UpGuard™

A Complete Guide to

Data Breaches

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

UpGuard

Table of Contents

Introduction

In 2022, the average cost of a data breach reached a record high of US$4.35 million[1], and in 2023, that figure is expected to rise to $5 million. Every week, a new round of businesses make news headlines for suffering a breach. Some barely recover from the reputational damages that follow, and others never do. Without sufficient security controls in place to prevent data breaches, it's only a matter of time before your business becomes another costly breach statistic.

This document outlines a cybersecurity strategy based on common cyberattack tactics to help you establish a resilient data breach prevention program.

1. IBM (2022). Cost of a data breach 2022. [online] www.ibm.com. Available at: https://www.ibm.com/reports/data-breach.

UpGuard

Getting Started with Data Breaches

What is a Data Breach?

A data breach is a security incident where sensitive information is copied, transmitted, viewed, stolen, or accessed by an unauthorized individual.

Data breaches are most prevalent in industries that deal with large amounts of personal data, such as the healthcare and financial sectors. However, with digital transformation multiplying connections between businesses, their vendors, and customers, every organization is now a potential link to a data breach target, making data breaches an increasingly industry-agnostic threat.

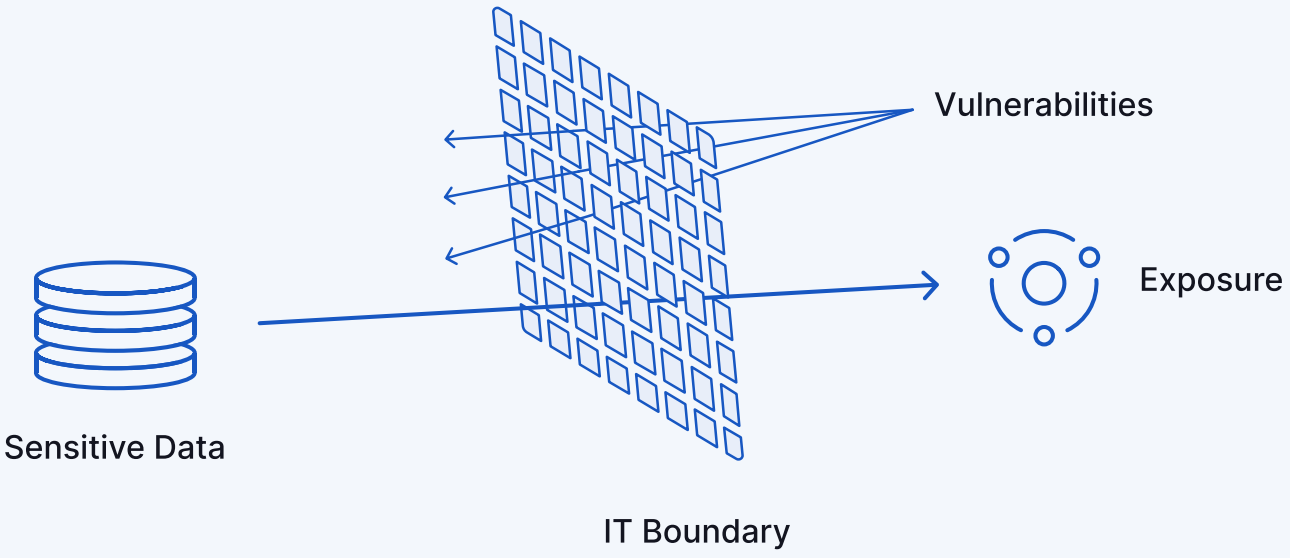
Data breaches occurring through compromised third-party vendors are known as third-party breaches. In a third-party breach, instead of attacking an organization's network directly, hackers target third-party vendors with access to an organization's internal systems. Because vendors tend to have weaker cybersecurity standards than most high-value targets, this cyberattack pathway allows hackers to breach victims faster and with less effort.

The Difference Between Data Leaks and Data Breaches

The terms "data breach" and "data leak" are commonly used interchangeably, but these are two different events.

Data Leaks

Any unintentional exposure of sensitive data to the public is classified as a data leak. These events could include overlooked misconfigurations exposing internal databases, or the unauthorized publishing of sensitive information on the internet.



A Famous Data Leak Example

A famous example of a data leak is the Microsoft Power Apps data leak that UpGuard researchers discovered in 2021.

The data leak was caused by a default Power Apps misconfiguration resulting in the exposure of over 38 million sensitive records.

UpGuard notified Microsoft about the leak, who promptly responded to it, preventing a potential large-scale data breach impacting many reputable organizations, including:

- American Airlines
- Ford
- J.B. Hunt
- The Maryland Health Agency
- The New York City Municipal Transportation Authority
- The New York's Department of Education

> "We found one of these [portals] that was misconfigured to expose data, and we thought, we've never heard of this. Is this a one-off thing, or is this a systemic issue?"

Greg Pollock
UpGuard's vice-president of cyber research

Other Data Leak Examples

Data leaks don't just occur through overlooked misconfigurations. They also happen when sensitive data is intentionally published online without authorization. A popular example of such a data leak is cybercriminals publishing credentials stolen in a ransomware attack on their ransomware blog.

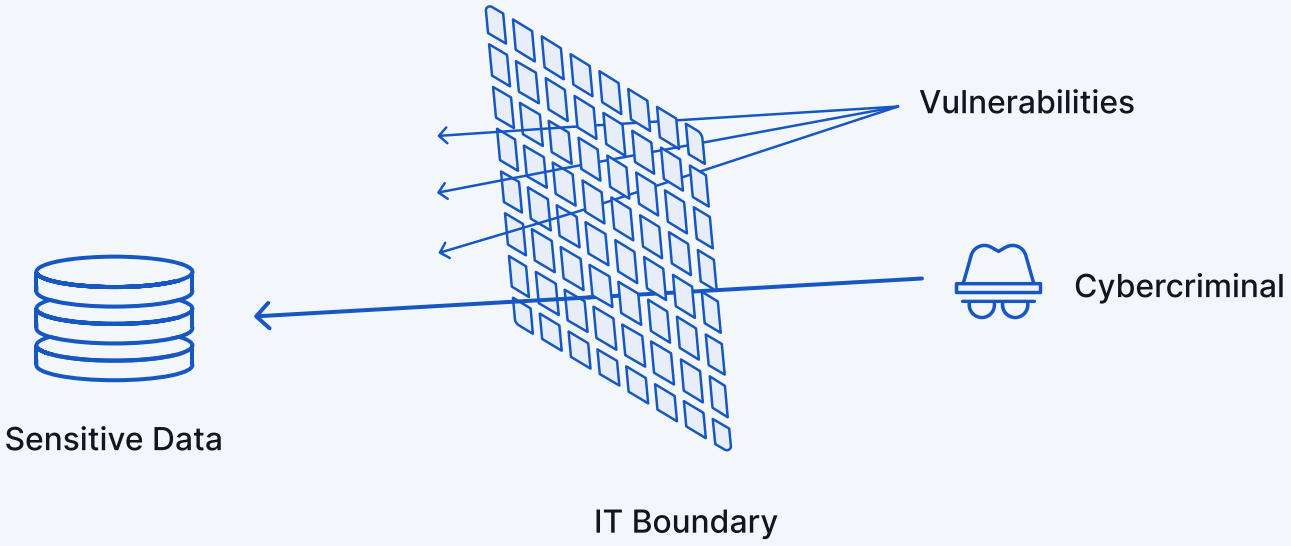
> A ransomware blog is a ransomware gang's official noticeboard hosted on the dark web.

Other examples of initiated data leaks include:

- Cybercriminals publishing stolen data for sale on a dark web marketplace following a data breach.
- Cybercriminals freely publishing stolen data on dark web forums.
- Insider threats publishing internal trade secrets and intellectual property on the internet.

Data Breaches

A data breach, on the other hand, is the outcome of a planned cyberattack. These events are caused by an external party forcing their way through an IT boundary and into sensitive network resources, usually by exploiting security vulnerabilities.



It's important to understand the difference between data breaches and data leaks, as each event follows a distinct data compromise pathway requiring a unique set of security controls.

The most successful data breach prevention strategies address the complete scope of data breach attack vectors, including data leaks. An example of such an integration is provided in the data breach prevention framework on page x of this ebook.

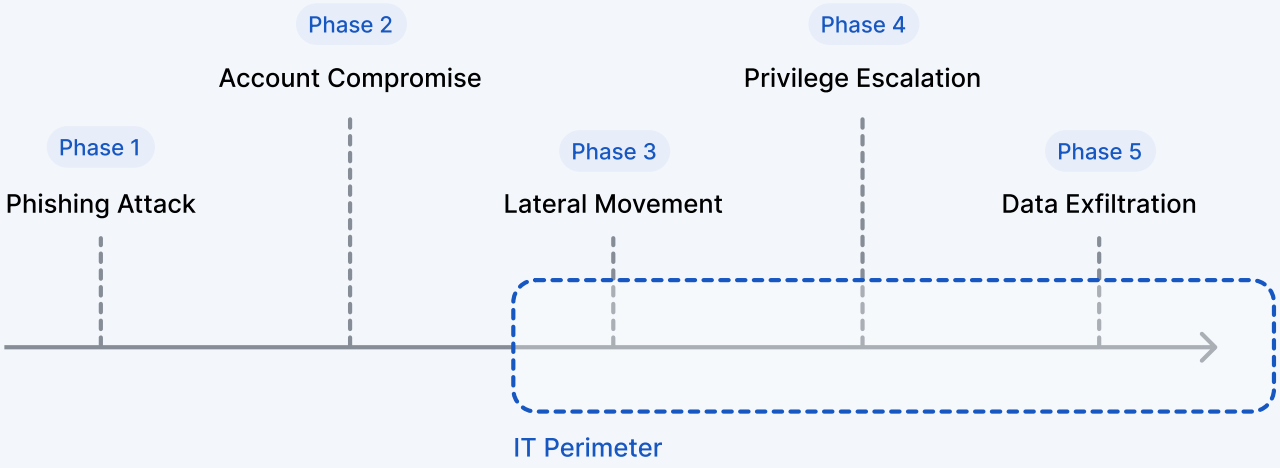
UpGuard

The Cyber Attack Pathway

The Cyber Attack Pathway

The silver lining of living in a world of mass breaches is that we now have enough data to understand the steps leading to a data breach. These five stages are outlined in a model known as the cyberattack pathway. Understanding the cyberattack pathway is the first step to designing an effective data breach prevention strategy.

The typical cyberattack pathway can be broken down into 5 phases.



Phase 1 - Phishing Attack

During phase 1 of the attack, an email posing as an important message from an authoritative sender is sent to a victim. These emails include malicious links leading to fraudulent websites designed to steal network credentials.

> In 2022, phishing was the most expensive initial attack vector, resulting in average data breach damage costs of USD 4.91 million[2]

Phase 2 - Account Compromise

During phase 2, the victim performs the intended action of the phishing attack. This could involve clicking a link leading to a credential-stealing website or downloading a malicious file attachment that creates a means for cybercriminals to access the victim's computer remotely. In either case, the objective is to compromise the victim's account and use it to access the organization's network.

Phase 3 - Lateral Movement

After penetrating the network, hackers move laterally to learn the network's layout. Sometimes hackers remain dormant for months, watching internal activities and learning user behaviors. Then, when they're ready, deeper network regions are accessed based on these learnings using previously compromised credentials. Hackers are also actively searching for privileged credentials to compromise in this stage to facilitate access to highly sensitive data resources.

2. 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute.

Phase 4 - Privilege Escalation

After locating and compromising privileged credentials, cybercriminals gain deeper access to highly sensitive network regions that can only be accessed with privileged accounts.

Once inside this critical region, cybercriminals begin the hunt for the following types of sensitive data:

- Personal data;
- Customer data;
- Social security numbers;
- Corporate email accounts details;
- Personal email account details, such as Gmail accounts;
- Any digital footprint details that could be used in an identity theft campaign (to potentially arm further, more targeted phishing attacks);
- Vulnerability disclosure and reports - an internal register of all computer system vulnerabilities security teams are yet to remediate.

Phase 5 - Data Exfiltration

Finally, after valuable data resources are located, cybercriminals deploy trojan malware to establish backdoor connections to their servers (known as command and control servers) and begin clandestinely transferring sensitive data out of the victim's network.

UpGuard

Preventing Data Breaches

Preventing Data Breaches

A simple yet effective data breach prevention strategy involves adding resistance to the cyberattack pathway to make it increasingly difficult for hackers to progress toward their data theft objective.

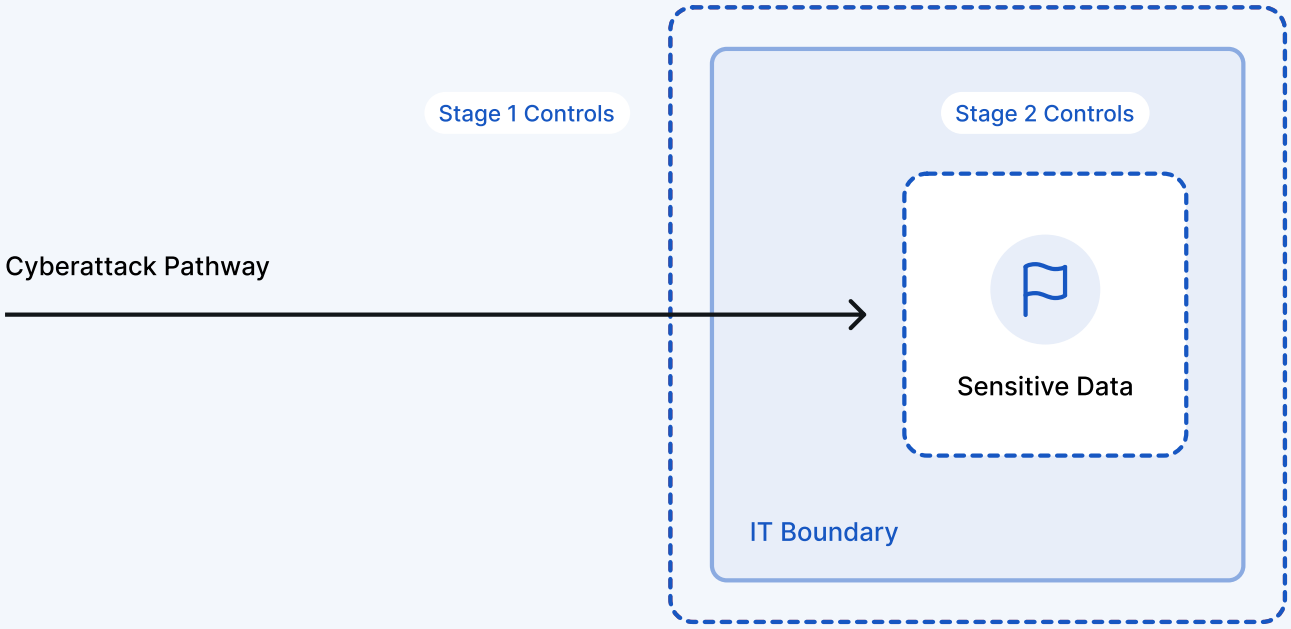
This strategy can be broken down into two stages:

Stage 1

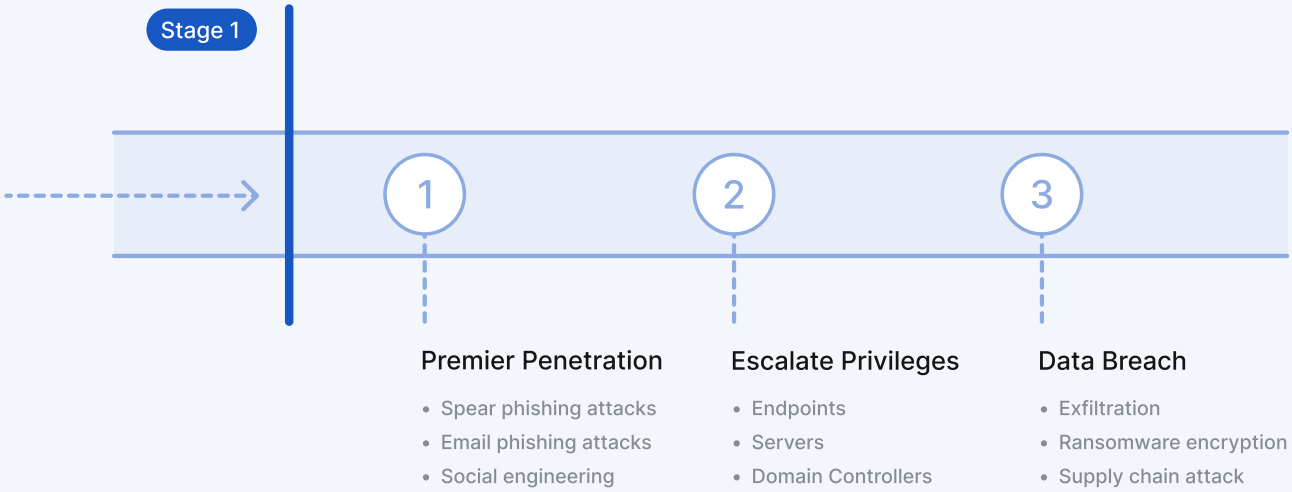
Preventing network compromise.

Stage 2

Preventing access to sensitive data.



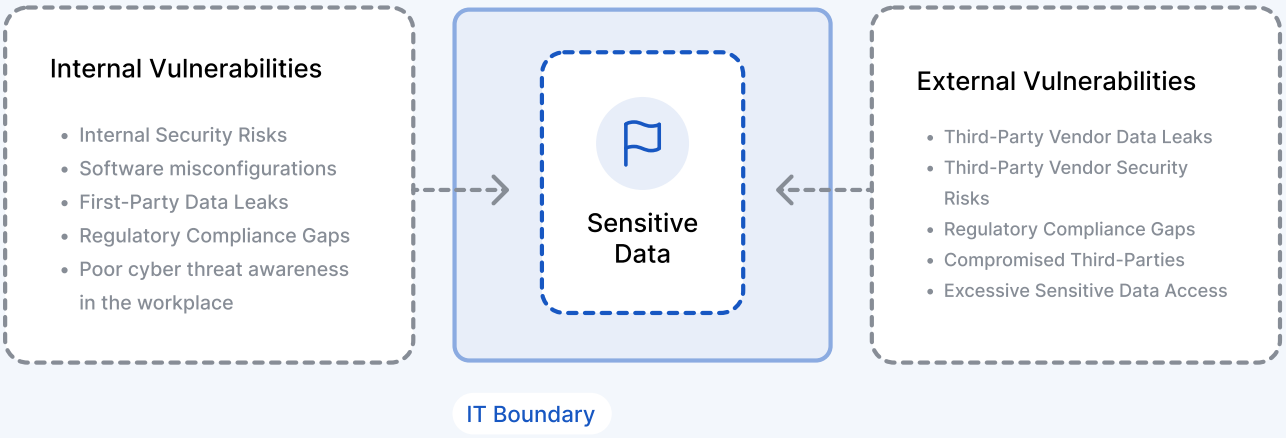
Stage 1:
Preventing Network Compromise



Data breach attempts are much harder to stop after a cybercriminal has entered your private network. The objective of stage 1 is to stop data breach attempts before your network is compromised - that is, to prevent hackers from progressing beyond phase 1 of the cyberattack lifecycle.

To maximize your chances of mitigating data breaches, there should be a greater emphasis on security controls preventing network penetration.

Network compromise could occur from internal network vulnerabilities or vulnerabilities across the third-party vendor network. A network protection strategy should, therefore, address the complete scope of attack vectors facilitating breaches - across both the internal and third-party attack surfaces.



The four cybersecurity disciplines of attack surface coverage:

This complete scope of attack surface coverage is achieved through four cybersecurity disciplines.

1. Cyber Awareness Training

Employees are the first line of defense for every cybersecurity program. Despite how much you invest in a cybersecurity program, it's useless if an employee can be tricked into handing over the keys to your private network.

Cybercriminals trick employees into divulging private network credentials in one of two ways:

- **Phishing** - The practice of sending fraudulent emails purporting to be from reputable sources to coerce recipients into divulging private information.
- **Social engineering** - The use of emotional manipulation to force victims into divulging private information. Social engineering attacks don't just happen via email. They could occur over the phone (for example, a caller posing as a member of the IT department), or even in person (for example, a job applicant asking the receptionist for access to the WI-FI network to modify their resume).

Data breaches occurring through compromised employees aren't the result of carefully executed strategies designed by internal threats. The reason is much simpler. These breaches happen because employees don't know how to recognize and respond to cyber threats.

Implementing cyber awareness training will equip your employees to avoid falling victim to phishing attempts. And if your training is effective, this single effort could protect your business from the leading cause of data breaches globally[3].

The following topics should be covered in cyber awareness training:

- Phishing attacks
- Removable media
- Passwords and authentication
- Physical security
- Mobile device security
- Working remotely
- Public Wi-Fi
- Cloud Security
- Social media use
- Internet and email use
- Social engineering
- Security at home

An ideal cyber awareness training program should be coupled with frequent simulated phishing attacks to keep cyber threat awareness front of mind.

[3]Cisco Umbrella. (n.d.). 2021 Cybersecurity threat trends: phishing, crypto top the list. [online] Available at: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list.

2. Internal Security Vulnerability Management

Internal security vulnerabilities could range from product misconfigurations, open ports, lack of MFA, and even typosquatting susceptibility. Discovering these security threats is a collaborative effort between internal audits - using risk assessments and/or security questionnaires - and security ratings.

Security ratings are objective qualitative measurements of your organization's security posture, ranging from 0 to a maximum score of 950. When used in conjunction with internal risk assessments, security ratings help you track the impact of all required remediation efforts on your overall security posture, supporting continuous alignment with your corporate risk appetite.

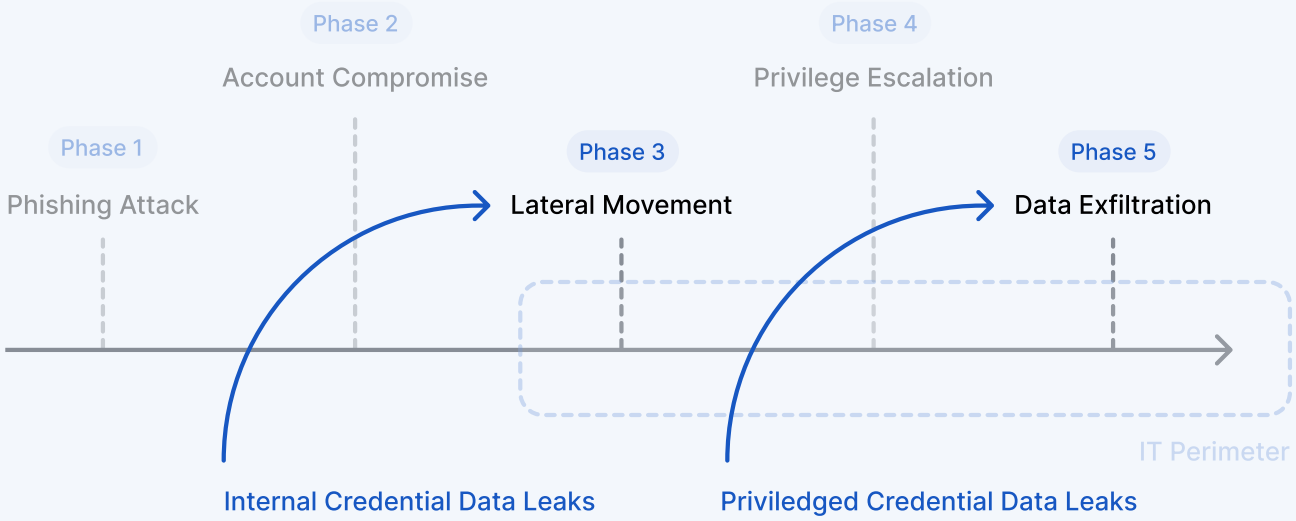
A straightforward strategy for minimizing network compromise risk is keeping your company's security rating as high as possible.

Security ratings are a simple, high-level metric for tracking data breach susceptibility.

3. Data Leak Management

Most conventional data breach mitigation strategies lack a data leak management component. This is unfortunate since data leaks could significantly expedite data breaches by compressing the cyberattack pathway.

Data leaks exposing internal credentials could help cybercriminals to circumvent all security controls preventing unauthorized network access, allowing them to jump straight to phase 4 of the cyberattack pathway. Leaked privileged credentials compress the cyberattack pathway even further, allowing hackers to jump straight to the final data exfiltration phase.



The average cost of a data breach in 2022 was USD 4.35 million[4]

According to the 2022 Cost of a Data Breach report by IBM and the Ponemon Institute, victims that respond to data breaches in less than 200 days spend an average of $1.1 million less on data breach damages. So if you're currently a victim of data leaks, not only are you increasing your risk of suffering an expedited data breach, you're also increasing your risk of paying more in data breach damages.

Both internal and third-party data leaks impact your risk of suffering a data breach. A data leak management strategy should be capable of discovering and shutting down leaks across these threat landscapes.

Common dark web data leaks hosts include:

- **Ransomware blogs** - ransomware gang noticeboards displaying public announcements and links to stolen data.
- **Dark web marketplaces** - cybercriminals marketplaces selling stolen data from cyberattacks.
- **Dark web forums** - cybercriminal forums hosting discussions about cybercrime.
- **Telegram groups** - Private message groups between cybercriminals.

4. 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute

When choosing a data leak detection solution, there are two important considerations:

1. False Positives

   Not all data leak announcements are legitimate. Cybercriminals often falsify such announcements in ransomware blogs to mislead and divert security investigations. Due to the high likelihood of this happening, detected data leaks should always be manually reviewed for false positives - either by internal IT security teams or externally if leveraging the support of managed data leak detection services.

2. Third-Party Data Leaks

   Almost 60% of data breaches are caused by a compromised third-party vendor[5] (third-party breaches). Since third-party data leaks facilitate third-party breaches, overlooking these attack vectors means overlooking events most likely to result in your organization suffering a data breach.

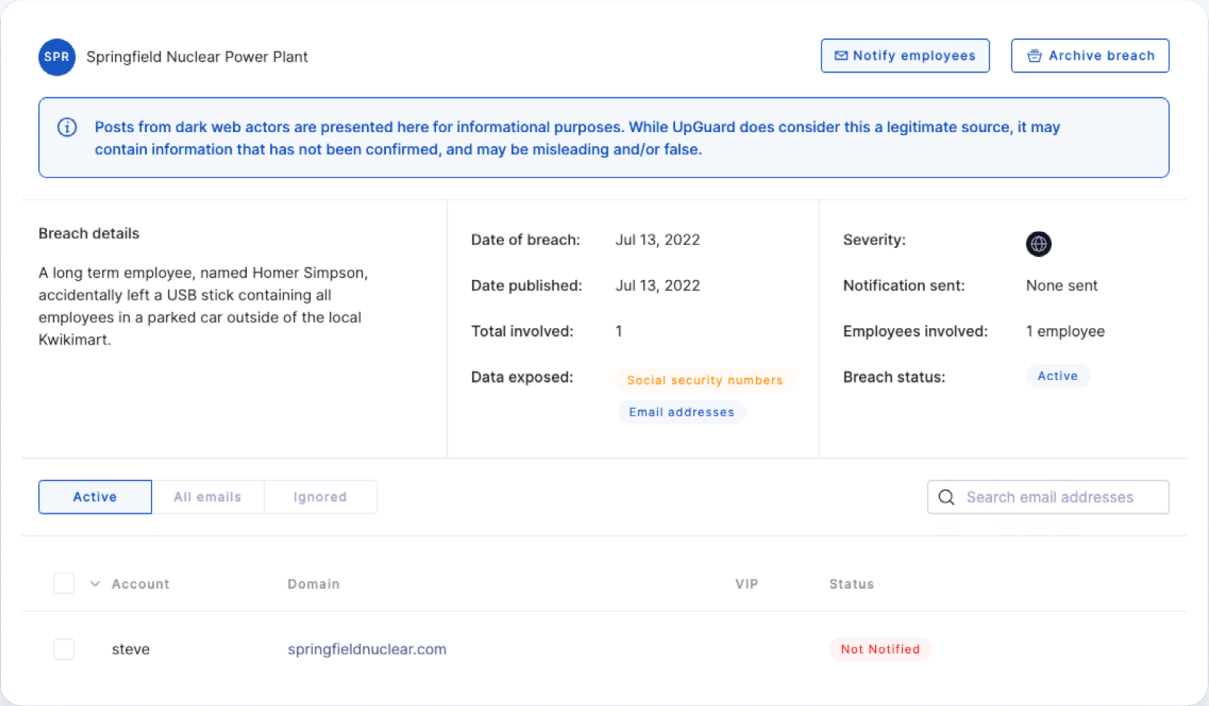
The scope of data leak dumps is vast and ever-expanding. Tracking data leaks at a rate that matches their appearance across thousands of potential hosts can only be successfully managed with the support of an automated scanning solution.

5. Security, H.N. (2018). Third parties: Fast-growing risk to an organization's sensitive data. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2018/11/20/third-party-risks/.

How UpGuard Helps with Data Leak Management

UpGuard's data leak detection solution combines an AI-assisted search engine with manual reviews from cybersecurity analysts to reduce false positives and unnecessary response efforts.

For the most comprehensive coverage of potential data leaks linked to your business or any of your vendors, UpGuard continuously monitors common data leaks hosts on the dark web, including ransomware blogs and data collection releases.



4. Vendor Risk Management

Vendor Risk Management (VRM) is the process of mitigating security risks arising from third-party vendors and service providers. VRM programs address the unique security risks and exposures faced at each stage of a vendor relationship.

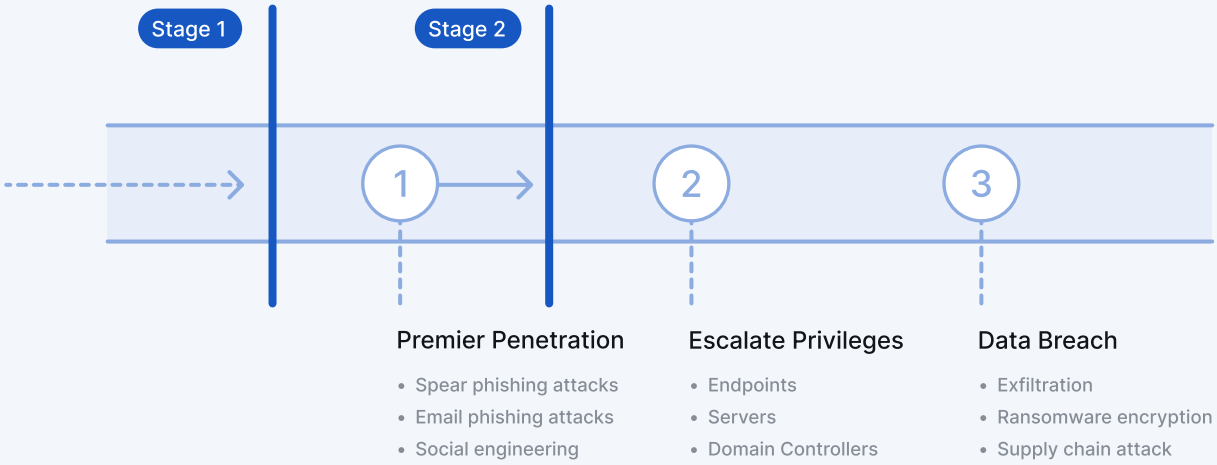
1. **Onboarding** - Using a combination of risk assessment and security ratings, a VRM program evaluates the security postures of prospective vendors to ensure alignment with risk appetites.
2. **Regulatory Compliance** - By mapping security questionnaire responses to popular cybersecurity frameworks, a VRM program can identify compliance gaps to support ongoing compliance and prevent costly violations.
3. **Continuous Monitoring** - With continuous third-party attack surface monitoring, a VRM program detects emerging vendor security risks that could lead to third-party breaches.
4. **Termination** - With bespoke risk assessments scrutinizing access levels, a VRM program ensures offboarded vendors no longer have access to sensitive resources.

A critical component of Vendor Risk Management is third-party attack surface monitoring. This feature identifies potential security vulnerabilities that could facilitate third-party breaches and, by extension, the compromise of your internal sensitive data.

Detecting and addressing third-party security risks prevents hackers from penetrating your network through a compromised vendor.

Stage 2:

Preventing Access to Sensitive Data



Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) introduces a series of additional user-identify confirmation steps between a login request and access approval.

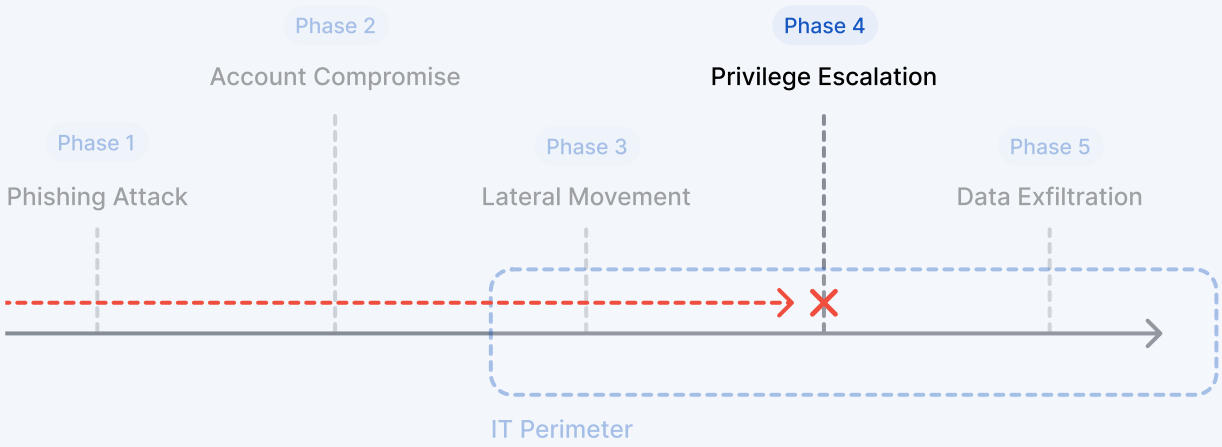
The most secure form of multi-factor authentication includes a biometric authentication method. Biometric data, such as fingerprints, or advanced forms of facial recognition, is very difficult for cybercriminals to steal or replicate.

A powerful user authentication protocol often used in conjunction with MFA is Passwordless Authentication. Passwordless Authentication requires users to submit proof of their identity

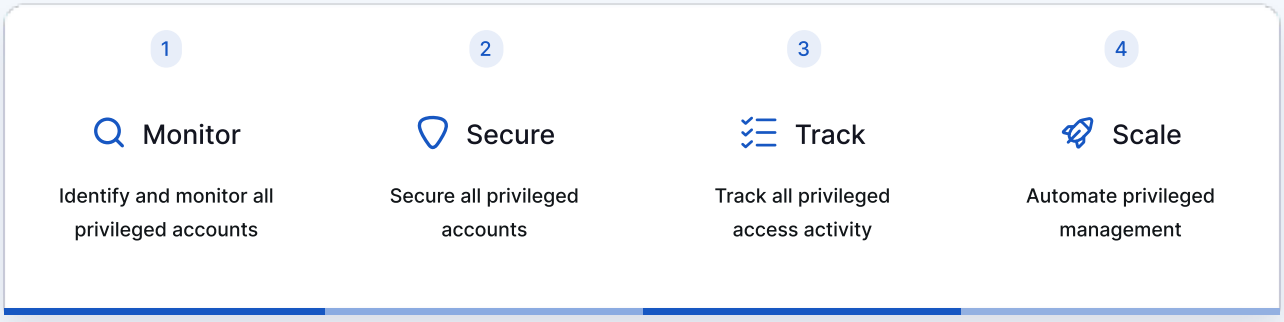
without entering a password. Common authentication methods include the submission of fingerprints or hardware token codes.

Privileged Account Management (PAM)

Privileged Access Management is the process of monitoring and securing users with the authority to access sensitive business resources. With PAM controls in place, a hacker could be prevented from progressing beyond the fourth stage of the cyberattack pathway (privilege escalation).



A Privileged Account Management strategy protects sensitive resources from unauthorized access through a 4-pilar framework.



Zero-Trust Architecture (ZTA)

Zero Trust is a Cybersecurity architecture developed by the NIST (National Institute of Standards and Technology). This framework assumes all network activity, whether internal or external, is a security threat. To prove otherwise, user accounts are continuously authenticated whenever sensitive resources are requested.

> A Zero Trust Architecture includes other account compromise controls, such as Multi-Factor Authentication and privileged escalation management policies.

Zero Trust is a Cybersecurity architecture developed by the NIST (National Institute of Standards and Technology). This framework assumes all network activity, whether internal or external, is a security threat. To prove otherwise, user accounts are continuously authenticated whenever sensitive resources are requested.

Network Segmentation

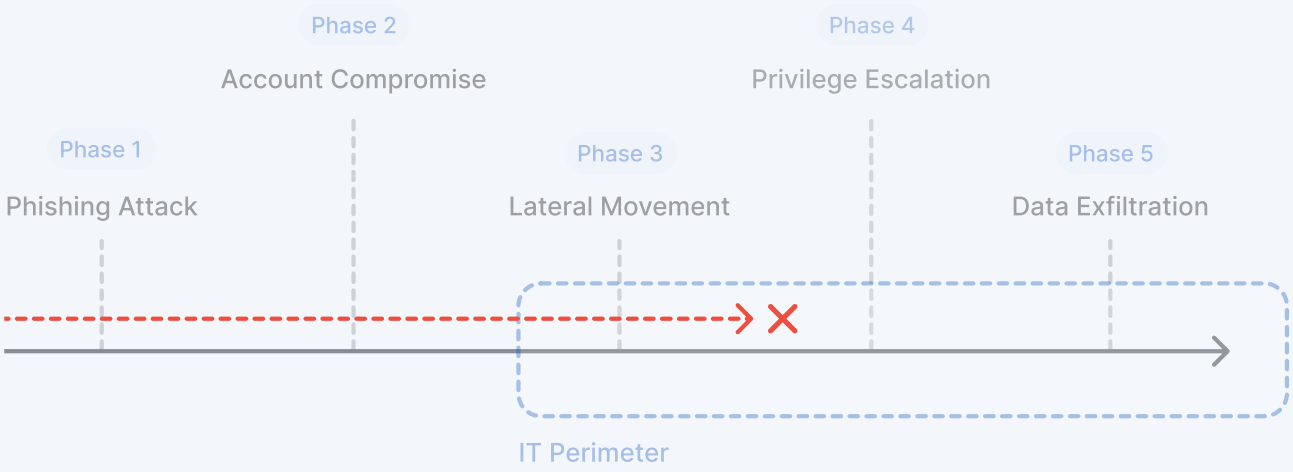
After a hacker has breached a network, they start moving laterally to identify where all the sensitive resources are located. Lateral movement can be disrupted by segmenting sensitive network regions from general user pathways.

To maximize obfuscation, all user accounts with access to these closed regions should be guarded with Multi-Factor Authentication, with all connection requests approved from within jump boxes (hardened machines in an isolated network hosting privileged credentials).

Data Encryption

Should all the above stage 2 controls fail, and hackers gain access to a sensitive customer database, the data contained therein will be of very little use to hackers if it's encrypted. The Advanced Encryption Standard is the ideal encryption method to use since its the standard trusted by government entities.

A data encryption policy should apply to all internal data at rest and in motion - not just the sensitive regions. Encrypting all internal data could prevent hackers from learning user behaviors to arm their lateral movement and privilege compromise efforts, thereby disrupting the attack's progression between phases three and four of the attack pathway.



UpGuard

Protect Your Organization from Data Breaches with UpGuard

UpGuard's suite of features reduces data breach risks across multiple threat categories to create the most comprehensive data breach prevention solution.

Internal and Third-Party Risk Discovery

Based on an analysis of 70+ attack vectors, UpGuard offers a continuously updated quantitative measurement of your internal security posture and the security postures of all your vendors.

Data Leak Detection

With an AI-powered search engine also addressing third-party data leaks, and a team of cybersecurity experts assessing for false positives, UpGuard helps you efficiently detect and shutdown the complete scope of data leaks before they're abused by cybercriminals.

Vendor Risk Management

With features addressing risk exposure throughout the vendor lifecycle, including security ratings for prospective vendors, customizable questionnaires, and security assessments highlighting compliance gaps, UpGuard offers a complete framework for an effective vendor risk management program.

Free trial →

UpGuard

We're here to help, shoot us an email at sales@upguard.com

Looking for a better, smarter way to protect your data and prevent breaches?

UpGuard offers a full suite of products for security, risk and vendor management teams.

Free Trial →

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

www.upguard.com

+1 888-882-3223

650 Castro Street, Suite 120-387, Mountain View CA 94041 United States