

Acronis



Acronis Cyber Protection 101

What you need to know

Table of contents

■ What is cyber risk?	3	Distributed denial-of-service (DDoS) attacks	10
Types of cyber risk	3	Advanced persistent threats (APT)	10
Addressing the risk	3	Zero-day exploits	11
■ What is data protection, cybersecurity, and cyber protection?	4	Fileless attacks	11
Data security	4	Data leakage	11
Cybersecurity	4	■ Protecting your business	12
Cyber protection	4	Antivirus software	12
■ The power of integration	5	Anti-ransomware	14
Common challenges in cybersecurity	5	Backup and recovery	14
Integration as an advanced security measure	5	Patch management	15
■ What are vulnerabilities?	6	URL filtering	15
Vulnerability assessment and penetration testing	6	Firewalls	15
Useful terms	6	Virtual private networks (VPN)	16
■ Attack techniques to be aware of	7	Data loss prevention (DLP)	16
Malware	7	Multilayered security (defense in depth)	17
Ransomware	7		
Phishing	9		
Drive-by downloads	9		
		About Acronis	18
		Cyber protection is complicated, let's do it together	18

What is cyber risk?

Cyber risk describes the probability of loss or harm resulting from cyberattacks or data breaches. Any organization that uses modern technology must contend with some level of cyber risk, and taking steps to address this risk is crucial to business health and security.

Types of cyber risk

Based on the intent (malicious or accidental) and the actor (internal or external), cyber risks may be grouped into four categories:

- **Internal malicious** — deliberate acts of espionage, theft, or other malfeasance committed by employees or other inside actors.
- **Internal unintentional** — acts leading to damage or loss, caused by human error or negligence by employees or other inside actors.
- **External malicious** — intentional, premeditated attacks from outside parties, such as cybercriminals, hackers, and nation states. It is the most common cyber risk for organizations.
- **External unintentional** — acts by external third parties that cause unintentional loss or damage to the organization.

Addressing the risk

- **Risk management** — an ongoing process of identifying, assessing, and controlling cyber risks by implementing plans to address them.
- **Risk mitigation** — part of risk management related to taking specific action to reduce an organization's risk exposure and limit the probability of those risks reoccurring the future.
- **Risk transfer** — a mechanism of risk management defined by the transfer of risks from one party to another. A common example of risk transfer is cyber insurance, wherein an MSP may transfer a business' data breach liability to a third party (insurance company).

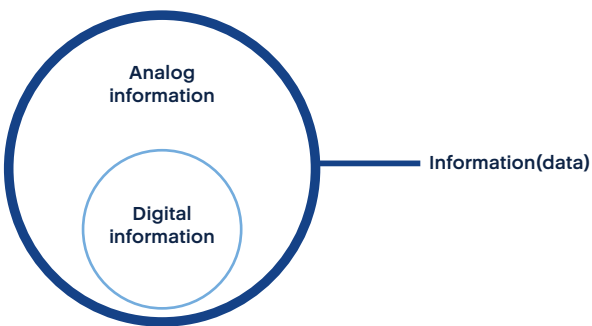
No matter how thorough your security program is, cyber risks can never truly be eliminated, as new vulnerabilities and malware are discovered each day. The risk that remains in place after security measures and controls are put in place is called residual risk.



What is data protection, cybersecurity, and cyber protection?

Data is at the core of modern business: utilized in everyday operational processes, and essential for innovation and decision making. It also enhances our lives on a daily basis. Data is now the world's most valuable resource, which means data safety is not only an essential part of business operations – it is now a basic human need.

Data security

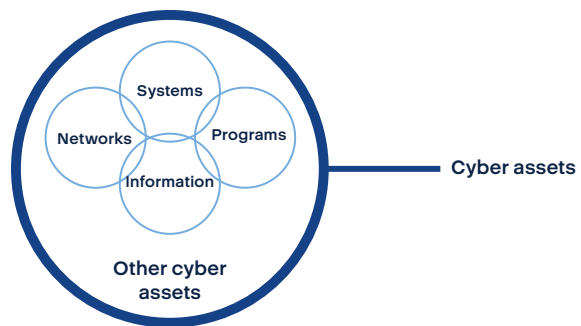


Data security relates to the protection of data itself from unauthorized disclosure, destruction, or modification — whether intentional or accidental — through the use of safeguards that limit the data's accessibility. Ways of securing data include:

- **Encryption** — transforming original data into an unreadable, encoded format (cyphertext) that can be decoded only by individuals who know the decryption key.
- **Data backup** — creating recoverable copies of data, in case the original data is lost or compromised.
- **Data masking** — masking sensitive areas of data while retaining the original data's characteristics, so that individuals without the required authorization can't access it.
- **Data erasure** — completely removing data that's no longer in use, ensuring that it's unrecoverable by unauthorized parties.

Data security is mainly focused on data itself, especially data identity and access management.

Cybersecurity



Cybersecurity, on the other hand, relates to the protection of your IT assets — including networks, programs, and systems — against cyberattacks. Rather than focusing on data itself, cybersecurity is concerned with the systems that make the storing, computing, transfer, and authentication of data possible.

Challenges for data owners

Today's organizations face some critical challenges. Data creation, processing, and storage is increasingly done at the edge, greatly increasing operational complexity and making data flows harder to track. The rapid increase of data volumes also increases storage costs, while complexity strengthens the need for IT personnel amidst a worldwide IT talent shortage. Meanwhile, ever-greater computing power and artificial intelligence (AI) are widely accessible, allowing cybercriminals to target businesses more often and effectively than ever before.

Cyber protection

Safeguarding your data — and the applications and systems that rely on it — requires an approach that combines data protection and cybersecurity to ensure

both protection against cyberthreats and ability to restore data in case of incidents, preserving business continuity. To ensure the efficiency, ease, and reliability of this approach, the complex and often-competing challenges that we refer to as the Five Vectors of Cyber Protection should be addressed in a balanced way:

Safety

Ensure that reliable copies of your data, applications, and systems are always available

Accessibility

Make your data, applications, and systems easily available from anywhere at any time

Privacy

Control who has visibility and access to all of your digital assets

Authenticity

Create undeniable, certifiable proof that a copy is an exact replica of the original

Security

Protect your data, applications, and systems against today's ever-changing cyberthreats

Addressing each of these five vectors is the only way to guarantee complete cyber protection and answer all modern challenges in the digital space.

The power of integration

Common challenges in cybersecurity

COMPLEXITY

- **Skill gap** — 84% of organizations experience a cybersecurity skills shortage, with total global talent shortage exceeding 4 million
- **Multiplicity** — 69% of security administrators report that IT currently spends more time managing security tools than effectively defending against threats. 53% admit that the number of security tools is so burdensome that it adversely impacts security and increases risks

COST

- **Total cost of ownership (TCO)** — 72% of global organizations saw their IT costs increase during the pandemic, due to the need for numerous tools to enable remote access and collaboration while efficiently protecting against cyberattacks

SECURITY EFFICIENCY

- **Attack surface growth** — 88% of employees say that they'd like to continue working remotely to some extent
- **Attack complexity** — 63% of SMBs have experienced a data breach in 2019 alone, with antivirus solutions failing to prevent 57% of attacks

Integration as an advanced security measure

To counter the growing challenges of complexity, cost, and efficiency of security, advanced cyber protection solutions integrate numerous security capabilities in a single solution to:

- **Save time and resources** with a central management of a vast range of security capabilities amidst a worldwide security personnel shortage
- **Minimize total cost of ownership (TCO)** with a single solution for defense-in-depth security
- **Guarantee more efficient and compatible defense capabilities** through integration
- **Map the functionalities of different security measures** together to increase their efficiency and precision, or even introduce new security capabilities

Examples of the latter might include more timely addressing of vulnerabilities by integrating vulnerability scanning and patch management, or implementing anti-malware scanning of data backups to ensure seamless recovery.

What are vulnerabilities?

In cybersecurity, vulnerabilities are weaknesses which can be exploited by a threat actor to cross authorized boundaries. The collection of all vulnerabilities is known as an attack surface.

New vulnerabilities are found every day, but not all vulnerabilities are equal with respect to ease of exploitability or severity of impact on businesses. For example, a Windows vulnerability that can give an attacker operating system-level privileges is much more severe than a Skype vulnerability that allows eavesdropping on Skype test calls. To prioritize the response according to the vulnerability's threat level, cybersecurity specialists use an open industry standard known as the Common Vulnerability Scoring System (CVSS). The standard rates the impact of each vulnerability using a numerical score of one to 10. The score can be translated into a qualitative representation — low, medium, high, or critical.

Vulnerability assessment and penetration testing



Vulnerabilities need to be analyzed and addressed to mitigate potential damage on the company. Vulnerability assessments and penetration testing are two types of vulnerability testing. Each has different strengths, and they're often combined to achieve a more thorough analysis.

A vulnerability assessment is usually highly automated (through vulnerability scanners) and searches for known weaknesses in the target system — such as outdated software, unapplied patches, common gaps in network controls, or weaknesses in applications. However, vulnerability assessments don't take into account other environmental controls that might render the vulnerability useless as an exploit.

Penetration testing, on the other hand, is a manual process that attempts to simulate the actions of an attacker. Testers try to exploit found vulnerabilities to understand whether it is exploitable and severe — the degree to which a cybercriminal could gain unauthorized access to assets.

If vulnerability assessment is like checking whether a door is closed and locked, penetration testing is akin

to also opening the door, walking in, and simulating a burglary.

Useful terms

False positive — A test result that incorrectly suggests the presence of a vulnerability. Precisely identifying vulnerabilities is necessary to properly manage resources used in addressing them. Third-party testing by independent laboratories can help gauge accuracy of a software solution.


False negative — A test result that incorrectly suggests the absence of a vulnerability. False negatives leave unknown vulnerabilities present in the system. Third-party evaluations by independent testing labs can help you understand the detection precision of software solutions.

Common vulnerability and exposures (CVE) — a list of publicly known cybersecurity vulnerabilities. Each entry (vulnerability) includes an identification number (CVE-ID), a description, and at least one public reference. The CVE system provides a baseline for evaluating an organization's security tools' coverage of vulnerabilities.

Attack techniques to be aware of

Malware

Shorthand for malicious software, malware is an application written with the intent to cause damage to systems, steal data, gain unauthorized access to a network, or wreak havoc. Malware infection is the most common cyberthreat that organizations face. It's often used to steal data for financial purposes, but can also be applied as a weapon in state-orchestrated attacks, as a form of protest by hacktivists, or to test the security posture of a system. Malware is a collective term and refers to a number of malicious software variants, such as trojans, worms, or ransomware.



350,000 new pieces of malware are detected every day

Common types of malware

Virus: The most common form of malware, viruses attach themselves to clean files, replicate, and try to infect other clean files — much like their biological namesake. Viruses must be executed to run, either by an unsuspecting user or by an automated process running the host application. A virus may delete files, cause reboots, join machines to a botnet, or enable remote access to the system via a backdoor.

Worm: Worms get their name from the way they infect systems. Unlike viruses, they don't need a host file or application — instead, they simply infect a system and then self-replicate across other systems through the network, using each consecutive infection to spread further. Worms reside in memory and can replicate hundreds of times, consuming network bandwidth.

Trojan horse: A reference to the story of the Trojan War, where the Greeks hid inside a wooden horse to infiltrate the city of Troy, Trojan horses (or simply Trojans) disguise themselves as a legitimate application or just hide within one. This type of malware acts discretely, opening

security backdoors to give attackers or other malware variants easy access to the system.

Backdoor: Backdoors are a stealthy method of bypassing normal authentication or encryption on a system. They're used for securing remote access to a system, or for obtaining access to privileged information to corrupt or steal it. Backdoors may take many forms: as a standalone program, as a hidden part of another program, as code in the firmware, or as part of the operating system. While some backdoors are secretly installed for malicious purposes, there are deliberate, widely-known backdoors that have legitimate uses, such as providing a way for service providers to restore user passwords.

Ransomware

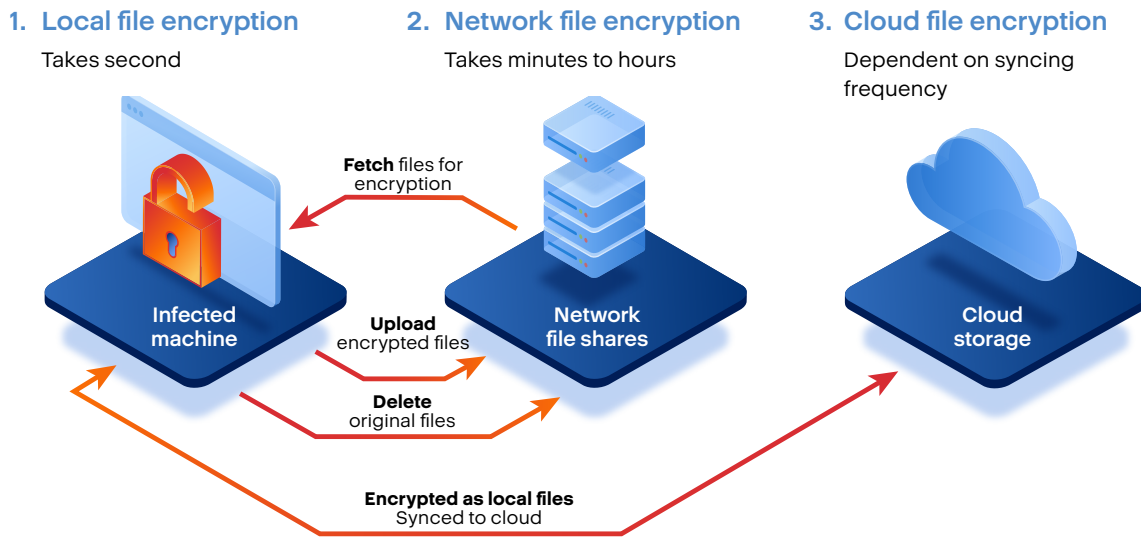
Ransomware is also a form of malware, but one that demands special attention. Originally, ransomware was designed to take control of a system, locking users out until they paid the attackers a ransom in order to restore access. Modern variants of ransomware usually encrypt the user's data, and may even exfiltrate copies off the system to dramatically increase the attackers' leverage over their victims.

Typical ransomware infection flow

Ransomware usually infects users through a distribution campaign in which attackers use techniques such as social engineering or phishing, tricking users to download a dropper that installs the ransomware on the system, e.g. via malicious website. More aggressive ransomware, such as NotPetya, exploits gaps in security to infect systems without the need for trickery.

Once installed, the ransomware finds all files of a specific type locally and across the network, creating a new encryption key and encrypting the files. The original files, recovery points, and backups are deleted to ensure users can't restore the system. Ransomware usually changes the file extension, (e.g. myFile.doc.encrypted) and adds a "help" file explaining how victims can pay the ransom to recover their data.

Ransomware encryption process



Ransomware evolves

58% of victimized companies admit they paid a ransom after an attack



File backups used to be sufficient for guarding against ransomware, but modern variants often target backups and Windows Volume Shadow Copy Service (VSS) snapshots — eliminating victims' ability to recover files from a known good state.

Real-world examples of advanced forms of ransomware include:

Maze is one of the most notorious ransomware families and has impacted numerous businesses and organizations, including Xerox, LG, and the City of Pensacola, Florida. The ransomware is usually distributed via email or by exploiting vulnerabilities, and hinders detection via obfuscation techniques (intentionally making it hard to read). Maze targets not only workstations and servers, but backup repositories as well. In addition to a ransom demand, the threat actors behind the Maze ransomware threaten to leak victims'

corporate data to the public, a tactic that's been adopted by other ransomware attacks.

Conti is the successor of the notorious Ryuk ransomware. The group behind it now also operates a data leak website. Conti is usually distributed through a malicious link that exploits a browser or application vulnerability to breach the network. Rather than being executed automatically, Conti is designed to be controlled by an adversary, running multiple computations at the same time, targeting different assets. Conti disables all Windows services related to security and backup, and deletes volume shadow copies to block common rollback techniques used by cybersecurity providers such as SentinelOne or SonicWall.

Sodinokibi was the third-most dangerous ransomware strain in 2020, based on the number of impacted businesses. Sodinokibi is usually distributed via email containing a malicious link that exploits system vulnerabilities, most commonly an Oracle WebLogic vulnerability ([CVE-2019-2725](#)). The ransomware uses simple code obfuscation techniques to evade detection. Once it infiltrates a machine and encrypts all sensitive files, the ransomware targets and deletes volume shadow copies and backup folders, making the recovery process harder.

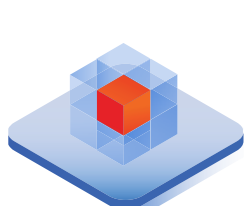
DoppelPaymer is another advanced ransomware family that uses a wide variety of distribution methods — from malicious COVID-19-related emails, to system exploits and infected versions of legitimate installers. DoppelPaymer's victims include both businesses and government organizations, such as NASA contractors, the government network of Torrance, California, and a state-owned oil company in Mexico. In a tactic shared with other cybercriminals, the actors behind this ransomware release stolen data publicly on their website and through social media. Much like Conti and Sodinokibi, DoppelPaymer deletes shadow copies of files and attempts to encrypt or delete backups.

Phishing

Phishing is a common attack technique that utilizes deceptive communications (including email, instant messages, SMS, and websites) from a seemingly-reputable source in order to gain access to sensitive information. The attacker impersonates a trustworthy organization, such as a bank, government institution, or legitimate business. The goal is to take advantage of the user's trust and trick them into clicking a malicious link, downloading a malicious attachment (malware), or disclosing confidential information such as personally-identifiable information (PII), financial information, or user credentials. As an example, a phishing attack might look like a legitimate email for renewing your Microsoft 365 subscription, but actually contain an embedded link that takes you to a malicious page disguised as a Microsoft 365 renewal page — the goal being to steal your credentials or credit card information.

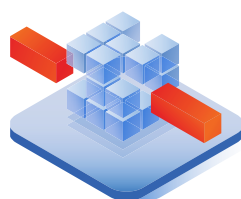
How a drive-by attack happens

User browses legitimate website which has been hijacked



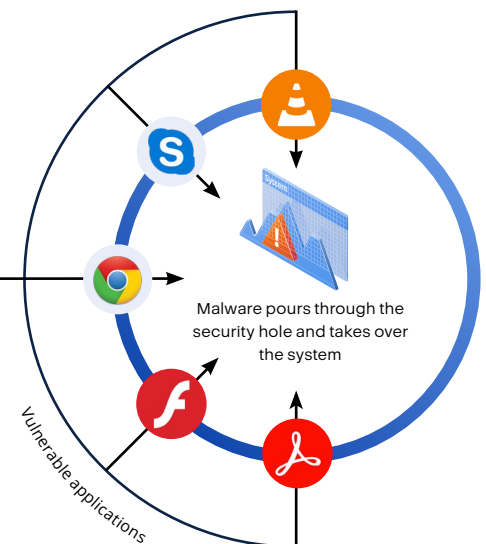
Embedded malicious elements

Automatically downloads to PC
Probes the system for vulnerabilities



Exploit kit

Malware



Spear phishing

95% of all attacks on enterprise networks are the result of successful spear phishing

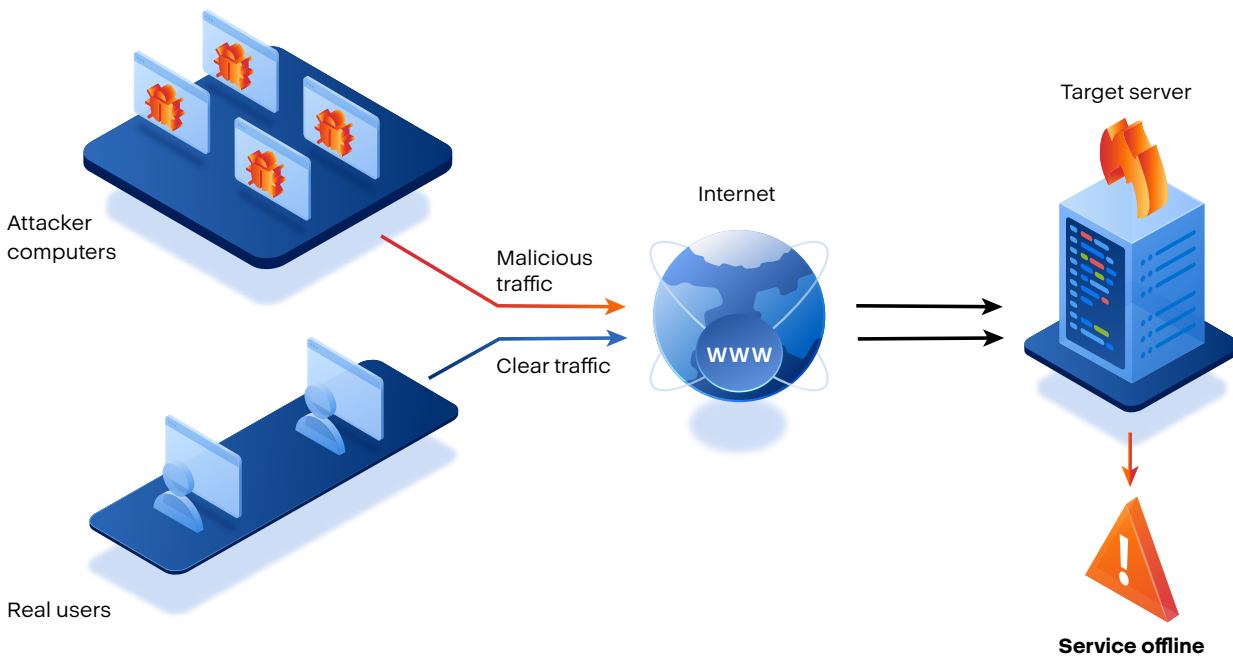


Spear phishing is a form of phishing that targets a specific victim who have been researched using insider knowledge or publicly available information (e.g. social media). These attacks tend to be quite convincing, as they're highly-personalized — often involving real names and roles within the company. For example, an attack might be disguised as an email from a user's direct manager or IT support department. Such malicious techniques are hard to recognize unless detected by cybersecurity products.

Drive-by downloads

As the name suggests, drive-by download attacks take advantage of a website's security flows due to improper configurations or missed patches. They inject a malicious script that exploits a vulnerability in a web browser, application, or operating system to download malware onto the victim's device. The malicious code is usually obfuscated to avoid detection. These attacks are especially dangerous because they don't require consent or user action — they are automatically triggered when a user visits a page. Even legitimate websites may be compromised in this way.

Distributed denial-of-service (DDoS) attack chain



Distributed denial-of-service (DDoS) attacks

Distributed denial-of-service attacks target servers, services, or networks in order to disrupt the traffic, preventing access for legitimate users. DDoS attacks are most commonly intended to cause financial or reputational damage to an organization or government body.

Such attacks usually utilize large networks of malware-infected systems (computers and IoT devices) that the attacker controls. Such individual devices are commonly referred to as “bots” (or zombies), and a collection of them is known as a “botnet”.

Attackers use these botnets against servers or networks, having each bot send requests to the target’s IP address simultaneously, overloading the server or network to make it unavailable to normal traffic. Remediation is usually difficult as the bots are legitimate devices, making it hard to separate attackers from normal traffic.

Advanced persistent threats (APT)

Advanced persistent threats are complex attacks intended to establish an illicit, long-term presence in a network in order to collect highly-sensitive data or compromise an organization’s operability.

How are APT attacks carried out?

Most commonly used cybercrime techniques are intended to compromise web assets, network resources or authorized users, establishing a foothold in the targeted network. As such cyberthreats are faced by organizations on a regular basis, ATP attacks are known to use DDoS attacks simultaneously with other techniques as a means of weakening the security mechanisms — and as a smoke screen for distracting IT personnel. Once assets are compromised, the perpetrators install malware (backdoor shell) that grants network access and enables remote, stealthy operations.

Once access is established, the attackers expand their reach, compromising users with access to critical data such as financial records, trade secrets, product line information, and employees’ and customers’ PII. These capabilities enable the attackers to extract and sell sensitive data, or to sabotage the organization from inside, causing maximum havoc.

With APT attacks, stolen information is often stored in a secure location inside the compromised network. In order to extract the collected data without being detected, the attackers may again use DDoS attacks or other techniques to create white noise and distract IT personnel.

Differences with other web threats

Compared to traditional web application threats, APT attacks:

- Are costlier and more complex.
- Utilize numerous attack techniques.
- Are manually executed (usually by a group of cybercriminals).
- Don't use hit-and-run tactics — their goal is to remain unnoticed in the network for as long as possible.
- Aim to infiltrate an entire network, rather than a localized part of it.

Zero-day exploits



Zero-day exploits refer to a vulnerability that is actively being exploited in the wild, but is not yet known to the software provider — thus, a patch to fix the exploit is unavailable. Security administrators have “zero days” to eliminate the vulnerability. Eventually, all vulnerabilities become known and security patches can remediate the risk they pose, but this process may take months or even years. Zero-day exploits pose a significant threat to businesses, as they're quite hard to detect — doing so requires deep system knowledge and constant monitoring of all applications.

Fileless attacks



As the name suggests, fileless attacks are carried out without malicious files on disk. Instead, the threats reside only in random access memory (RAM), leveraging applications and processes known to be “safe” in order to collect data, deliver malicious executables, or gain unauthorized system access. The infection leaves no traces on the target hard drive, nor even in RAM after a system reboot. The nature of these attacks makes them especially difficult to detect without advanced cybersecurity solutions that employ multiple layers of defense, working together cohesively. According to the Ponemon Institute, fileless attacks are [10 times more successful](#) than file-based ones.

Data leakage



Security breaches can lead to the unauthorized transmission of data to an external environment, or to unauthorized parties within the organization. Data leakage is primarily an insider threat, most often resulting from internal actors who provide third parties with unsanctioned access to sensitive data — either deliberately, or due to negligence or mistakes in data handling. Information can be leaked both electronically — through network communications such as email, instant messengers, or social media — and physically, through peripheral devices such as USB drives or printers.

When intentional, such security breaches are usually performed for financial gain, with culprits aiming to steal highly-sensitive data such as trade secrets, cardholder data, or PII. This can lead to severe financial and reputation damage to businesses, and subsequent regulatory fines.

Protecting your business

Antivirus software

Antivirus software, or anti-malware, is a type of computer program that detects and removes malicious applications. Once installed, the software usually runs in the background, providing real-time protection against viruses, trojans, worms, and other malware. Most antivirus solutions support both automatic and manual scanning. Automatic scans may inspect downloaded files, external storage devices, and files created by software installers. Automatic scans of the entire hard drive are usually performed on a scheduled basis, while manual scan capabilities allow users to scan specific files or the whole system whenever they deem it necessary.

Signature-based detection

Signature-based detection has been used since the earliest days in security monitoring, when intrusion detection systems (IDS) relied heavily on it. In cybersecurity, attacks leave a footprint or pattern associated with them on the system or network. Signature-based solutions store a repository of static signatures, known as virus definitions, associated with known malware variants. When a scan is performed, the anti-malware solution creates a signature for each file, comparing it with the virus definitions in its repository. If a match is found, the file is qualified as a threat and is blocked or deleted.

Although signature-based detection is fast and accurate, it relies on known patterns, which means it's reactive. If a new, unknown malware variant infects the machine or network, signature-based detection methods won't

catch it. Moreover, malware variants with obfuscated code can't be detected because their signatures are also masked.

Hackers are very successful against signature-based detection due to:

- **Malware cryptors** — tools can obfuscate the code of malicious software in order to make it undetectable by signature-based scanners.
- **Managed malware crypting services** — malware-as-a-service is easily accessed, allowing attackers to obtain malware without building their own.
- **Polymorphic malware** — some types of malware constantly change their identifiable features to evade detection.
- **QA processes in cybercrime** — cybercriminals usually test malware against commonly-used antivirus solutions to ensure that it's not easily detectable. Automated testing is offered as a service among cybercriminals.

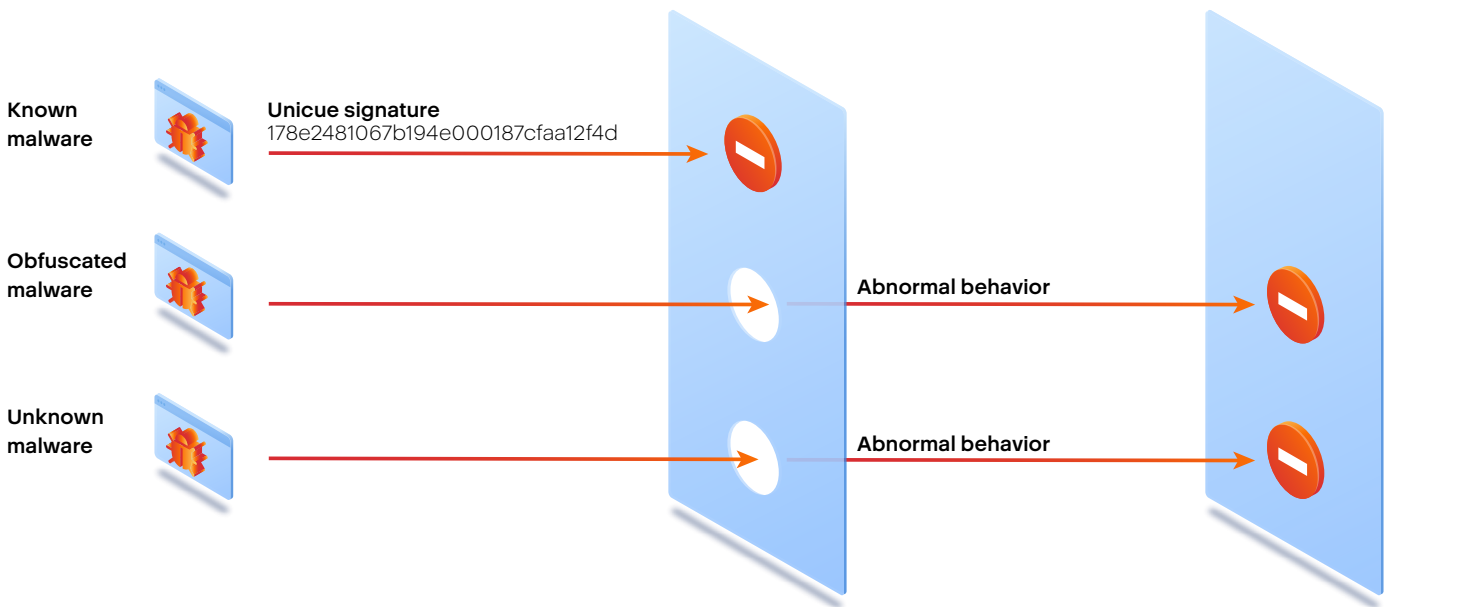
90% of malware showing defense evasive behavior



While signature-based detection serves as a fundamental basis for anti-malware protection due to its accuracy and speed, it requires continuous updates to the virus definition repository.



Malware attack



Behavioral-based detection

On the other hand, behavioral-based detection uses heuristics that are more generic, or fuzzy signatures that can catch variants. Behavior-based detection doesn't look for unique characteristics of a threat, but rather for environmental factors that signal its presence. Think of it this way, signature-based detection is like testing a blood sample to see if the patient is infected with a specific virus or bacteria, while behavior-based detection is like observing a patient's symptoms to determine whether they are ill.

Behavior-based detection is a more complex technique and often relies on artificial intelligence (AI) or machine learning (ML). It requires a holistic view over all processes to determine which ones may be a threat. A program that attempts to gain escalated privileges, for example, may indicate a threat.

Although it's quite efficient in catching sophisticated or unknown threats, behavioral analysis can be prone to false positives. Additional context can help sort these out, but false positives do increase security management efforts. Furthermore, behavioral analysis can be resource-intensive. To better understand an antivirus solution's performance with regards to detection rate, false positives, and impact on system performance, you

can refer to independent tests conducted by certified testing laboratories such as AV-TEST, AV-Comparatives, or ICSA Labs.

Allowlisting and denylisting

Anti-malware products usually have the capability to explicitly allow applications, devices, and users to access a particular privilege or service ("allowlisting"), or to explicitly block the access of certain assets ("denylisting"). Denylisting usually serves as a generic rule for unauthorized applications that are known to pose a threat, while allowlisting can reduce false positives by excluding apps or files that are known to be legitimate from detection rules. [NIST](#) recommends using allowlists and denylists in high-risk security environments, but it's also useful in environments that must comply with strict regulatory requirements.

Traditional antivirus solutions don't protect data

Although anti-malware products are responsible for preventing, detecting, and removing malware, they usually don't have built-in data protection capabilities. This means that in the event of a successful security breach where files are infected and corporate data is encrypted or deleted, traditional antivirus solutions can't aid in recovering the affected data.

Moreover, anti-malware solutions usually do not remediate present vulnerabilities (both known and unknown), which continue to serve as an easily exploitable attack vector for cybercriminals. Unpatched vulnerabilities can result in malware evading detection.

Running two antivirus solutions at the same time

Though it may not seem intuitive at first glance, having two antivirus solutions doesn't increase your security — and is usually not a good idea. Doing so can lead to one product identifying the other as a virus (false positive) or, if malware is detected, one product may quarantine it while the other tries to remove the quarantine and sends recurring alerts about the already contained threat. Running two anti-malware solutions also drastically increases memory consumption. In more extreme cases, it can lead to file corruption or system crashes.

Anti-ransomware

Ransomware to target someone every 11 seconds by 2021



Anti-ransomware software specifically detects and deletes ransomware. While anti-malware solutions can usually detect many forms of ransomware, anti-ransomware tools differ in their ability to stop ransomware once it has executed and to revert any changes made, such as file encryption.

To revert changes and rollback the system and files to a known good state, anti-ransomware products usually rely on backups or shadow copies to restore clean data. More advanced ransomware variants, however, target and delete or encrypt backups and shadow copies, making recovery almost impossible. To guarantee protection, anti-ransomware solutions must also safeguard the repository they're using to recover clean files in the event of a breach.

Backup and recovery

One of the best ways to protect your data is to back it up. Copying your data to external storage (whether in the cloud or on-premises) lets you recover your systems

if any malware manages to get past your defenses. Backups may also be useful in the event that a patch renders the system unstable.

The 3-2-1 backup rule



There's a well-known rule in the backup industry to ensure efficient data protection: Keep three copies of your data (one as production data, and two as backups), stored on two different locations (e.g. on disk and on tape), with one copy off-site (e.g. in cloud storage) for disaster recovery.

Traditional backups are not secure

Traditional backups are not truly secure, as they're vulnerable to attacks, breaches, and modifications. This could lead to backup data being deleted, encrypted, or infected with malware. In the event that both your systems and backups are compromised, you won't be able to restore your environment. Many security-oriented backup solutions have built-in self-defenses, while more advanced anti-malware products may offer the ability to scan backups for malware.

Another flaw of traditional backups is that they're usually performed on a schedule. If a file is corrupted between backups, you'll only be able to recover it to the state of the most recent backup, which could be days or even weeks earlier. Advanced backup products feature the capability to back up changes to critical files on a continuous basis, ensuring a more efficient recovery without data loss.

Backups and forensics

Some advanced cybersecurity solutions offer the ability to collect environmental data during malware attacks for later use in forensics investigations, or as evidence in court. Well-protected backups are ideal for storing forensics data, ensuring easy access, sufficient storage capacity, and safety.

Patch management

Only 15% of companies report to have an effective patch management process in place



Software solutions often have millions of lines of code. Companies try their best to test their solutions before release, but bugs and vulnerabilities are commonly found afterwards. To fix these issues, companies release patches (code changes that fix bugs and other issues) or hotfixes (which fix very concrete bug/issue, not always publicly released).

Patch management is the process of helping users to identify, download, install, and verify patches, to ensure systems and applications stay up to date and therefore secure. This can all be quite rigorous and time-consuming for IT administrators, but automated solutions make it much easier.

Why is patching so important?

Keeping business-critical applications and operating systems up-to-date increases the overall security posture and strengthens the operational capabilities of an organization by fixing bugs, issues, and vulnerabilities in software solutions.

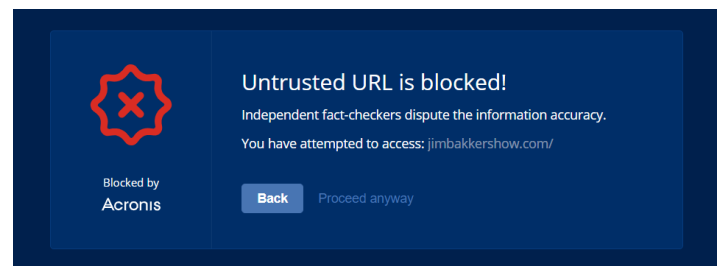
57% of data breaches are directly attributed to attackers exploiting a known unpatched vulnerability



Patches are frequently issued for popular applications as a preventive measure against cyber breaches. However, with the mean time to patch (MTTP) being 102 days ([according to the Ponemon Institute](#)), organizations may be underestimating how vulnerable unpatched systems are against cyberattacks. One example is the case of the notorious WannaCry ransomware, which exploited

a Windows vulnerability and spread across more than 150 countries, causing \$4 billion in losses while crippling hospitals and national mobile companies. A patch to fix this exploit was released by Microsoft two months prior to the beginning of the attacks, yet countless systems remained unpatched and unprotected.

URL filtering



URL filtering, similar to blocklisting, is a technology that blocks access to known malicious websites. It is mainly used to prevent users from reaching:

- Phishing websites that try to steal credentials
- Websites that operate as command-and-control servers (C&C), sending instructions to — or receiving data from — systems compromised by malware
- Websites that download malware
- Fake e-commerce shops that may steal money or cardholder data

In strictly regulated or high-risk environments, it's a good practice to also block URLs that aren't explicitly malicious but do pose a potential threat, such as fake news websites or social media platforms.

Firewalls



Firewalls have served as a first line of defense for over 20 years. They act as a security barrier between internal networks and external ones — such as the internet

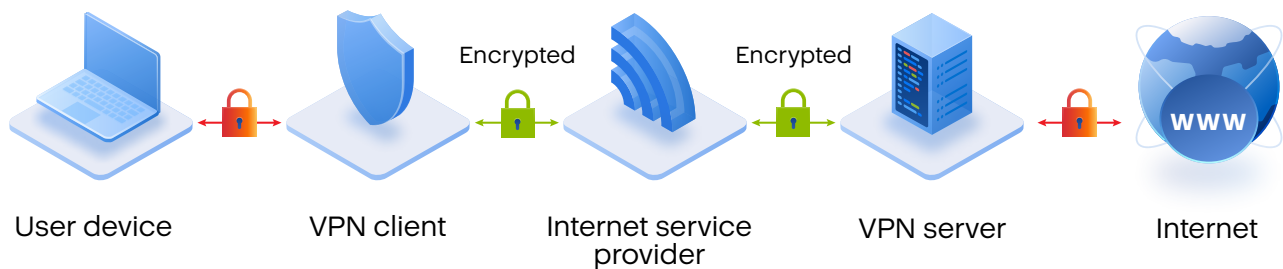
— by monitoring incoming and outgoing traffic, and blocking risky or malicious actions based on a predetermined set of security rules. Firewalls may be software, hardware, or virtual appliances.

Virtual private networks (VPN)

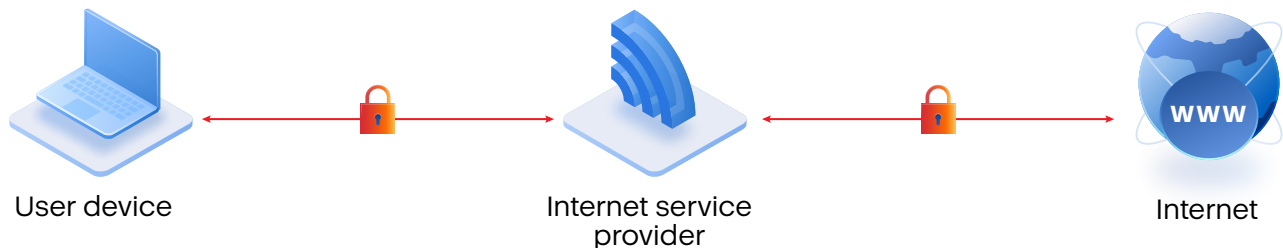
Surfing the web usually leaves traces that are easily associated with your internet protocol (IP) address — a unique set of digits that identifies your device. This is especially dangerous when connected to public or unprotected Wi-Fi networks, as any data transmitted through your online sessions (including browsing history, PII, and location info) could be eavesdropped upon by cybercriminals who've managed to gain escalated privileged access to the network.

A VPN serves as a secure gateway that connects your device to another server on the internet, allowing you to browse safely by using the server's IP address instead of your own. VPNs also create a security tunnel between your device and the server, encrypting all traffic between them.

VPN



Without VPN



Data loss prevention (DLP)

Data loss prevention (DLP), also known as data leakage prevention, is a technique that protects sensitive corporate data from leaving the company due to user negligence, mishandling of data, or malicious intent. DLP technologies enforce data handling policies by allowing or blocking data access and transfer operations based on a set of predefined security rules.

Context- and content-aware controls

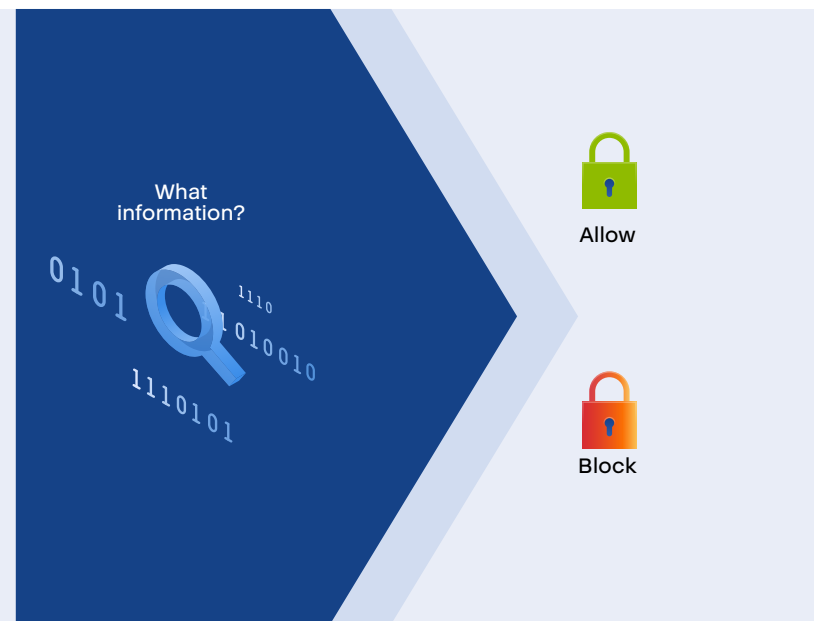
DLP solutions allow or block data access and transfer operations, generally based on two different types of controls:

- **Context-aware controls** allow you to control data operations based on the operations' context (environmental factors) — attributes such as involved users, channels used, type of accessed/transferred data, flow direction, or date and time.
- **Content-aware controls** allow you to control operations based on the actual information (content) that is being accessed or transferred.

Context-aware controls



Content-aware controls

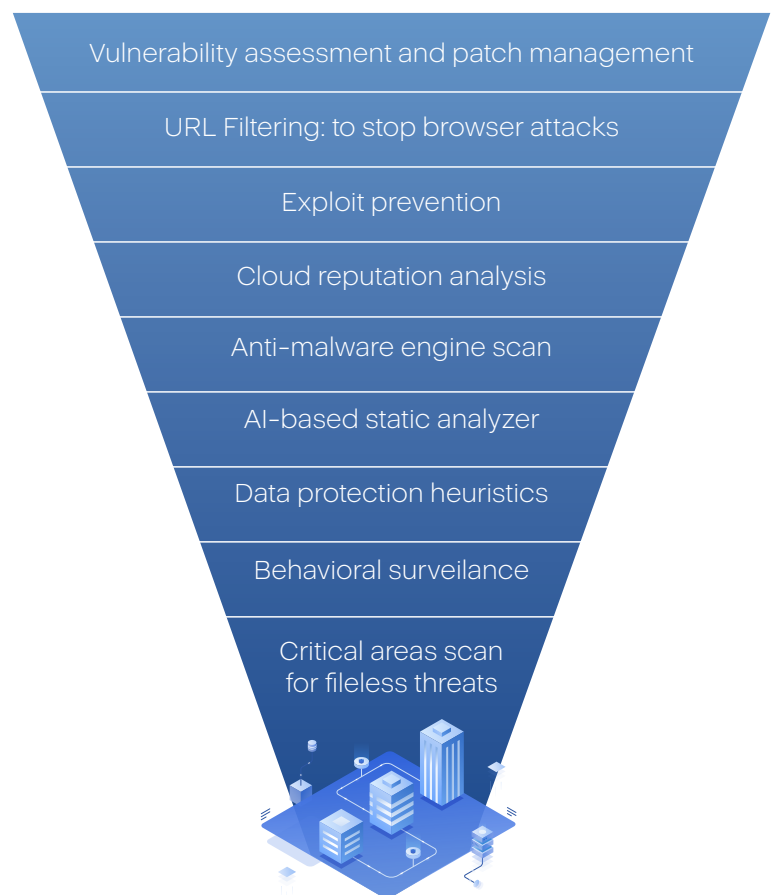


Channels you need to control

Data can leave the company through two main groups of channels — local (e.g. peripheral devices, printers, and USB drives) and network-based (e.g. emails, web, and social media). Although some DLP solutions monitor only network communication, it is best to monitor both local and network channels to ensure efficient data loss prevention.

Multilayered security (defense in depth)

The term “defense in depth” (DiD) originates from the medieval military tactic of layering castle defenses. Also known as multilayered security, DiD is a comprehensive cybersecurity strategy approach based on the notion that no security tool or component provides a universal defense against any threat. On the contrary, DiD is all about implementing a series of security measures, each protecting against a different attack vector and covering the flaws of other measures. Advanced cybersecurity solutions employ this multilayered approach to guarantee more comprehensive protection.



About Acronis

Acronis is a frontier in cyber protection, driven by the passion to protect every workload. We've created the only all-in-one cyber protection solution for environments of any size – and solved the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern world.

With our unique combination of automation and integration, you gain all of the prevention, detection, response, recovery, and forensics capabilities needed to safeguard all of your workloads while streamlining your protection efforts.

Cyber protection is complicated, let's do it together

Contact us to learn how we can proactively protect you against today's advanced and emerging threats.

CONTACT US

