sāf.ai
Data, Evolved.

DATA EXFILTRATION AND DATA THEFT

Resiliate

Data resiliency & integrity platform

Immunize your data from ransomware, data theft, and other cyber threats.

WHAT IS DATA EXFILTRATION?

Data exfiltration is the unauthorized transfer of data from a network, either manually or by automated process through malicious programming over a network. This occurs through a variety of methods, including email, removable media, and network protocols. Attackers often use malware or social engineering tactics to gain access to a network, and then use that access to extract sensitive information.

HOW ATTACKS HAPPEN

Social Engineering and Phishing Attacks

- Popular network attack vector used to trick victims into downloading malware and giving up their account credentials. Designed to look legitimate and from trusted senders, they either contain a malicious attachment that injects the user's device with malware or a link to a website that looks similar to a legitimate website but is spoofed to steal login credentials.

Outbound Emails

- Using email to exfiltrate any data that sits on an organizations' outbound email systems, such as calendars, databases, images, and planning documents. This data is stolen from email systems as email and text messages or through file attachments.

Downloads to Insecure Devices

- AKA accidental insider threat, e.g. accessing sensitive corporate information on a trusted device then transferring the data onto an insecure device.

Uploads to External Devices

- AKA malicious insider threat, e.g. exfiltrating data by downloading information from a secure device, then uploading it onto an external device.

Human Error and Non-secured Behavior in the Cloud

- When users access cloud services in an insecure manner, they enable bad actors to make changes to virtual machines, deploy and install malicious code, and submit malicious requests to cloud services. Human error and procedural issues also play a role as the appropriate protection may no longer be in place.

FIRST PROTECT. THEN ALERT.

A modern organization's technology is constantly in flux (e.g., introducing new applications to improve productivity, replacing out-of-date hardware & software, allowing software updates & patches, moving data to the cloud, etc.). This creates an ever-changing attack surface with nearly limitless possibilities for an attacker to breach your network. In the instance of data theft, there are nearly as many methods to surreptitiously exfiltrate sensitive data and damage the organization – its reputation, its brand, and its customers.

In this environment, consistently detecting and stopping data exfiltration with network and endpoint perimeters (e.g., intrusion detection systems (IDS), intrusion prevention systems (IPS), and data loss prevention (DLP) solutions) is nearly impossible. Attack methods are constantly changing and increasingly use techniques that are more difficult to detect / can be mistaken for regular network traffic, with attackers potentially lurking in networks unnoticed and exfiltrating data for months or even years.

Resiliate brings the focus back to the data and the user using a powerful AI that interweaves each block of data with its own neural net enabling data-centric security that cannot be bypassed (unlike perimeters) and that protects data against: unauthorized access and changes, data corruption and destruction, and data exfiltration.

While there are myriad ways of breaching a network and covertly exfiltrating data, at the data layer, the malicious activity is much easier to identify and stop – if you have the proper tool. Any data theft involves a pattern of malicious file access that is clearly aberrant relative to the historical patterns of what data is accessed and how, by certain users and groups. For example, a malicious actor will exhibit an aberrant access pattern as they seek to identify valuable data across a network or as they access files en masse.

With Resiliate, each file's AI maintains a complete history of that file and its metadata. Using that history and by automatically assigning trust credits and cost values to users, groups, and files, Resiliate establishes trust flows that determine the level of access that a user should have to specific resources based on their role, clearance level, and the sensitivity of the information they are trying to access.

Resiliate is capable of monitoring for any suspicious activity, such as attempts to access or transfer large amounts of data, or attempts to access sensitive data from unauthorized locations. When any such activity is detected, the system can trigger an alert and take appropriate action, such as revoking access or blocking the attempted transfer. Since this capability is built right into each individual file, it cannot be turned off or bypassed, and is nearly impossible to cheat.

This allows Resiliate to detect abuse of authorized access despite users having appropriate level of clearance (i.e., protecting against credential theft and insider threats all the way up to "evil admin"). The system detects and adjusts the trust to protect sensitive data.

So it doesn't matter what gets into your network, Resiliate ensures that data exfiltration attempts are detected and stopped, keeping sensitive information secure.

Using the same core principles, Resiliate also offers unprecedented data resiliency and protection against threats from ransomware and other cyber threats in the same solution.