Bitdefender®

Cyber Risk Management

Many experts say that data, and not gold or oil, has become the most valuable commodity in the world in recent years. As the value of data increases, cyber-attacks become a threat that business leaders have no choice but to place at the top of their priority list.

SUMMARY

1. General context

Many experts say that data, and not gold or oil, has become the most valuable commodity in the world in recent years, and this makes companies dealing with data a serious target for cyber criminals. As the value of data increases, cyber-attacks become a threat that business leaders have no choice but to place at the top of their priority list. Five years ago, professionals working in cyber security field were making efforts to gain the attention and support of companies' senior management, but their visibility has increased in the last two or three years due to issues related to cyber risk management, and several eye-opening cases.

We do more and more of our business online. At the same time, it has become easier than ever for cyber criminals to find ways to spread malware or exfiltrate data from companies. As they understand the value of the data organizations hold, the number and impact of data breaches is increasing all over the world.

.Businesses' increasing dependence on IT goes hand in hand with the increase in cybercrime

a. Notorious breaches of 2017

High-profile cyber attacks with significant consequences are a constant presence in the mainstream media. In 2017, hacks made headlines around the world.

In 2017, the world saw more data breaches than in any other year, compromising more than 174 million records, announced the Identity Theft Resource Center on December 20. That's 45% more breaches than in 2016. And the trend is expected to continue in 2018

APRIL
Leaked government tools

An anonymous group called the Shadow Brokers leaked hacking tools developed by the US National Security Agency, allowing hackers to compromise a variety of Windows servers and OSes. Some of these tools were later used by cybercriminals to spread WannaCry, BadRabbit and Petya malware.

MAY
WannaCry (ransomware)

WannaCry took control of hundreds of thousands of businesses running outdated Windows software and locked down computer systems. Numerous industries, including health care and car companies, were hit in more than 150 countries.

JUNE
NotPetya (malware)

The computer virus NotPetya targeted Ukrainian businesses using compromised tax software, and spread to major global businesses such as FedEx, British advertising agency WPP, Russian oil and gas giant Rosneft and Danish shipping company Maersk.

JULY
Equifax (Credit bureau)

Cybercriminals exfiltrated the personal data of 145 million people, including social security numbers – this means almost half of the US population. Because of the sensitive nature of the information hacked, it's considered the worst corporate data breach ever.

AUGUST
Taringa (Latin America's largest social media network)

A massive data breach that leaked login details involved 28 million accounts.

OCTOBER
Yahoo (web services provider)

Parent company Verizon revealed that in 2013 every one of Yahoo's 3 billion accounts (e-mails, passwords) was hacked.

Bad Rabbit (ransomware)

It infiltrated computers by posing as an Adobe Flash installer on news and media websites that hackers had compromised.

NOVEMBER
Uber (transportation network company)

Uber's CEO announced that in 2016 attackers stole data of 57 million users around the world and information for 600,000 drivers. He also revealed that Uber paid hackers off to hide the massive data breach.

b. Data breach cost impact

Data breaches cause enormous disruption and cost companies millions of dollars. FedEx attributed a $300 million loss to the NotPetya attack, and its subsidiary TNT Express had to suspend business. The NotPetya ransomware impacted thousands of networks and led to hundreds of millions of dollars in damage. Equifax lost over 30% of its market capitalization value, or about $5 billion. Yahoo sold itself to Verizon for $4.48 billion, $350 million being cut from Verizon's original offer after the disclosure of the 2013 breach and the following massive data loss scandal.

Ponemon Institute's 2017 Cost of Data Breach Study puts the average total cost of data breach for the 419 companies from 11 countries and two regions participating in the research at $3.62 million, and the average cost for each lost or stolen record containing sensitive information at $141. The average organizational cost of data breach varies by country. Organizations in the US had the highest total average cost last year, at $7.3 million, and companies in Brazil had the lowest, at $1.52 million.

Also, a Bitdefender analysis found ransomware payments hit $2 billion in 2017, twice as much as in 2016.

This type of consequences brings the cyber risk issue to the top of senior executives' minds all over the world.

c. See the numbers

To better understand the amplitude of this phenomenon, we should analyze the numbers.

The 10 biggest data breaches of the 21st century, the vast majority of which occurred in the last 5 years, affected over 4 billion people (with some overlap). The top 3 include the 2014 eBay case, when hackers gained access to 145 million customers, the 2016 Adult Friend Finder breach, with more than 412 million user accounts exposed, and the 2013 (revealed in 2017) Yahoo epic data breach, when all 3 billion of its user accounts, including email addresses, passwords, but not financial information, were impacted.

The cost of cybercrime globally is estimated to grow from $450 billion in 2016 to $2,000 billion (2 trillion) in 2019. For comparison, the US GDP is about $20 trillion. (Juniper Research, Cost of Cybercrime)

Over 5 million data records are lost or stolen every day worldwide, which means 58 records every second, according to the Breach Level Index.

Cyberattacks are ranked third in terms of likelihood (right after natural disasters), and sixth in terms of impact (between water and food crises), according to the Global Risk Report for 2018 released by the World Economic Forum.

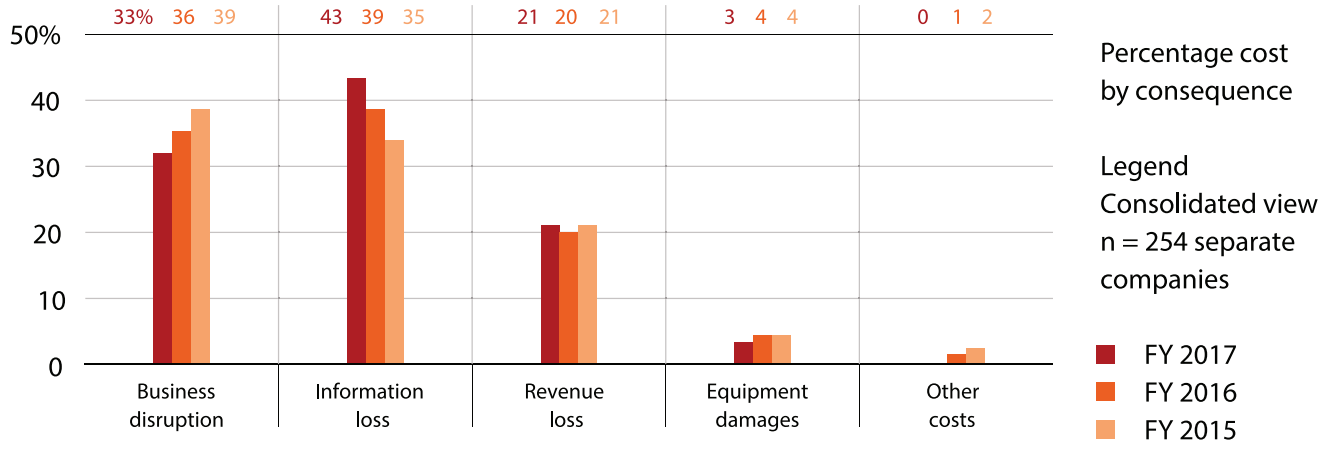
These numbers show that, due to the digital economy going mainstream, the rules of the game are changing and cyber risk is here to stay. And to grow. The magnitude of cyber threats is well recognized by business decision makers, and it's no wonder that a global cyber risk perception survey conducted by insurance broker Marsh concludes that 65% of executives viewed cyber risk as a Top 5 risk affecting businesses.

2. GDPR, a European rule with global impact

In this context, the European Union initiated the new General Data Protection Regulation (GDPR), which is the most important change on data privacy regulation in the last 20 years. The official site of the GDPR highlights that the regulation is designed to harmonize data privacy laws across Europe, to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is considerably different from the time in which the 1995 directive was set up, and also aims to reshape the way organizations across the region approach data privacy. The GDPR applies to all companies processing and holding the personal data of citizens residing in the Union, regardless of the company's location.

Personal data is considered any information that can be used to directly or indirectly (by cumulation or correlation) identify a person – name, e-mail address, bank details, medical information, computer IP address, posts on social media etc.
The GDPR becomes enforceable on 25 May 2018, after a two-year transition period.

Every entity that processes personal data must ensure it is properly safeguarded against loss, theft, unauthorized access, etc. The GDPR includes a personal data breach notification rule that states that a personal data breach must be reported to the regulator within 72 hours of it being identified. And if the security breach is likely to result in a high privacy risk for individuals, they should also be informed of the breach.
The GDPR imposes stiff fines on data controllers and processors for non-compliance, determined considering the nature of infringement, volume and type of affected data, preventive measures implemented, instruments and processes that help limit the consequences of the breach. With the appropriate compliance procedures in place, companies can prevent personal data breaches, avoid fines (up to EUR 20 million or 4% of global turnover) and reputational damage, and demonstrate trustworthiness and responsibility to customers.



Accenture, "2017 Cost of Cyber Crime Study"

3. How to address cyber risk management in a GDPR-consistent manner

GDPR will raise the bar for cybersecurity controls because of its potential impact on an organization. Businesses could face regulatory administrative penalties on one side, and class actions brought about by individuals on the other. So GDPR becomes a central norm of data management best practice in terms of ensuring the safety of sensitive data.
But how can organizations manage cyber risk exposure, an important component of GDPR readiness?

The ability to demonstrate due diligence in evaluating what risks the personal data is exposed to, and to defend your decisions in terms of risk mitigation (including cyber risks) is key to defending the organization in situations of audits or lawsuits.

To prepare for GDPR, a detailed and structured approach is required. Of great help are frameworks such as The National Institute of Standards and Technology Framework (NIST) Cybersecurity Framework, which contains a dedicated chapter for Risk Assessment. According to NIST, the goal of a risk assessment is for an organization to understand "the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."

A risk assessment typically involves 6 steps:

- Identify and document asset vulnerabilities
- Identify and document internal and external threats
- Acquire threat and vulnerability information from external sources
- Identify potential business impacts and likelihoods
- Determine enterprise risk by reviewing threats, vulnerabilities, likelihoods and impacts
- Identify and prioritize risk responses

This process needs to cover the entire IT environment and, depending on the size of the organization and the complexity of the environment, a risk assessment including a review of the collected data can take from 7 days to 1-2 months.

One source of vulnerabilities for enterprises is the applications environment – more specifically, the unpatched, vulnerable software applications.

4. Software application vulnerabilities – key vectors of cyber attacks

In a 2017 report on the Threat Landscape published by the European Union Agency for Network and Information Security in January 2018, the 2nd and 3rd places are occupied by threat categories directly linked to the application environment: web-based attacks and web application attacks. Web-based attacks are those that make use of web-enabled systems and services such as browsers (and their extensions), websites (including Content Management Systems), and the IT-components of web services and web applications. Web application attacks are directed against available web applications, web services, and mobile apps. This type of attack is very popular, and is expected to stay so because web apps and web services used are usually exposed and openly accessible.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	☒
2. Web based attacks	↑	2. Web based attacks	↑	☒
3. Web application attacks	↑	3. Web application attacks	↑	☒
4. Denial of service	↑	4. Phishing	↑	☒
5. Botnets	↑	5. Spam	↑	☒
6. Phishing	→	6. Denial of service	↑	☒
7. Spam	↓	7. Ransomware	↑	☒
8. Ransomware	→	8. Botnets	↑	☒
9. Insider threat	→	9. Insider threat	→	☒
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	☒
11. Exploit kits	↑	11. Data breaches	↑	☒
12. Data breaches	↑	12. Identity theft	↑	☒
13. Identity theft	↓	13. Information leakage	↑	☒
14. Information leakage	↑	14. Exploit kits	↓	☒
15. Cyber espionage	↓	15. Cyber espionage	↑	☒

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ☒ Going up, ☒ Same, ☒

Agency for Network and Information Security, Threat Landscape

Data generated by the US National Vulnerability Databases show the evolutions of vulnerabilities since 2010, with a record in 2017 of 14,000 vulnerabilities meeting specified limitations. These are known vulnerabilities and, according to Gartner, will represent 99% of the vulnerabilities exploited by 2020.

In other words, zero-day vulnerabilities and attacks are over-rated, statistically speaking. An organization is 100 times more likely to face a cyber attack based on a known vulnerability, than a zero-day cyber attack. This means the vast majority of cyber breaches are entirely preventable. And, in these situations, authorities enforcing GDPR will probably go for higher penalties. It will be much easier to escape penalties in a zero-day attack leading to data loss, than in situations where the vulnerability was known, but remediation action was not taken to prevent a breach.

This was the case of Equifax. The vulnerability for the Apache Struts application was known and the patch was available about 3 months prior to the attack. Equifax belonged to a vast category of enterprises that fall behind with patching application by more than 30 days. Companies frequently fail to patch security flaws in a timely manner and it's quite common to see delays of even longer than 3 months. In many cases, the delay is not due to the organization's lack of care, but to other reasons:

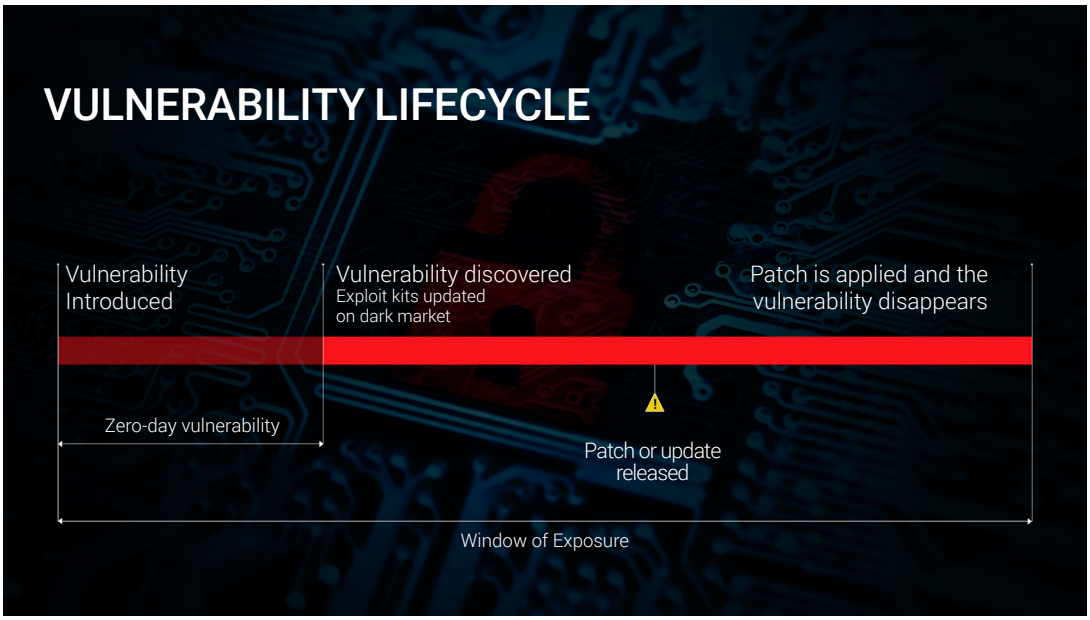
- People in IT operations (that typically handle the patch management process) are overloaded

- Small organizations lack automation tools for delivering patches

- In larger organizations, patching is not a straight-through process. An unfortunate patched deployed across the entire organization can hamper operations for hours or days. In some organizations, IT ops are required by processes and procedures to test each patch before deploying it to production systems.

So how can organizations, large and small, manage vulnerabilities and reduce their exposure to attacks?
To better understand how to manage software vulnerabilities and reduce cyber risk exposure, a good place to start is to analyze the vulnerability lifecycle.

It starts with a vulnerability being introduced together with software (app or OS), or a software update. At first, the vulnerability is unknown to the public; it's a weakness waiting to be discovered and an exploit to be created. If all this occurs under the radar and an attacker uses the exploit kit against an organization before the vulnerability is made public, the respective entity faces a zero-day attack. After the vulnerability is discovered and made public, the vendor starts working and releases a security patch. From patch release to patch installation there is usually a span of 30 days. With the patch application, the window of exposure is closed, as the vulnerability disappears.



Analyzing this lifecycle, we can identify two distinct phases: before and after the release of the patch.

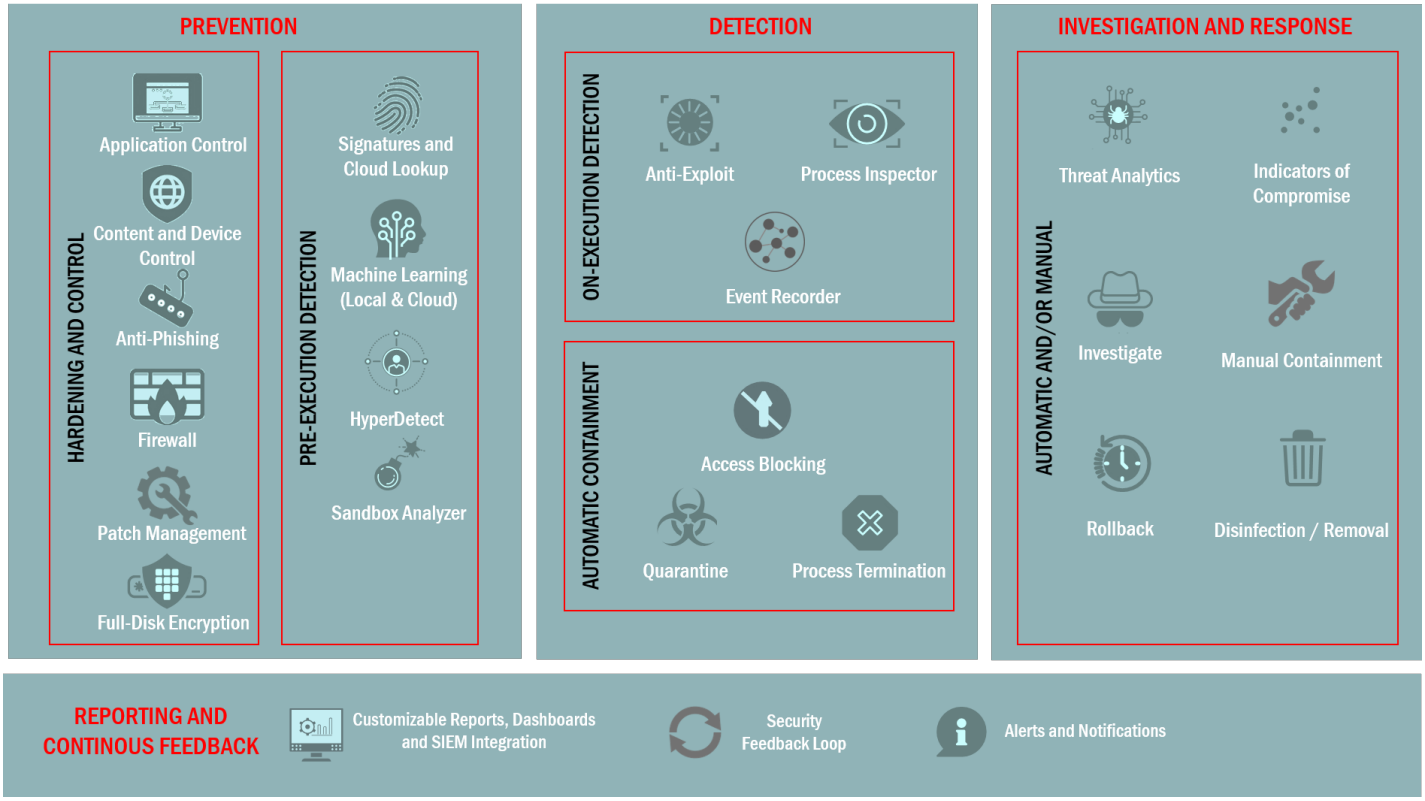
Bitdefender provides different tools and approaches to reduce the risk of cyberattack for each phase, while our integrated Endpoint Security Solution covers both phases.

5. How to keep the risk of zero-day attacks at bay with Bitdefender Endpoint Security Solution

Bitdefender Endpoint Security Solution is based on a layered next-generation defense architecture, consisting of multiple layers that work together to protect the endpoints against the entire spectrum of attacks, and targets each phase of a cyber attack. The mechanisms are grouped on several categories: prevention, detection, investigation & response, report & continuous feedback.

This layered approach is highly effective in protecting the endpoint infrastructure against both known and entirely new, zero-days attacks. Independent industry testing and real-life attacks have demonstrated its effectiveness – during the WannaCry wave, all Bitdefender customers, with patched or unpatched software, were fully protected and none was affected.

The layered next-gen protection is the solution that Bitdefender recommends to protect against unknown, zero-days cyber attacks. It provides a blanket to protect personal data and avoid GDPR consequences.



6. How to Employ the Patch Management Module

If layered next-gen defense refers to how Bitdefender protects organizations against the unknown malware, Patch Management is a module that helps manage cyber risk exposure to known vulnerabilities, and helps organizations remain compliant with GDPR requirements.

The Patch Management Module, fully integrated into Bitdefender GravityZone, enables organizations to keep systems up to date across the entire Windows install base. GravityZone Patch Management administers software updates for Windows operating systems and the largest collection of software applications in the market. The patching module delivers updates for the entire fleet of workstations, physical servers or virtual servers.

Bitdefender Patch Management Module helps organizations get ready for GDPR by managing cyber risk exposure in 4 simple steps, listed below. As a prerequisite, all endpoints need the Bitdefender Endpoint Security agent installed and centrally managed from a cloud/on-premise Bitdefender GravityZone console.

1. Assess current endpoint software vulnerabilities
2. (Optional) Acquire threat and vulnerability information from external sources
3. Automate security patch application
4. Use reporting to prepare for GDPR related audits and incident documentation

Current endpoint software vulnerabilities can be assessed by running a patch inventory assessment on the endpoint infrastructure. Although it seems resource intensive, it's remarkably fast and low in resource utilization. Out of the assessment, the organization gets a report displaying all endpoints and the number of security patches missing on the endpoint. There are two main options to display the missing patches.

The security administrators can first use the endpoint-level view, which is useful in managing patches for specific endpoints but is not very effective at managing a large infrastructure. For this, the module also provides a view of all patches missing at infrastructure level. Both views enable administrators to get additional information about missing patches. Each security patch typically covers one or multiple vulnerabilities, documented in the Common Vulnerabilities and Exposures database. The patches can be installed on demand but, for operational effectiveness, the patch scan and patch installation can be done automatically. There are options allowing the administrators to configure patches issued by trusted vendors only to be installed automatically as well as separating security patches from non-security patches.

Applying patches ensures that the software's known vulnerabilities are eliminated fast and effectively, to mitigate cyber risk and keep personal data safe. But 100% security is not economically feasible. Cyber incidents will happen, and enterprises need to be prepared for GDPR incidents and audits. To demonstrate that preventive security was in place and properly functioning, Reports are mandatory. Bitdefender Patch Management Reports enables organizations to extract and save reports periodically, showing the current patch inventory (known vulnerabilities) and the status of patch installation across the endpoint environment. Using these reports, companies will be able to show their due diligence efforts, using all the available information on known software vulnerability, to protect the personal data information stored on its endpoint infrastructure.

The Bitdefender GravityZone console can provide much more information on the security status of protected endpoints. This information can further be used proactively in forensics and documentation efforts necessary for Cyber Incident Management, another topic relevant to GDPR readiness.

BD-NGZ-Apr-27-2018-11-ar
Bitdefender-2018-Whitepaper-CHM-creation1122-A4-en_En