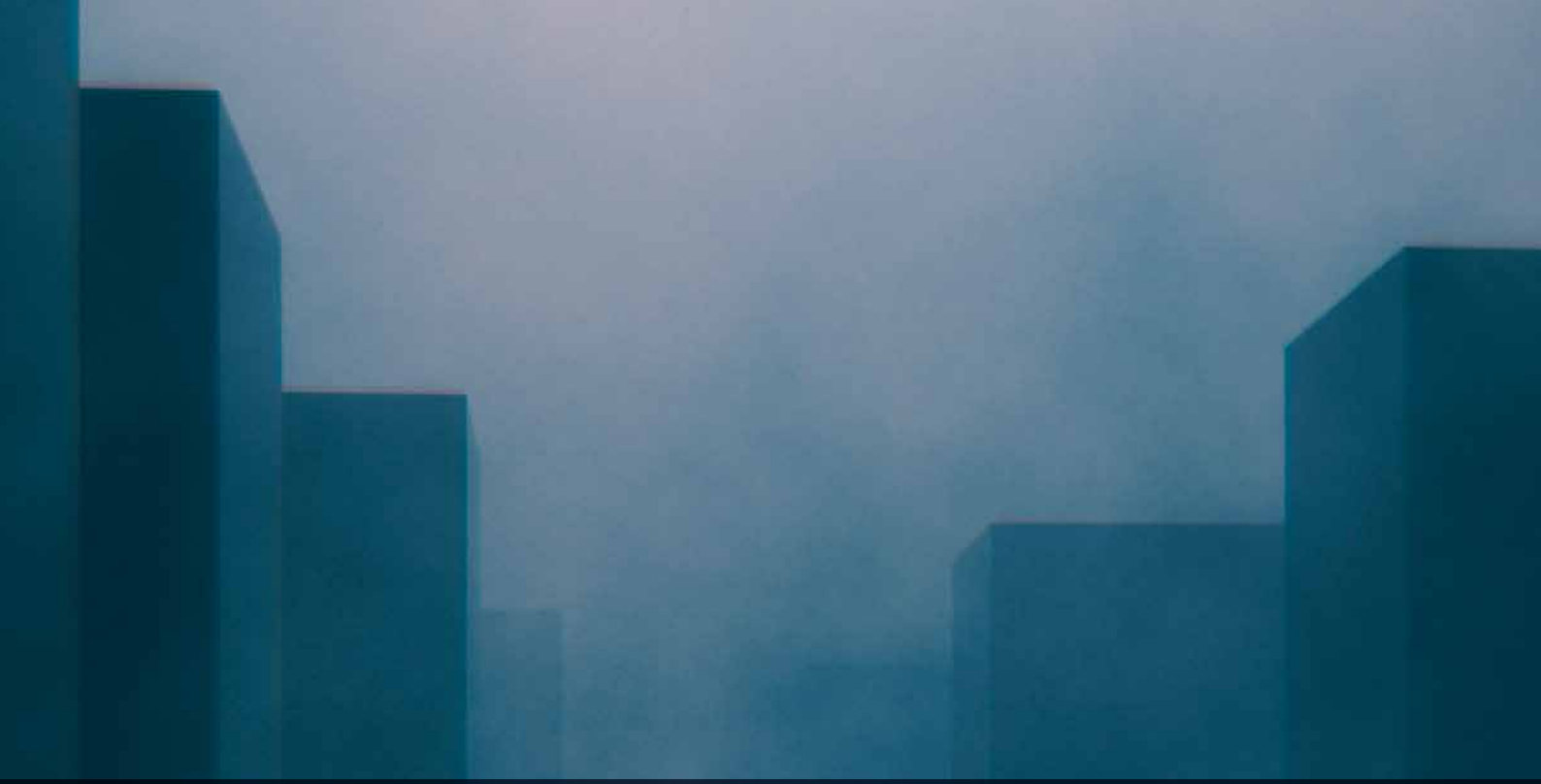


CISOs' Toughest Dilemma: Prevention Is Faulty, yet Investigation Is a Burden

A Bitdefender survey on IT security purchase professionals from large companies in the US and Europe

April 2018

Bitdefender®

Abstract

In a fast-changing landscape where large cyberattacks make the news virtually every month, companies have started shifting their security defense paradigm toward gaining more visibility into the way attacks occur, and how they become targets. By 2021, the global cost of cybersecurity breaches will reach $6 trillion, double the total for 2015, according to the World Economic Forum.[1] Building shields in an effort to safeguard IT infrastructures is no longer enough, due to the porous nature of perimeters and the known failure rate of a fortress approach.

These cyber security risks have led to changes in the security landscape and analysts have seen companies' security spending has already started migrating from prevention-only approaches to focus more on detection and response. Advisory firm Gartner expects that spending on enhancing endpoint detection and response (EDR) capabilities will become a key priority for security buyers through 2020.[2] Traditional cybersecurity features, also perceived as passive defensive practices (e.g. endpoint protection platforms (EPP), firewalls, app security and intrusion prevention systems), which focus on prevention, are constantly being improved by active defense mechanisms, such as EDR tools, to provide relevant, accurate reports into security operations and analytics.

EDR is experiencing solid growth, with revenues expected to increase 50% per year until 2020 to more than $1.5 billion. Analysts say the main growth driver is that protection alone has failed too many times and enterprises need additional visibility and detection to augment their EPP methods.[3]

Endpoint detection and response solutions will not only help CISOs protect their infrastructure against sophisticated cyber threats, facilitate early detection and gather intelligence, but also bring visibility to stealthy attacks, enabling rapid containment.

In addition to the improved detection and response approaches to prolific security incidents, EDR tools also address the shortage of cybersecurity professionals, estimated to reach a record need of 1.8 million qualified information security personnel by 2022, up 20% from 2015.[4] Two-thirds of information security professionals reported having too few workers to address current threats, while the number of cyber threats rises to new heights each year.

More specifically, endpoint detection and response tools best fit resource-strapped businesses with lean IT teams that operate without a coordinating hub for cybersecurity activities, also known as Security Operation Center or SOC. Even though SOCs are increasingly common, almost half of organizations don't have one[5], creating many security challenges: slower identification of intrusions, ad-hoc or no processes following a security breach, inability to efficiently protect the most valuable assets from advanced attacks, and delayed isolation of corrupted infrastructures. Detection and response capabilities allow these companies to easily and immediately detect the attack and react to minimize the impact on its network, brand reputation and customers.

The Bitdefender survey, which polled 1,050 people responsible for purchasing IT security within companies with 1,000+ computers in Europe and the US, explores CISOs' needs in the prevention-detection-response-investigation era and weights how the lack of visibility, speed, and personnel affects building stronger security practices in companies with both over-burdened and under-resourced IT teams.

[1] - *World Economic Forum, Global Risks Report 2017, January, 2017*
[2] - *Gartner, Detection and Response is Top Security Priority for Organizations, March, 2017*
[3] - *Gartner, Avivah Litan, EDR Market grows to $1.5 billion in 2020, March, 2017*
[4] - *Booz Allen Hamilton Holding Corp, ISC2, Frost&Sullivan, Global Information Security Workforce Study, 2017*
[5] - *EY, Global Information Security Survey 2017–2018, January, 2018*

Executive summary

As cybercriminals and malware developers shift to sophisticated and more complex threats, such as new threats or file-less attacks, to evade traditional solutions, companies have started adding layers of protection that back up the standard endpoint protection platforms (EPPs). However, even though stacking multiple solutions, such as EDR capabilities, brings stronger security, CISOs still face trouble managing multiple platforms, chasing false alerts and increasing security teams' resources while keeping costs down.

Bitdefender's survey of large companies in the US and Europe shows that most Chief Information Security Officers have had difficulties in deploying and maintaining complicated endpoint security architectures. Some 72% of information security professionals admit their IT team experiences both agent and alert fatigue. Four in five respondents in Sweden, Denmark and Italy say their IT team experience alert and agent fatigue (82%, 80%, and 81% respectively), compared to 58% of Germans.

In this context, organizations that plan to expand their IT security teams to fight zero-day exploits, advanced persistent threats, and other devastating types of cybercrime face severe recruiting challenges, with more than one in six CISOs in the US and Europe, on average, admitting the company they work for is negatively affected by the global cyber skills deficit. Almost three quarters (74%) of Swedes – the highest percentage from those surveyed - acknowledge the adverse effects of the shortage of cybersecurity professionals; Italians scored lowest, yet still a significant proportion, at 41%.

Overall, 69% of CISOs perceive their team as under resourced. Again, with the exception of Italy, over half of respondents in all markets consider their IT security team is too small.

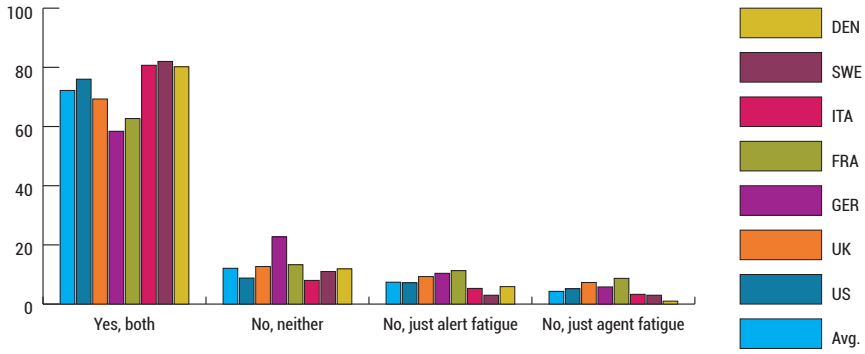
While most companies have started taking steps to defend against advanced attacks by developing Security Operations Centers (SOCs) – fundamentally an internal team of IT security specialists that deals with security issues on an organizational and technical level – many still have no internal structure to deal with modern threats. With no SOC in place, CISOs complain about different security flaws. Over two thirds of IT execs from UK and Denmark said speed to investigate suspicious activity is one of their toughest tasks, while 64% of Americans mentioned monitoring activities, and 52% of Germans perceive the ability to quickly respond and remediate potential threats as the main obstacle created by the absence of a well-funded and well-resourced SOC. Half of Danes leading security teams in companies with no SOCs note keeping up with alerts as a challenge, while 43% of Italians have difficulties finding unknown attackers inside the network, and 48% of French indicate poor visibility of their IT environment.

Most CISOs say fighting attacks of increasing complexity demands increasing budgets. In total, 43% of IT security professionals say they have a big enough budget to efficiently secure infrastructures. While half of Swedes and Italians would rate budgets as sufficient (58% and 54% respectively), less than 30% of French and Brits (31%) say the same. Meanwhile, a third of UK, US and German respondents (33%, 34% and 33% respectively) say their budget could not accommodate infrastructure expansion, and 24% of Germans say their budgets could not support a future increase in headcount.

On top of that, in terms of manpower and time consumption, managing EDR tools is described as difficult or very difficult by half of IT execs. 15% of US CISOs said it is very difficult, and 73% of Brits say it is difficult deploying these technologies. Some security professionals who use both protection and detection and response-based security feel they are too noisy. Of all endpoint alerts triggered by monitoring and response technologies handled by Swedish security teams, 56% are false alarms. In this field, high scores have been reported in all surveyed countries: UK and US (49%), Denmark (47%), France (45%), Germany (37%), and Italy (36%).

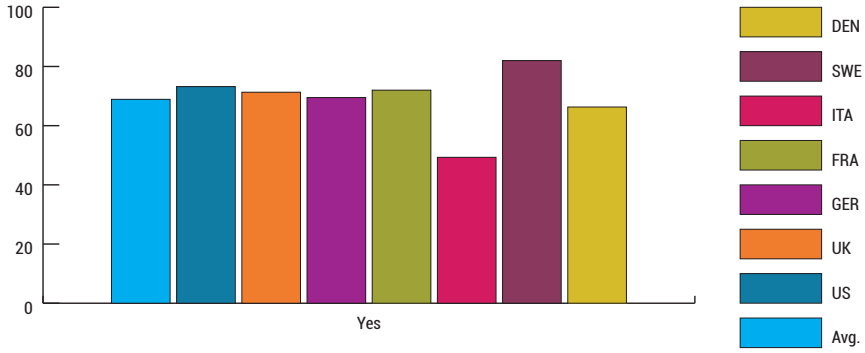
This survey further explores the consequences of a company's lack of awareness of an ongoing breach, and the obstacles that prevent rapid incident detection and response, despite seven in 10 companies already having dedicated budgets for EDR solutions. On average, security professionals have to provide detailed reports on previous and identified cyberattacks to their top managers or boards every eight months. At the same time, most CISOs say they will need in-depth security incident reports provided by an EDR solution for future cyberattacks to become GDPR-compliant (General Data Protection Regulation).

Does your IT team experience alert and agent fatigue? (%)



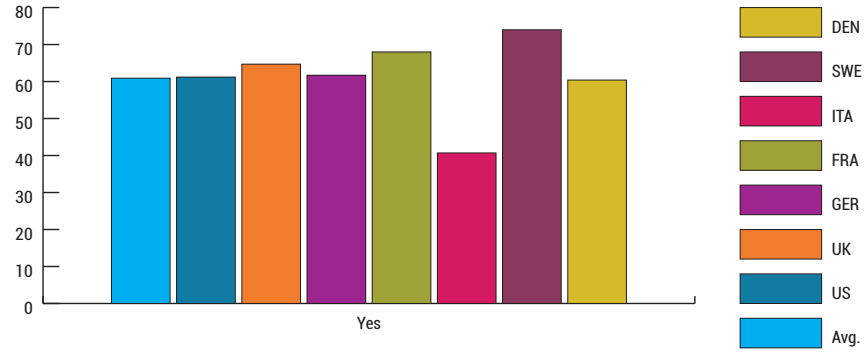
	Avg.	US	UK	GER	FRA	ITA	SWE	DEN
Yes, both	72.2	76	69.3	58.4	62.7	80.7	82	80.2
No, neither	12.1	8.8	12.7	22.7	13.3	8	11	11.9
No, just alert fatigue	7.4	7.2	9.3	10.4	11.3	5.3	3	5.9
No, just agent fatigue	4.3	5.2	7.3	5.8	8.7	3.3	3	1

Do you consider your IT security team to be underresourced? (%)



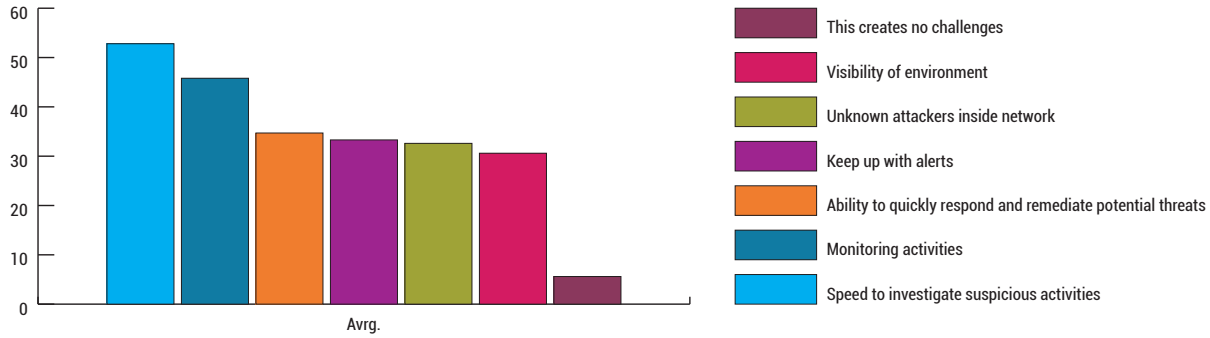
	Avg.	US	UK	GER	FRA	ITA	SWE	DEN
Yes	68.9	73.2	71.3	69.5	72	49.3	82	66.3

Would you say your company is negatively affected by the global cyber skills deficit? (%)



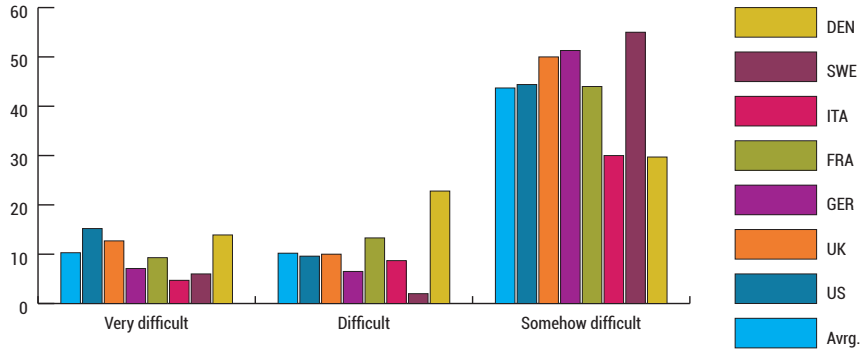
	Avg.	US	UK	GER	FRA	ITA	SWE	DEN
Yes	60.9	61.2	64.7	61.7	68	40.7	74	60.4

What are the biggest challenges the absence of a Security Operation Center (SOC) creates? (Tick up to three) (%)



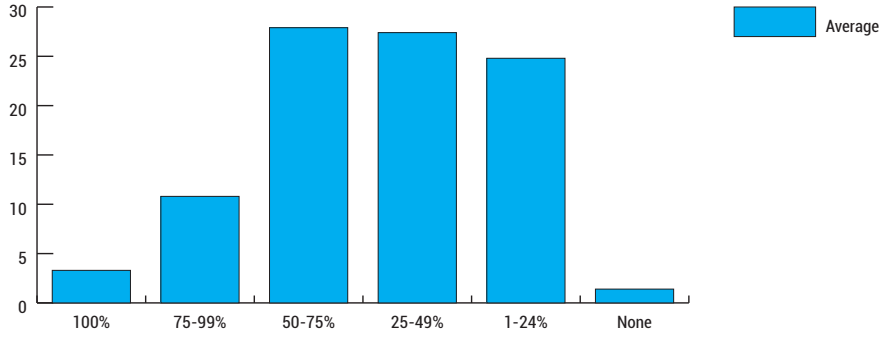
	Avrg.
Speed to investigate suspicious activities	52.8
Monitoring activities	45.8
Ability to quickly respond and remediate potential threats	34.7
Keep up with alerts	33.3
Unknown attackers inside network	32.6
Visibility of environment	30.6
This creates no challenges	5.6

How difficult is managing detection and response capabilities in terms of manpower and time consumption? (%)



	Avrg.	US	UK	GER	FRA	ITA	SWE	DEN
Very difficult	10.3	15.2	12.7	7.1	9.3	4.7	6	13.9
Difficult	10.2	9.6	10	6.5	13.3	8.7	2	22.8
Somehow difficult	43.7	44.4	50	51.3	44	30	55	29.7

Of all the endpoint detection and response (EDR) alerts your security team handles, what percentage are false alarms? (%)



	Average
100%	3.3
75-99%	10.8
50-75%	27.9
25-49%	27.4
1-24%	24.8
None	1.4

Visibility at dusk proves essential

Half of the CISOs surveyed admit their company was breached in the past year, but one in six does not know how the breach occurred. An even higher percentage think their company is currently likely or very likely to face an ongoing security breach without knowing it (25%). The main consequence of being unaware of a breach while it is happening is business interruption, according to more than half of IT execs. Depending on the industry, these interruptions can have a significant impact on reputation, mainly if they lead to widespread media coverage or publicly expose customer data, or if they trigger direct financial losses, both mentioned by 44% of European and American CISOs. Intellectual property loss, legal fines and penalties, or even job loss for those responsible for preventing the attack could also be side effects of late detection and not minimizing the dwell time of infections.

As a result, 82% of companies have security tools, processes, and staff to detect and respond to advanced attacks. Two-thirds have this service as an in-house or do-it-yourself operating model while a quarter have opted for outsourced models.

Using their current security tools, UK respondents think 63% of advanced attacks can be efficiently prevented, detected and isolated. This compares to 61% in the US, 60% in Italy, 58% in France and Sweden, 52% in Germany, and 44% in Denmark.

US CISOs said it took, or would take, four weeks to detect an advanced cyberattack. This is the highest average of any market. Respondents from the UK, Germany, France, Sweden and Denmark all said they need three weeks to detect an advanced cyberattack.

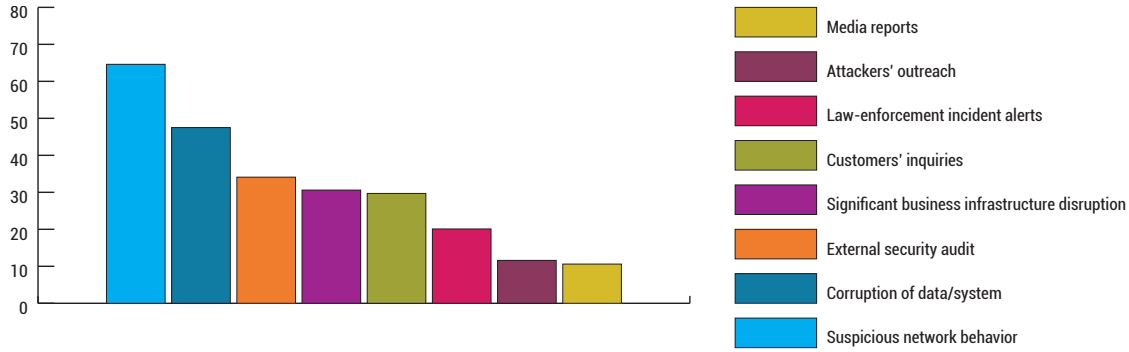
Asked if they had experienced an advanced attack or malware outbreak, more than half of respondents in the UK (57%), USA (55%), France (58%) and Italy (53%) said that they had. During 2017, the WannaCry and GoldenEye ransomware outbreaks showed CISOs that known yet unpatched vulnerabilities can have dire consequences on businesses and infrastructures if weaponized with wormable behavior.

Suspicious network behavior has been decisive in uncovering a malware outbreak or an advanced attack, mentioned as a key clue by 75% of Italians, 73% of Danes, 69% of Brits, 67% of Swedes, 65% of Americans, 54% of French, and 51% of Germans. The second most frequently given answer, across all markets except Sweden, was corruption of data or systems, while external security audit was the third most frequently given answer by respondents in the UK (23%), USA, (39%), France (30%), Italy (30%), Sweden (39%) and Denmark (48%). For German CISOs, the third most frequent answer was a significant business infrastructure disruption, at 35%.

Not only does increased visibility help organizations figure out when and how they were breached, it also enables them to take preventative measures to plug similar security events in the future. In the context of GDPR (General Data Protection Regulation), planning a security strategy for protecting company and client data based on increased visibility across the entire infrastructure, helps drive compliance and a strong security posture.

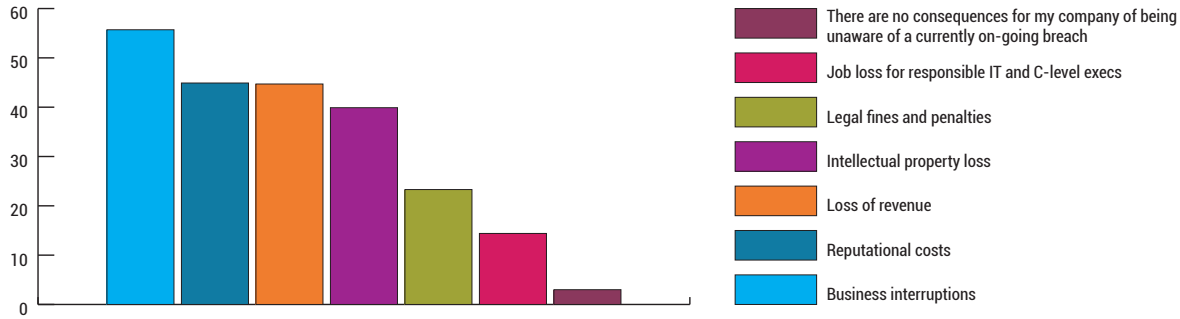
With security breaches estimated to sometimes last for months without triggering any warnings, an inability to accurately observe and take action against an ongoing intrusion could mean compromising all customer and mission-critical data, directly impacting business continuity and reputation. Detecting ongoing breaches as close to the initial point of compromise as possible reduces potential fallout from a data leak and helps organizations strengthen their reputation by taking action before irreparable damages occur. However, spotting an ongoing breach also means fighting alert fatigue caused by noisy traditional security solutions. This means IT and security teams are usually racing against time when filtering security alerts, something that's difficult to pull off, especially if understaffed and overburdened.

How did you identify an advanced attack or malware outbreak? (multiple answers possible - %)



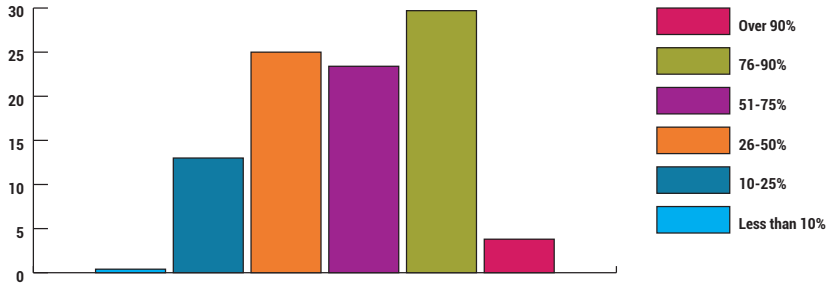
Suspicious network behavior	64.6
Corruption of data/system	47.5
External security audit	34.1
Significant business infrastructure disruption	30.6
Customers' inquiries	29.7
Law-enforcement incident alerts	20.1
Attackers' outreach	11.6
Media reports	10.6

What are the main consequences for your company of being unaware of a currently on-going breach? (multiple answers possible - %)



Business interruptions	55.7
Reputational costs	44.9
Loss of revenue	44.7
Intellectual property loss	39.9
Legal fines and penalties	23.3
Job loss for responsible IT and C-level execs	14.4
There are no consequences for my company of being unaware of a currently on-going breach	3

Using your current security tools, what percentage of advanced attacks can be efficiently prevented, detected, and isolated? (%)



Less than 10%	0.4
10-25%	13
26-50%	25
51-75%	23.4
76-90%	29.7
Over 90%	3.8

Filling the empty seats

As 250,000 new malicious programs and an increasing number of tailor-made threats try to wreak havoc on corporate IT infrastructures each day, the need for qualified information security personnel is higher than ever. Simultaneously, most companies struggle for rapid incident detection and response, with teams that can't keep up with the sheer number of alerts their EDR solution identifies, and the difficulties in deploying and maintaining the entire endpoint security architecture.

With almost half of alerts signaled by EDR tools being false alarms, the lack of personnel is the main obstacle CISOs in the UK, Germany, and Sweden face that prevents rapid detection and response during a cyberattack. In France, the US, and Italy it was the lack of proper security tools (50%, 43%, 35%) and in Denmark it was the lack of knowledge (55%). Lack of proper security tools is the third most frequent obstacle in the UK (39%) and Denmark (48%), but it also scored high in Sweden (41%) and Germany (32%). Companies also feel their breach containment is becoming harder due to higher costs (a third on average).

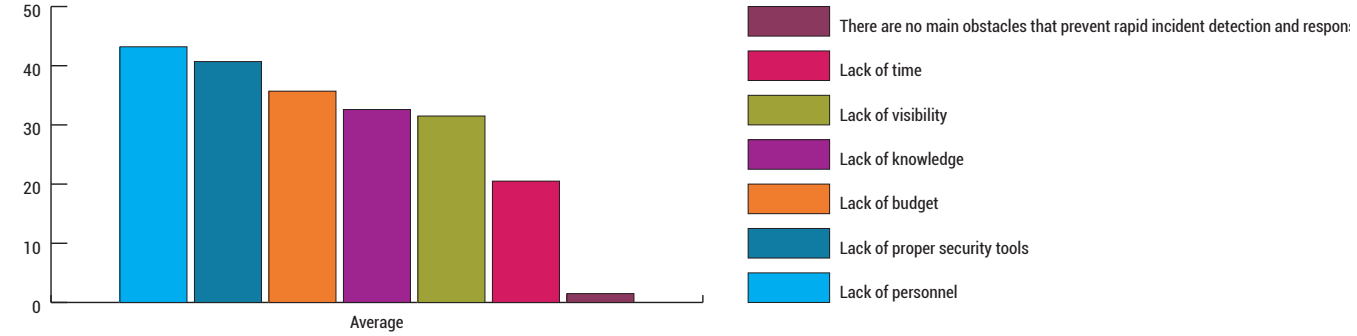
To help combat the growing gap, EDR solutions plan to help security teams to focus only on the real and dangerous threats that would have otherwise not tripped any alarms. However, most CISOs say that, while it improves security analysts' ability to discover, investigate and respond to advanced threats and broader attack campaigns on multiple endpoints, EDR can be difficult to manage, especially in companies that lack a SOC and aren't very sophisticated in IT security, yet want to elevate their security posture and take a more strategic approach.

For Germans, lack of skilled personnel tops the list of main obstacles (40%) in strengthening their company's cybersecurity posture. Lack of predictability tops the list for respondents in US (41%), France (47%), Italy (33%) and Sweden (48%), while Brits perceive the lack of infrastructure-agnostic security as the main obstacle (33%). Those in Denmark cited lack of visibility (55%).

"Companies and organizations that have powerful and resource-intensive EDR tools but no SOCs in place are basically bleeding financial resources without maximizing the true potential of these security tools," says Liviu Arsene, Global Cybersecurity Analyst at Bitdefender. "It's like owning a private jet but not having a qualified pilot or crew to fly and manage it. Traditional EDR tools require both manpower and skilled security experts to fully cope with and handle all security alerts, otherwise EDR deployment simply remains compliance oriented and not a security tool."

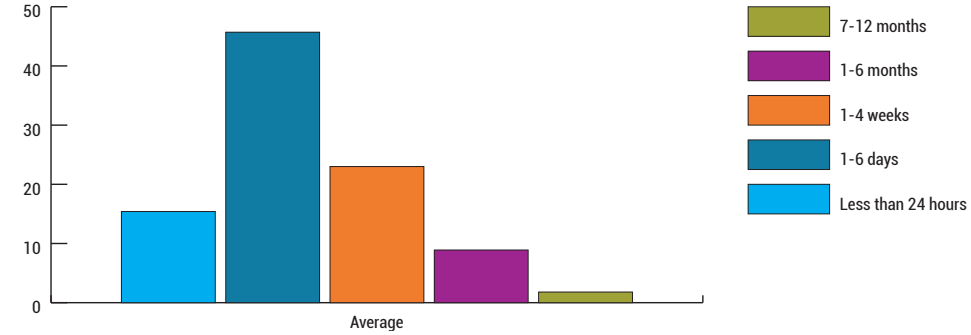
Agent fatigue is to blame for when security teams that are overburdened with managing EDR tools end up ignoring or disregarding the never-ending tide of security alerts, defeating the aim of detection and response. Triggered alerts could take days, weeks, and even months before they're addressed and investigated, meaning security breaches could take just as long to detect as without an EDR solution in the first place, if insufficient staff is present.

What are the main obstacles that prevent rapid incident detection and response? (%)



	Average
Lack of personnel	43.2
Lack of proper security tools	40.7
Lack of budget	35.7
Lack of knowledge	32.6
Lack of visibility	31.5
Lack of time	20.5
There are no main obstacles that prevent rapid incident detection and response	1.5

How long did it take you / would it take you to detect an advanced cyber-attack? (%)



	Average
Less than 24 hours	15.4
1-6 days	45.7
1-4 weeks	23
1-6 months	8.9
7-12 months	1.8

Running with tied legs

Companies that use an EDR solution have acknowledged that a cyberattack can occur at any time, and traditional protection platforms can only address 99% of the threats in the wild. EDR tools focus on the last 1% of threats, allowing for much greater fidelity in incident investigations. On average, some 82% of security professionals in Europe and the US say that reaction time is a key differentiator in mitigating cyberattacks. Italy, the US, France, and the UK scored highest, CISOs' main argument behind this is that time is of the essence when isolating the incident to prevent spreading (68%), identifying how the breach occurs (55%), and evaluating losses and the impact of the breach (51%), mainly. Delayed response to a cyber incident can also make it harder to accurately identify the initial time of attack and assess the timeframe (30%), understand the motivation for the cyberattack (19%), or improve the incident response plan for future attempts (17%).

As a result, the second main important driver for enhancing the company's cybersecurity posture is also speed-related: faster detection and response capabilities are mentioned by almost half of those surveyed, immediately below improving data protection (51%).

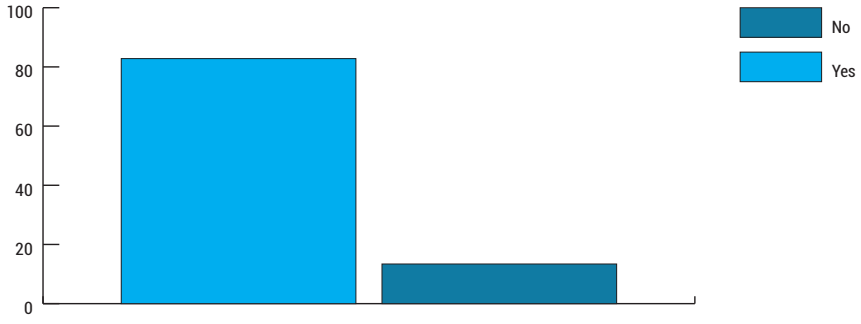
EDR tools that don't have a priority-based alert filtering mechanisms can slow the detection and response process of real threats, as it may send IT and security staff on investigation paths that either lead nowhere or are trivial. EDR alerts should not be about the sheer number of triggered alerts, but about intelligent, reliable, and meaningful alerts with a high probability of pointing to a real threat. Traditional EDR tools may seem like a security enabler, but without dedicated and staffed SOC teams, they may either hinder the organization's security capabilities or make no significant contribution to the overall security posture.

Detecting data breaches revolves around closing the gap between the initial compromise and subsequent data exfiltration. The major benefit of meaningful EDR alerts is that accurate and actionable security alerts lead to fast detection and response, without overburdening IT or security staff with trivial notifications.

"Timely detection of data breaches directly affects organizations in a positive way, as incident response procedures can be immediately triggered to contain, mitigate, and prevent full-blown security incidents that could otherwise financially affect the organization," Arsene adds. "Zeroing in on potential security breaches as they occur makes a world of difference between business continuity and irreparable financial or reputational damages."

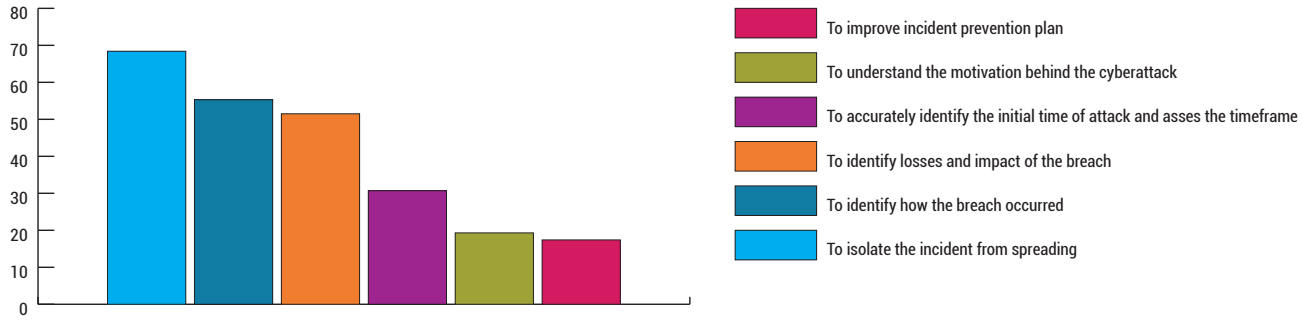
Otherwise, damages caused by a data breach can scale over time the more a breach is present in an organization's infrastructure. Failure to detect a breach as it occurs may lead to full infrastructure compromise, irreversible data loss, and financial repercussions from which some companies may never recover. With attacks becoming more sophisticated, advanced, and pervasive, companies are left vulnerable by the traditional set it-and-forget it security model in which organizations and businesses acquire but don't continuously manage security tools or update incident response plans. The true power of an effective security posture lies in a layered security defense, augmented by next generation detection and response tools that accurately nail potential data breaches as they occur. Based on the data in this survey, it's fair to say that organizations cannot afford the absence of the right security tools.

Is reaction time a key differentiator in mitigating cyberattacks?



Yes	82.8
No	13.4

If yes, why is speed a key differentiator in mitigating cyberattacks? (multiple answers possible - %)



To isolate the incident from spreading	68.4
To identify how the breach occurred	55.3
To identify losses and impact of the breach	51.5
To accurately identify the initial time of attack and asses the timeframe	30.7
To understand the motivation behind the cyberattack	19.3
To improve incident prevention plan	17.4

Investigation reaches board-level thinking

Companies provide detailed reports on previous and identified cyberattacks to their managers or board of directors every eight months on average. Danes must send detailed reports on breaches or attempted breaches to their C-level suite the least frequently on average (12 months), whereas Italians provide them the most frequently (six months). Those in the UK and the US need to deliver these assessments every nine months, while the Germans and the French every eight months.

Most CISOs surveyed trust next generation security, including endpoint detection and response capabilities, as the best security approach against advanced attacks. Security audits, and traditional security - endpoint protection platforms - come second and third, mentioned by more than a third of respondents.

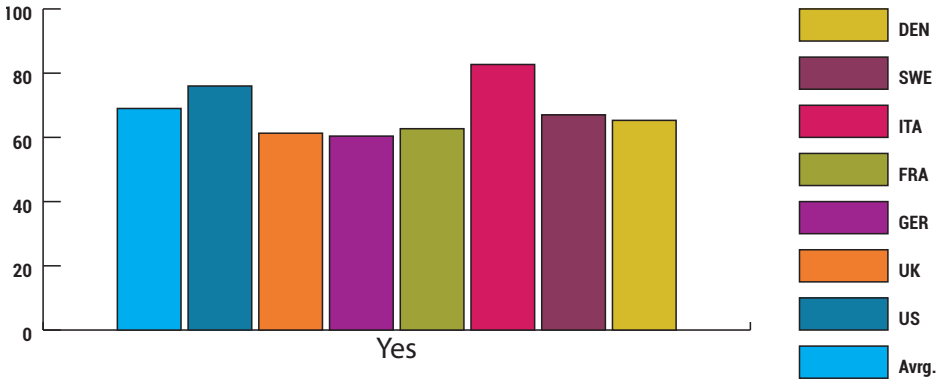
Just weeks before the EU General Data Protection Regulation takes effect globally, many organizations still find themselves struggling to comply. The new requirements include that data be protected adequately, and when breaches do occur, organizations need notification capabilities that align with GDPR standards. Being GDPR non-compliant after May 2018 means not only negative publicity and damage to the companies' reputation, but also penalties of up to 4% of a company's global annual revenue.

Mainly, companies need to identify data that falls under the regulations' control – "any information relating to an identified or identifiable natural person" – document how this data is secured, and create incident response plans. In this respect, 78% of respondents in the US and Europe stated that they will need in-depth security incident reports provided by EDR solution for future cyberattacks to be GDPR compliant.

EDR reports should not be regarded as merely a tool for improving incident response plans and building new security defense strategies, but also as an effective means for CISOs to bring security-driven decisions to the board room. By presenting actionable intelligence reports to board members, CISOs can ultimately argue for increased security budgets for new technologies and headcount by showing relevant stats, figures, the effectiveness of the current security stack, and how larger budgets can help drive business and value. With board members mostly focused on financials, detailed EDR-related intelligence that can directly impact business revenue is the leverage CISOs need to make security vital in the long-term business strategy of the organization.

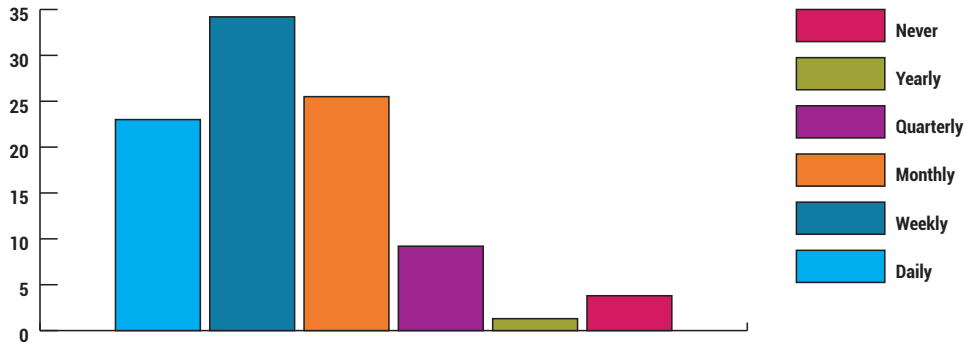
"With board members becoming increasingly involved in security aspects, detailed reports that remove security blind spots help drive intelligent resource and budget planning in line with the company's objectives, allowing for scalability, performance and security to drive company business," Arsene adds.

Does your company have a dedicated IT security budget for incident investigation and forensic (EDR)? (%)



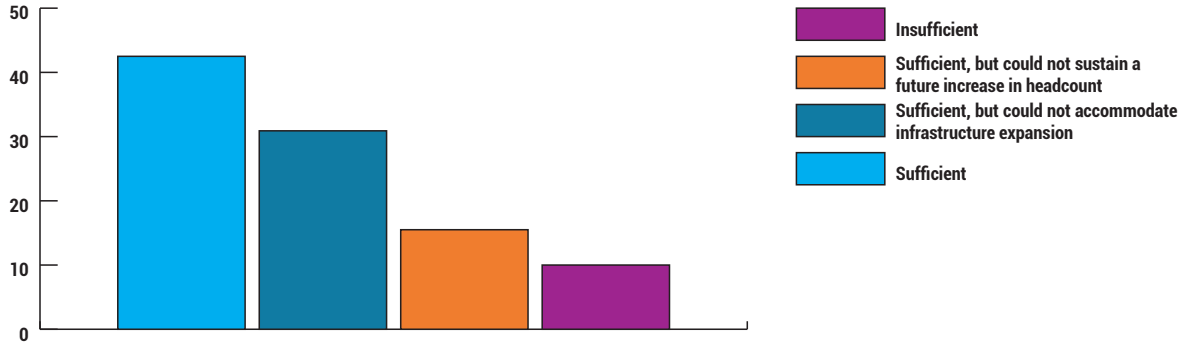
	Avrg.	US	UK	GER	FRA	ITA	SWE	DEN
Yes	69	76	61.3	60.4	62.7	82.7	67	65.3

How often do you need to provide detailed reports on previous and identified cyberattacks to your manager or board? (%)



Daily	23
Weekly	34.2
Monthly	25.5
Quarterly	9.2
Yearly	1.3
Never	3.8

How would you rate the IT security budget of the company you work in? (%)



Sufficient	42.5
Sufficient, but could not accommodate infrastructure expansion	30.9
Sufficient, but could not sustain a future increase in headcount	15.5
Insufficient	10

Key takeaways

"The survey results show that today's resource- and skill-constrained IT security teams need a better approach to endpoint detection and response (EDR)," Bitdefender's VP of Enterprise Solutions Harish Agastya says. "A funnel-based approach leverages preventative controls such as machine learning and behavioral monitoring at the front end of the attack monitoring cycle to detect a high percentage of known threats quickly. Threat analytics next sift through behavioral events in system activities and create a prioritized list of incidents for additional investigation and response, enabling the EDR layer to focus on threats further down the funnel in the unknown or potential threat category. EDR for everyone means less human intervention and a much higher level of fidelity in incident investigations. Really it's about better detection and response to threats quickly, enabling human administrators to ensure better protection of critical assets."

When considering EDR solutions, Bitdefender security specialists strongly advise enterprise CISOs to consider the importance and value of an integrated prevent-detect-investigate-respond-evolve approach to endpoint security:

- Prevent: block all known bad and a high percentage of unknown bad automatically at pre-execution and on-execution layers, without needing manual intervention
- Detect: gain visibility into suspicious events that could lead to an attack early by built-in intelligence from threat protection engines and analysis of a stream of behavioral events from an endpoint event recorder
- Investigate: aided by root cause and contextually relevant information on the class of threat that is detected (via the built-in intelligence), the reason of detection (via threat analytics), and ultimate verdict (via an integrated sandbox).
- Respond: via intuitive incident response interface that enables remedial actions immediately and widely across the enterprise without needing deep expertise.
- Evolve: enables the feedback loop from current detection to future prevention via in-place policy tuning and fortification.

Methodology

The survey, conducted in February-March 2018 by Censuswide for Bitdefender, included 1,050 IT security purchase professionals from large enterprises with 1,000+ PCs and data centers, based in the US and Europe. 250 respondents originate from the United States, while 154 are from Germany, 150 from the UK, France, and Italy each, 101 from Denmark, and 100 from Sweden. Some 69% of all respondents are male, while more than a third are aged 35 to 44.

More than 90% of the organizations surveyed in the US and Europe have over 500 employees, covering industry sectors such as IT and Telecoms (38%), Manufacturing and Utilities (14%), Finance (12%), Professional Services (10%) and Retail (7%), among others.

Author: Razvan Muresan

BD-Business-Mar.30.2018-Tk#: CREA-2570
Bitdefender-Business-2018-WhitePaper-EDR_RM_BB_DT_JM-crea2570-en_EN

Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business