Solution Brief

Stop Data Exfiltration

Ensure your crown jewels are safe.

In the **McAfee® Labs Threats Report: August 2015**, we take an in-depth look into one of the key steps in the data theft process: data exfiltration. This step entails the thief or actor moving or copying data from the owner's network to one that the attacker controls.

In the past 10 years, the industry has seen unprecedented growth in data breaches and the volume of people and organizations that they affect. Breaches have changed from gathering just credit and debit card numbers to now stealing virtually every piece of information we place online: names, dates of birth, addresses, phone numbers, healthcare information, account credentials, and much more.

Unfortunately, individuals are not the only targets. Cyberespionage by nation-states, criminal organizations, and hacktivists put sensitive individual and organizational data everywhere at risk.

Threat Actors and Motivation

A threat actor is an individual or group that attempts to gain unauthorized access to computer networks and systems. Across the security community, classifying such threats gives us three major categories: nation-states, organized crime, and hacktivists. The following table provides some insight into their motivations and potential data types that are valuable to them.

	Nation-State	Organized Crime	Hacktivists
General motives	Espionage Influence	Financial	Reputational Social
Example data types	Source code Emails Internal documents Military activity Government employee personally identifiable information (PII)	Bank account information Credit card data PII (including social security numbers, health data)	Emails Employee information Any sensitive internal data
Volume of data pursued	Small to large	Large	Small to large
Sophistication of exfiltration techniques	High	Medium to low	Medium to low
Location on the network	Unknown/often scattered	Known	Both known and unknown/ often scattered

Data Targets

Once an attacker compromises a system on the network, the attacker begins to explore other systems to uncover those that house the data they want. A complex network holds many types of data, making this a lengthy process for any actor without insider knowledge and increasing the chances of detection. Because of this, attackers try to be as stealthy and persistent as possible.

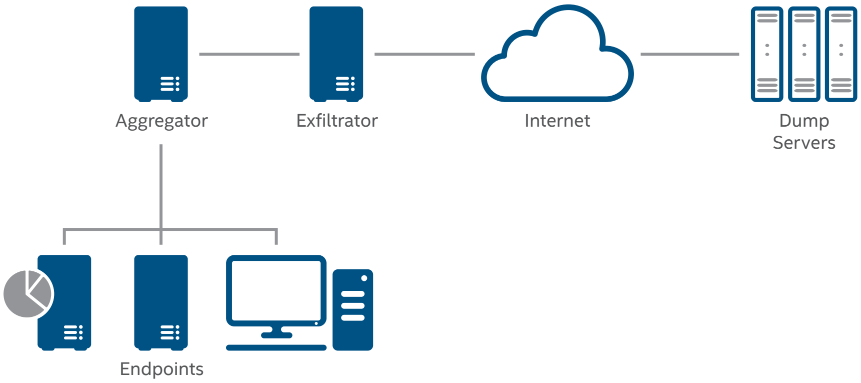
The main data targets can include:

Data Target	Types of Data	Actor Interest
Database systems	Protected health information (PHI), PII, credit cards, banking, and user accounts	Organized crime, hacktivists
Source code repositories	Source code, credentials, keys	Nation-states, hacktivists
Specialty systems	Varies	All, depending on endpoint type
File shares and similar systems	Source code, designs, communications, etc.	Nation-states, hacktivists
Email and communications	Designs, communications	Nation-states, hacktivists

Data Exfiltration

Once threat actors have located and obtained the data they want, the hardest part of the task begins: exfiltration of the treasure. Attackers will leverage the host's environment to act as an intermediary between the victim's and the attacker's networks. This staging infrastructure can be simple or complex, depending upon how deep and segmented the target data is on the network. Some of the roles systems can adopt in staging infrastructure can entail:

- **Endpoints:** Single or multiple data targets on the same segment or a routable segment to the aggregator.
- **Aggregator:** Serves as a collection point for the data from the target endpoints and uploads the data to the exfiltrator. The aggregator may or may not have Internet access. In sophisticated campaigns, multiple aggregators may transfer data to several exfiltrators to obfuscate the outbound data path.
- **Exfiltrator:** Takes data from an aggregator and facilitates the transfer of it to the attacker's dump server. This could be a simple transfer, or the exfiltrator may host the data for the attacker to retrieve.



Typical data exfiltration architecture.

Regardless of whether it is a simple or complex effort, the goal of the attacker is to get the targeted data onto a server that is outside the victim's network. Dump servers are the first points in which stolen information resides outside of the victim's control and can be easily accessed by the attackers. These servers can be:

- **Compromised systems:** Systems that have been compromised by the attacker during a separate campaign. These systems can be everything from personal WordPress blogs to servers belonging to companies with weak security controls.
- **Hosted systems in specific countries:** Countries with strong privacy laws are attractive to attackers because they may be able to host systems within their borders and remain undisturbed while being afforded a certain level of protection.
- **Temporarily hosted systems:** Short-lived systems hosted in the cloud through providers such as Amazon Web Services, Digital Ocean, or Microsoft Azure.
- **Cloud file-sharing services:** General-access online file-sharing sites such as Dropbox, Box.com, or PasteBin.
- **Cloud-hosted services:** Other Internet-based services, such as Twitter and Facebook, that allow users to post data.

Data Transports

Data transports are the protocols and methods that thieves use to copy data from one location or system to another, whether internal to internal (endpoint to aggregator) or internal to external (exfiltrator to dump server). Here is a summary of some of the most common transport protocols:

Transport	Description	Internal	External
HTTP/HTTPS	The prevalence of HTTP in network communications makes it an ideal protocol for hiding exfiltrated data with other traffic. It has been used as a general exfiltration transport by embedding commands in HTTP headers and within GET/POST/PUT methods.		■
FTP	FTP is commonly available on corporate servers and is easy to interact with using native system commands, making it a no-fuss transport.	■	■
USB	USB storage devices are frequently used for exfiltration when traversing air-gapped networks. We have seen malware that looks for a USB storage device with a specific marker, then copies to-be-exfiltrated data to a hidden sector on the device. When the device is placed into another infected system with network access, the exfiltration begins. USB storage devices can also be used by insiders to easily copy large amounts of data and physically remove it from the organization.	■	■
DNS	Specific DNS records, such as TXT or even A and CNAME records, can, to some extent, store data within them. With the control of a domain and a name server, an attacker can transmit small amounts of data by making specific lookups on the exfiltrating system.		■
TOR	The use of the TOR network is becoming more popular. It allows attackers to post exfiltrated data to servers that are difficult to trace. However, TOR traffic on corporate networks is rarely legitimate and thus can be easily detected and stopped.		■
SMTP/email	Both company- and non-company-owned SMTP servers can be used to send data out of the organization as attachments or in the body of email messages.		■
SMB	SMB is an extremely common protocol in Microsoft Windows environments and may already be enabled on systems.	■	
RDP	RDP supports various activities such as copy/paste and file sharing, and, in some cases, systems allowing RDP may be exposed to the Internet.	■	■
Custom transports	Custom transports are sometimes used in control server communications and sophisticated malware. A robust transport requires a great amount of effort, and its uniqueness makes the protocol easy to identify on the network—tilting the scale toward an established transport.	■	■

Data Manipulation

Attackers will take whatever steps are necessary to ensure they do not tip their hand to their targets when handling and exfiltrating sensitive data. The manipulation of data before its transfer can aid in avoiding detection, decrease transfer time, and even lengthen the time to detection. Some of the techniques commonly seen at this stage:

Technique	Description
Compression	Using the standard .ZIP file format not only provides a level of obfuscation but also speeds file transfers.
Chunking	Splitting data into small pieces before sending helps the transfer blend in with regular network activity.
Encoding/obfuscation	The most common type of data manipulation is a basic encoding or obfuscation algorithm. Using simple techniques such as performing an XOR operation with a static key, Base64 encoding, or simply converting each character to hex, the data can be manipulated just enough to avoid detection.
Encryption	It is surprising that encryption is not always used during exfiltration. Perhaps it is due to slower performance or just a lack of requirement. When used, it is common to see RC4 or AES encryption.

How Intel Security Can Help Protect Against Data Exfiltration

McAfee DLP Discover

The first step to properly securing data is to understand where the information resides and exactly what that data is. **McAfee DLP Discover** protects against data exfiltration by simplifying this first step through these capabilities:

- **Identify and control sensitive information:** Inventories and indexes all content through McAfee DLP Discover's automated scanning of all available resources, allowing you to better understand your sensitive data wherever it resides. With McAfee DLP Discover you can query and mine information to learn how it is used, who owns it, where it is stored, and where it has propagated.
- **Review and remediate violations:** Discovers content violations, registers and generates signatures, and sends alert notifications to protect sensitive data more effectively. Integration with management and incident workflow limits the proliferation of sensitive material.
- **Easily define policies for protection:** Provides intuitive and unified policy creation, reporting, and management to give more control over your information-protection strategy.

McAfee DLP Monitor

McAfee DLP Monitor gathers, tracks, and reports on data in motion across the entire network. You can easily uncover unknown threats to data and take actions to protect it and ensure your organization does not suffer the next big data breach.

- **Examine network traffic:** Examines network traffic at a deep level with McAfee DLP Monitor's industry-leading data scanning and analysis capability.
- **Quickly identify data:** Quickly details how data is being used, who is using it, and where it is going through real-time discovery, providing you with information on which to act. McAfee DLP Monitor can quickly identify more than 300 content types traversing any port or protocol, ensuring your organization is not blind.
- **Perform detailed forensics:** Conducts forensic analysis to correlate current and past risk events, detect risk trends, and identify threats. McAfee DLP Monitor allows you to quickly understand the situation, and develop rules and policies to address it.

McAfee DLP Prevent

McAfee DLP Prevent protects against data loss by ensuring that data leaves the network only when appropriate—whether through email, webmail, instant messenger, wikis, blogs, portals, HTTP/HTTPS, or FTP transfers. Being able to rapidly identify and mitigate exfiltration attempts is often the difference between keeping your prized data safe and becoming the next news headline.

- **Gain visibility to security incidents:** Provides summary and detailed views of security incidents and your mediation actions through customized views and incident reports.
- **Proactively enforce policies for all types of information:** Enforces policies for the information you know is sensitive, as well as for the information you may not know about. With a wide range of built-in policies—from compliance to acceptable use to intellectual property—you can match entire and partial documents to a comprehensive set of rules to protect all your sensitive information.

McAfee DLP Endpoint

McAfee DLP Endpoint enables you to instantly monitor and prevent data exfiltration on premises, off premises, and in the cloud. Quickly monitor real-time events, apply centrally managed security policies, and generate detailed forensics and proliferation reports without hindering day-to-day operations.

- **Enhanced virtualization support:** Enforces a per-user policy for multiple sessions and virtual desktop infrastructures, which allows for flexibility and better control of the data flowing to shared terminals.
- **Comprehensive incident reporting and monitoring:** Gathers all needed data, such as sender, recipient, timestamp, and network evidence for proper analysis, investigation, and audit—as well as for risk assessments and remediation.
- **Centralized management console:** Leverages the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console to define policies, deploy and update agents, monitor real-time events, and generate reports to meet compliance requirements.
- **Comprehensive content management:** Controls and blocks confidential data copied to USB devices, flash drives, smartphones, and other removable storage devices, including optical media and hard copy. Integration of DLP and digital rights management extends protection beyond your network.

McAfee Device Control

McAfee Device Control protects against data exfiltration via removable storage devices and media, such as USB drives, smartphones, CDs, and DVDs. It enables your organization to monitor and control data transfers from all desktops and laptops, regardless of their location, whether on premises or off premises. McAfee Device Control provides content- and context-aware device-blocking capabilities such as:

- **Comprehensive device and data management:** Controls how your organization's users copy data to USB drives, smartphones, recordable CDs and DVDs, and many other devices that can be leveraged for data exfiltration.
- **Granular controls:** Specifies which devices can and cannot be used, what data can and cannot be copied onto allowed devices, and restricts users from copying data from specific locations and applications.
- **Advanced reporting and auditing capabilities:** Simplifies compliance with detailed user- and device-level logging. Details such as device, timestamp, and data evidence are easily logged and reported to support audit and compliance inquiries.
- **Centralized management:** Offers real-time event monitoring and centralized policy and incident management through integration with McAfee ePO software.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com