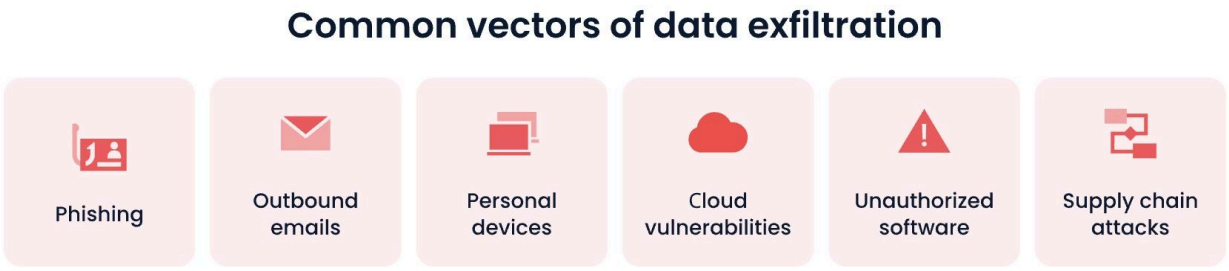


Cybercriminals or employees may carry out data exfiltration schemes, trying to gain access to an organization's assets and data with malicious intent. Former employees can also be a threat if they still have access to their accounts or if they create backdoor accounts before their departure. Third-party vendors with access to your organization's networks and systems can also exfiltrate data. A special category of insiders worth mentioning is users with elevated access rights. Privileged users often have full and permanent access to protected data, applications, and systems and thus pose additional security risks. In addition to malicious insiders, regular users can accidentally expose sensitive data by neglecting corporate data security policies. As a matter of fact, even external attacks are frequently made possible by negligent insiders. That's why people-centric security is vital for protection against data exfiltration.

In the next section, we'll review the most common methods of data exfiltration to help you better understand what areas of your organization's cybersecurity need improvement.

What are the common data exfiltration vectors?

The most commonly used data exfiltration techniques, sources, and vectors include:



Phishing

Email is still one of the major data exfiltration channels used by cybercriminals to distribute malware and perform phishing attacks. Phishing usually involves sending an email to deceive recipients into revealing sensitive information or downloading an infected attachment. As perpetrators claim to be sending their emails from a trusted source, those targeted can't always distinguish a potentially dangerous email from a legitimate one.

Outbound emails
A user can easily forward an email with sensitive data to a personal account. For instance, a negligent employee might email corporate data to a third-party supplier. Malicious insiders may willfully move information outside the organization's perimeter as a file attachment or a text message.

Personal devices
Employees may copy corporate data to flash drives, smartphones, cameras, and other external drives. From there, attackers can hack the unprotected devices and exfiltrate data. A user can also intentionally steal data using personal storage devices. In remote work and hybrid office environments, employees may expose data through home computers and network vulnerabilities.

Cloud vulnerabilities
Data stored in cloud-based environments can be susceptible to exfiltration too, especially if employees violate basic cybersecurity practices. Malicious actors can exfiltrate data from corporate cloud drives if they're poorly protected or misconfigured. Another concern is when a user uploads data to their cloud storage and provides extensive access permissions to it, exposing data to unauthorized parties.

Unauthorized software
Installing unauthorized software on corporate devices poses a severe risk to an organization's cybersecurity. Employees may either intentionally or inadvertently download unlicensed products containing malware or ransomware that transfers data to an external system without the user's knowledge. Another way malware can infect corporate devices and networks is through shady websites visited by naive employees using company computers.

Supply chain attacks
Your partners, suppliers, and other third parties with access to your organization's infrastructure are a source of supply chain cybersecurity risks. In a supply chain attack, cybercriminals may infiltrate one of your suppliers and escalate the attack to access your organization's data.

Let’s now look at several examples of real-life data exfiltration attacks.

Data exfiltration attack examples

To see how data exfiltration happens in real life and grasp the possible consequences, let’s examine three data exfiltration attacks that took place in 2024:

Case #1: Halliburton RansomHub ransomware attack

Affected entity	**Halliburton, the leading global oil service company**
What happened	**Ransomware attack**
Method of access	• **Direct losses totaling $35 million** • **Operational disruptions** • **$0.02 per share impact on adjusted earnings, attributed to lost or delayed revenue** • **Potential financial liabilities and reputational damage.**

On August 21, 2024, Halliburton discovered unauthorized access to its systems, which was later attributed to the RansomHub ransomware group. The attackers exploited vulnerabilities within the company’s IT infrastructure, allowing them to infiltrate the network and exfiltrate sensitive data. The exact nature and scope of this data remain under investigation.

Case #2: US telecommunications cyberespionage campaign

Affected entity	**US telecom companies, including major providers such as AT&T, Verizon, T-Mobile, and Lumen Technologies**
What happened	**Espionage attack**
Method of access	• **Compromise of call record metadata: details about who called whom, the duration of calls, and timestamps** • **Leakage of data gathered via lawful wiretaps** • **Potential for foreign interference in US domestic politics.**

In November 2024, US federal investigators uncovered a significant cyber-espionage campaign led by a Chinese state-sponsored group, Salt Typhoon. This operation targeted multiple US telecommunications providers and resulted in unauthorized access to sensitive data.

The attackers accessed and exfiltrated phone call logs and potentially live call audio. The breach primarily impacted individuals involved in government and political activities, including senior officials and prominent political figures such as Donald Trump.

Case #3: Western Sydney University data breach

Affected entity	**Western Sydney University**
What happened	**Unauthorized access to the internal systems**
Method of access	• **Compromise of around 7,500 individuals' personally identifiable information** • **580 terabytes of data exposed.**

In May 2024, Western Sydney University reported a significant data breach involving malicious access to its Microsoft Office 365 and Isilon environments. The intruders accessed email accounts and SharePoint files with approximately 580 terabytes of student and personnel data. The exfiltrated data included names, contact details, dates of birth, health records, government identification documents, tax file numbers, superannuation details, and bank account information.
The unauthorized access reportedly began as early as May 17, 2023, but it was not discovered until January 2024. Although no immediate threats or demands for ransom were reported, WSU took proactive steps to notify the affected individuals.

These examples show that data exfiltration can happen to any organization, and even detecting such an incident can take a reasonably long time. Read on to learn the top best practices for minimizing your data security risks and preventing data exfiltration.

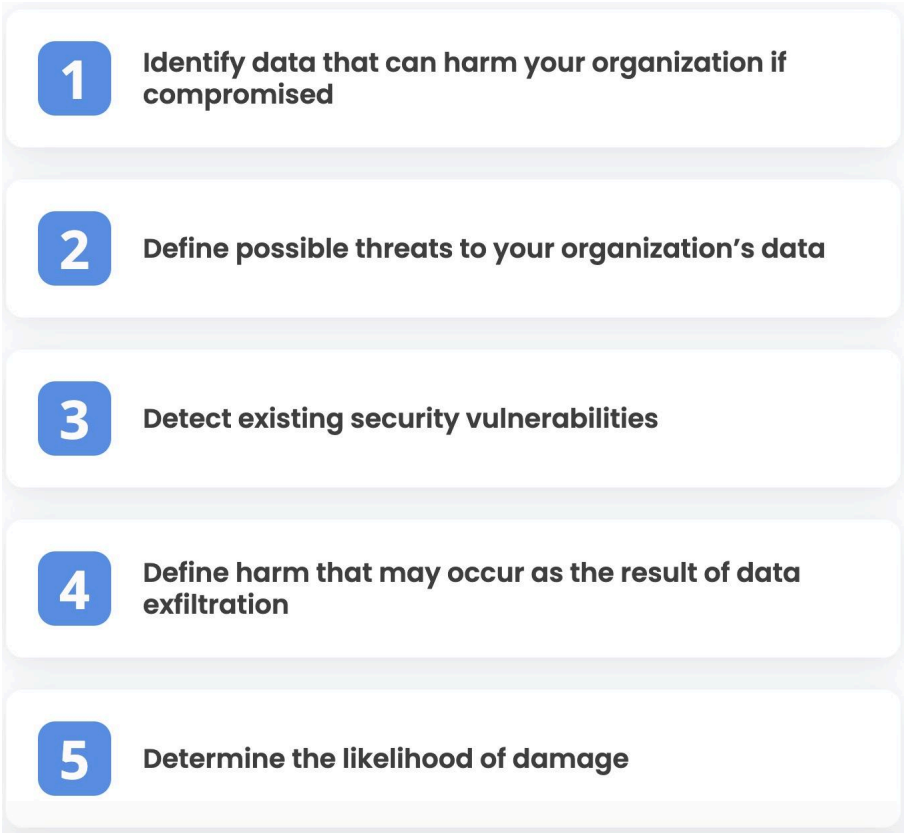
10 best practices to prevent data exfiltration

Preventing data exfiltration requires a holistic approach that includes reviewing your security measures, implementing an insider threat program, and educating employees. To get you started, we've gathered ten best practices to enhance your organization's cybersecurity and help you reduce the chances of data exfiltration.

1. Assess risks to your organization's data

To efficiently handle data exfiltration, you need to know what threats to expect and how to mitigate security risks before they become issues. Consider employing the following practices as part of your risk assessment:

Key steps of a data security risk assessment



A risk assessment helps you identify potential threats, prioritize risks, and evaluate how well your cybersecurity measures could mitigate those threats. With the results of your risk assessment, you can determine whether you need to implement any additional cybersecurity practices.

2. Implement information security policies

Once you know the risks to your data, it's time to reflect them in your information security policies (ISPs). ISPs can help you fight data exfiltration by directing and synchronizing your organization's data protection efforts. Pay particular attention to the following types of ISPs:

- Data management policy
- Network security policy
- Access control policy
- Vendor management policy
- Removable media policy

You may be able to create a single centralized information security policy containing all aspects of organizational security; however, take into account that you might need to develop multiple ISPs in order to fully secure all sensitive data.

3. Secure your data management

How you manage sensitive data is crucial to your information security. Document your data management processes, paying attention to how data is collected, stored, processed, and deleted, as well as who can access it and any other relevant information.

It's also critical to define your organization's data protection measures. Gartner offers four key data security methods you can use to protect your information from exfiltration:

4. Implement an insider threat program

Malicious insiders are hard to detect as they actually have authorized access, making it difficult to differentiate their regular job-related activities from mal-intended ones. Additionally, insiders know your network and the location of sensitive data. Insider threats are not only about malicious employees, as many external attacks are successful due to negligent workers and third parties putting

your data at risk. An insider threat program can help you manage all of these risks by coordinating measures for detecting and preventing insider threats. When creating the program, make sure to get support from your organization's key stakeholders. Further, assigning a specialized insider threat response team and deploying dedicated data exfiltration prevention tools will be of great help.

5. Implement the just-in-time approach to access management

Ensure that privileged access to specific systems and resources is provided only to users with a valid reason and only for the amount of time deemed necessary. With the just-in-time privileged access management (JIT PAM) approach, you can minimize the risks of data exfiltration and implement the principle of least privilege, with zero standing privileges as the goal. You can also systematically conduct user access reviews for current and former employees.

When managing access within your organization, it's a good idea to implement access control models, such as discretionary access control (DAC) and mandatory access control (MAC). We have a detailed article on this topic to help you understand the difference between DAC and MAC.

6. Monitor user activity

Data exfiltration monitoring requires you to track user activity to make sure users access and handle data securely. Monitoring user activity can help your organization proactively detect and respond to potential data exfiltration attempts, whether initiated by insiders or external threat actors. In the event of a data breach or suspected exfiltration, monitoring user activity provides valuable evidence for investigation and forensic analysis. Detailed records of user actions can help you reconstruct the sequence of events, identify the source of the breach, and support your incident response efforts.

Apart from monitoring regular employees, it's essential to keep an eye on third parties with access to your infrastructure and users with elevated access rights. Privileged users have access to the most sensitive parts of the corporate network and thus have more opportunities to exfiltrate data while remaining unnoticed. It is imperative that you keep a close eye on these users and their actions.

7. Leverage user and entity behavior analytics

Security user behavior analytics, or user and entity behavior analytics (UEBA) solutions are based on artificial intelligence algorithms. UEBA technology works by analyzing users' behavioral patterns and defining a baseline of normal and expected behavior. User actions that deviate from this baseline are considered potential risks and need to be examined by security officers.

UEBA tools usually need some time to track and analyze user activity to identify typical user behavior. Once this process is finished, UEBA will supplement your data exfiltration prevention efforts, helping you automatically detect data breaches in their early stages.

8. Develop a culture of cybersecurity awareness

Data exfiltration often results from phishing, transferring data to insecure devices, and account exploits caused by employees' poor password habits. To minimize the risks of such incidents, you should systematically educate your staff and update your security policies regularly. Implementing a people-centric security approach makes your employees the most important level of your security perimeter.

By consistently emphasizing the importance of cybersecurity and providing employees with the knowledge, resources, and support they need, you can nurture a culture of cybersecurity awareness inside your organization. Thus, you'll cultivate a sense of collective responsibility for data protection and empower your employees to actively contribute to the organization's overall security posture.

9. Ensure a quick incident response

Organizations often only become aware of data leaks when they notice missing data or discover that their data was sold to someone. And the longer a data breach goes unnoticed, the more damage an attacker can cause. Many organizations may not know about an incident for months. It takes 281 days on average to identify and contain a data breach, according to the Cost of a Data Breach Report 2024 by IBM Security.

Therefore, prompt data exfiltration incident response times are vital to protecting your data and ensuring your business continuity. Implementing dedicated incident detection and response solutions can help you detect data breaches early. You may

also consider creating an incident response plan that provides your cybersecurity team with clear scenarios for acting in urgent situations:

10. Manage your supply chain risks

Supply chain security is an ever-growing concern of cybersecurity experts that affects an organization's data security. According to the 2023 Software Supply Chain Attack Report [PDF] by Cybersecurity Ventures, the global cost of software supply chain attacks on organizations will reach nearly $138 billion by 2031.

Supply chain risk management goes beyond mere third-party risk management and requires employing a holistic cyber supply chain risk management (C-SCRM) strategy. C-SCRM involves assessing all cybersecurity risks that may come from your supply chain, taking measures to protect your data from vendors, and collaborating with suppliers to improve their security.

How to prevent data exfiltration with Syteca

Syteca is a comprehensive cybersecurity platform that helps you secure sensitive data and combat insider threats.

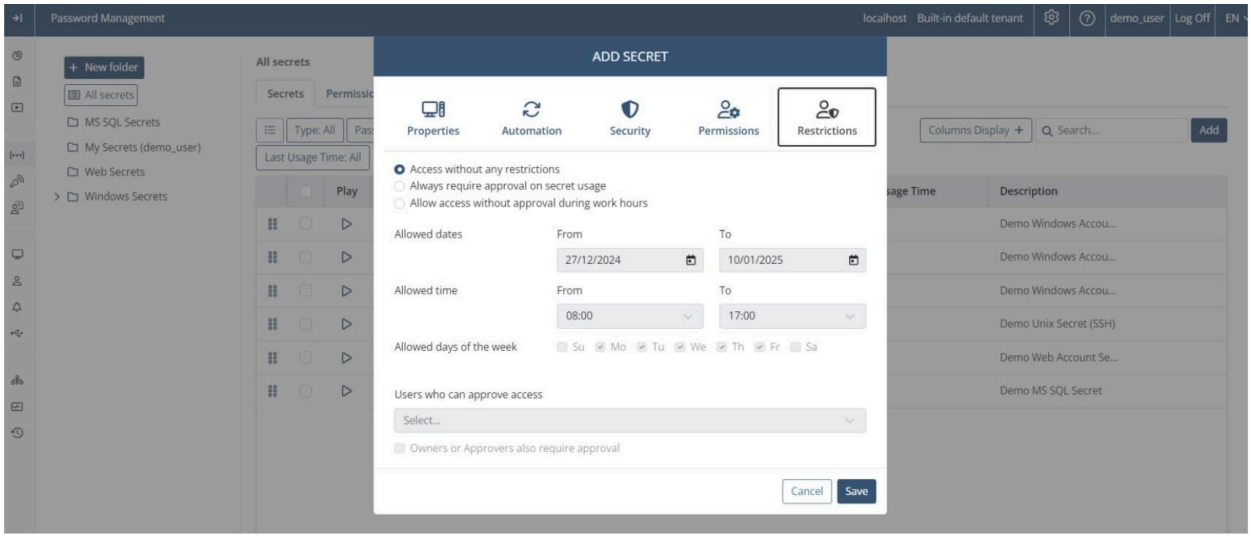
With an extensive set of user activity monitoring (UAM) and privileged access management (PAM) features, Syteca can help your organization establish a proactive and multi-layered approach to preventing data exfiltration. Syteca enables you to secure access to data, detect suspicious activity in real time, and quickly disrupt ongoing exfiltration attempts.

Manage identities and control access

By managing access privileges and verifying user identities, you will be able to secure data from unauthorized access and reduce the risks of account compromise.

Syteca offers the following access management features:

- Account discovery to reveal and onboard backdoor or unmanaged privileged accounts.
- Privileged access management (PAM) to granularly control access permissions for all privileged and regular users in your IT infrastructure.
- Two-factor authentication (2FA) to confirm user identities and secure user accounts.
- Password management to create access request and approval workflows, deliver temporary credentials, automate password rotation, and more.

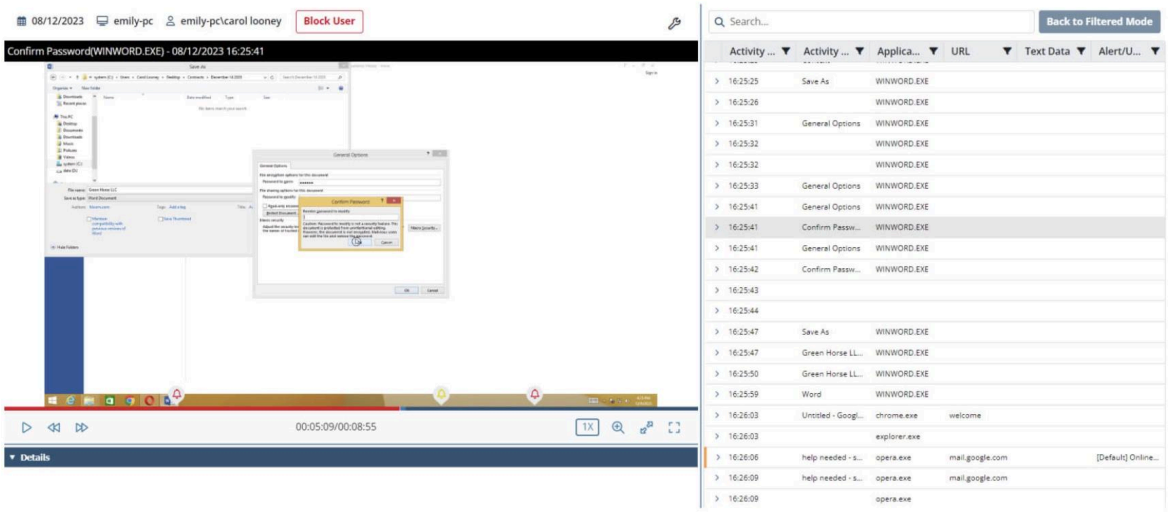


Monitor user activity

To detect security threats originating inside your organization, your security officers need the ability to oversee all activity within your IT infrastructure. Syteca provides the following user activity tracking capabilities:

- User activity monitoring (UAM) for real-time visibility into what employees, privileged users, and third-party vendors do inside your organization’s systems.
- Screen captures and metadata recording to create a detailed audit trail for your security officers and forensic investigators to analyze.

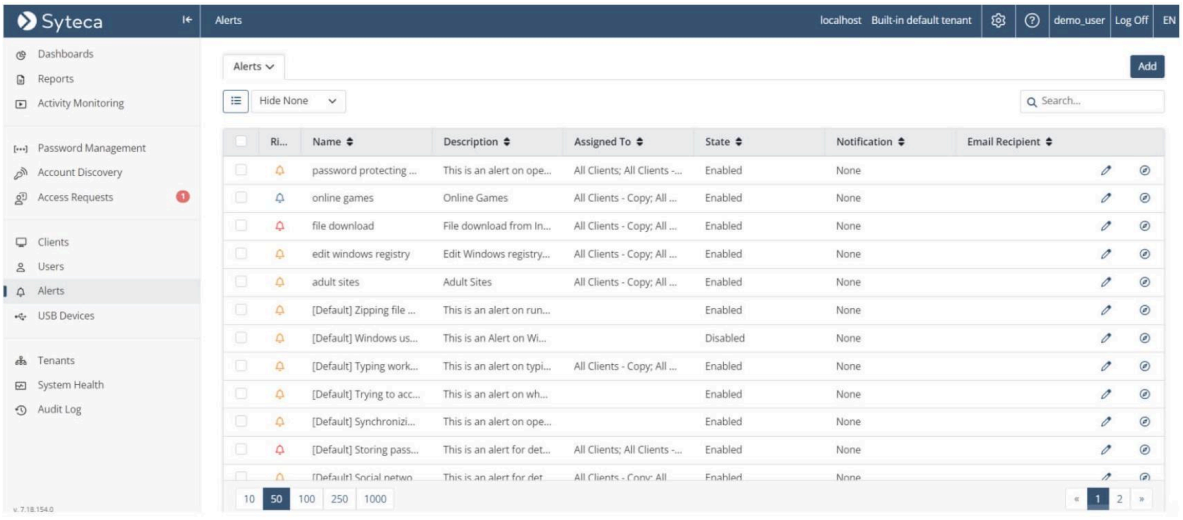
- Collected data pseudonymization to ensure user privacy and comply with data privacy requirements such as the GDPR.



Respond to security incidents

By detecting and responding to security threats quickly, your organization will be able to reduce the scale of potential damage and stop data breaches before they even happen. Syteca's incident response capabilities include:

- Real-time user activity alerts to receive live notifications about potentially harmful user activity.
- Automated incident response mechanisms that you can configure to tell Syteca how to respond to particular user behaviors, for example, by blocking users, killing processes, displaying warning messages, and blocking USB devices.



Additionally, Syteca assists you with incident investigation and remediation by generating customizable reports and exporting user sessions as tamper-proof digital evidence for forensic investigation.

Conclusion

Preventing and mitigating data extraction techniques is a complicated task that involves dealing with both possible attackers and negligent employees. By implementing the best cybersecurity practices from this article and using proven technologies such as user activity monitoring and access management, you'll cover the lion's share of potential vulnerabilities.

Book a Demo