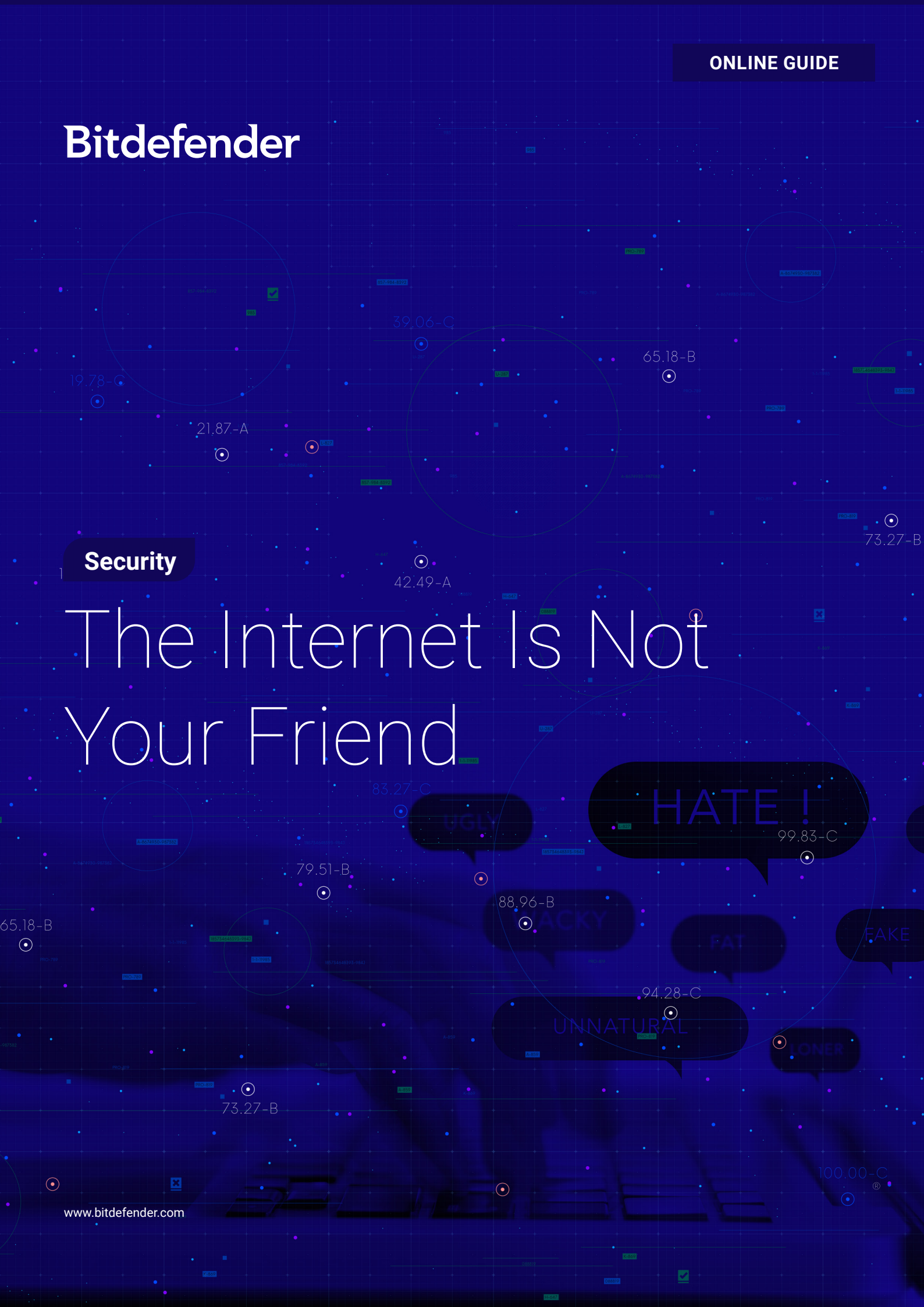
ONLINE GUIDE

Bitdefender



Security

The Internet Is Not Your Friend

www.bitdefender.com

The internet is not their friend – the challenges kids face in the modern digital world

Children's online security is a problem that becomes more complex each year. Many parents and teachers are unaware of the complex online ecosystem and the dangers of online security. This presentation aims to shed some light on the issues kids face each day and maybe even educate some adults about the present risks.

The internet is not as friendly as children believe, especially social media and gaming platforms. One of the most important aspects regarding kids' use of social media is the age limit of 13. Most parents and kids don't know that the terms of use for social networks such as Facebook, Snapchat, Instagram, TikTok, and all the rest set the age of 13 as the minimum.

The motive for these age limits is not difficult to understand. All social networks and many gaming platforms offer content that is sometimes unsuitable for children. Also, risks regarding personal safety are much more serious for young ones.

More likely than not, kids have already witnessed online content that was not meant for them, and they usually know it. Moreover, even the email account needed to set up a new phone has the same 13-year minimum age.

Kids' data should be kept under lock and key

Everything we share or post on the internet remains online. There's no magic button you can press to delete it all – shared information will likely remain accessible for a very long time, if not forever.

This is especially dangerous because private information such as personal pictures, for example, can end up in the wrong hands if you don't set the account to private.

Having friends is good, but knowing the people you add as friends is important. The people you add as friends on social media will see everything you post, but some of the online "friends" may actually be strangers.

Would you share your street address or personal photos with some stranger on the street? According to a 2019 survey, almost a third of children aged between 8 and 13 shared personal information with individuals they met online. This includes email addresses, phone numbers, home addresses and the name of the school they attend.

Children need to learn two important rules when it comes to social media: keep their accounts private and be very careful when adding new people to friend lists. This way, only real friends can see what they're sharing.

Not everyone we meet online has our best interest at heart, and kids don't always keep this in mind. Some of the information and content shared online or offered in private can be used to harm them. They should keep all this information a secret and flag any misuse to their parents, caretakers or teachers.

Many people pretend to be someone else when they're online, and you can't verify whether the information they provide is real. This applies to individuals your kid interacts with on social media networks and online gaming platforms – they could have bad intentions and lie about their age and background to earn kids' trust.

Mainstream online platforms also provide cover for online predators targeting young children. They tend to have multiple profiles and often persuade kids to send them explicit images of themselves that can be used for blackmail or to arrange a meeting with them in person.

Lonely or shy children are prime targets for online predators who may pose as children themselves as they form an online relationship.

They can also use another person's identity to obtain private data, pictures, and videos, and even propose meetings in real life.

The most important rule we should teach kids is to never share personally identifiable information such as complete name, date of birth, Social Security numbers, home or school address, phone numbers, email address, passwords, information from parent's credit cards, intimate pictures or any kind of information about their family.

If your child is old enough to have an online account and post on their profiles, make sure you underline the importance of sticking to good cyber practices for his or her physical and online safety:

- Don't accept friend requests from people they don't know, no matter the platform
- Never provide pictures, videos or any other type of personal data
- Don't respond to challenges made by real or virtual friends
- Tell parents or other adults about any correspondencethat upsets or scares them in any way
- Don't click on links, emails or attachments sent by individuals they don't know to prevent data or device compromise via malicious software or phishing

Identifying and preventing cyberbullying

Bullying is a serious issue, whether in the classroom or online. Some 59% of teens in the US say they have been bullied, threatened or harassed online, and 1 in 3 people aged 13 and 24 in 30 countries have confirmed some form of cyberbullying that prompted them to skip classes.

Three-quarters of surveyed kids and young adults participating in a UNICEF poll say that Instagram, Facebook, Snapchat and Twitter were among the most common platforms for cyberbullying.

One mean comment might not seem all that serious, but when it's happening online, where you usually don't see that person you talk with, it can hurt more. According to a 2020 study, hate speech among children and teens online increased by 70% during the pandemic, and the numbers aren't showing any signs of improvement, with around 80% of teenagers stating that individuals cyberbully just for laughs.

Revealing private information about someone to the rest of the world is also a form or bullying. That information is private for a reason. With an overwhelming number of young individuals sharing too much information online, over 42% of teenagers say that others have exposed or posted private info about them on the internet.

Cyberbullying comes in many forms. Here are the most common:

- Harassment that entails sending offensive or threatening messages on social media or SMS
- Gossiping about someone with the intent to instigate other people or to isolate them
- Impersonating or creating fake profiles in another person's name, or taking over/hacking into accounts to ruin their reputation
- Excluding people from various groups or activities
- Trolling – intentionally acting in a malicious manner
- Stalking others online via multiple platforms to intimidate and inflict emotional or physical harm
- Sending mean comments to denigrate someone

Remember that bullies usually crave attention, so the best course of action is to stop giving it to them.

A survey conducted by Bitdefender found that three out of 10 teenagers (aged 12 to 16 years) were bullied or harassed online, while five in 10 say they know someone who has dealt with similar incidents at least once.

The most frequent platform for cyberbullying is Instagram (40%), followed by Facebook (31%) and Snapchat (31%), according to the study.

"Instagram has a lot of offensive accounts, but it is easy to filter them," said a 15-year-old girl responding to our survey. "Facebook has loads of funny videos, but there's also lots of false information and political fights. There's people on Instagram who will harass girls for nudes. 8/10 times it's a person you know. On Snapchat pretty much anyone can add you and because pictures disappear. Lots of people send nudes."

Communication and measures you can take to protect against cyberbullying and other online threats

Dealing with cyberbullying and other digital threats can be a cumbersome job for parents and caretakers. However, communicating openly with your child is one of the best ways to deal with these issues.

Adults should be wary of any behavioral changes in their children and teach their kids early on to make smart decisions whenever they connect to their smart devices to chat, stream or post.

Sharing too much personal information online makes kids prime targets for identity theives, bullies and predators. As such, privacy settings, strong passwords and caution should be enforced on all online platforms your kids interact with.

Tell your kids to never delete messages from people who want to harm them and to immediately inform you when this happens.

If your child suddenly withdraws from family life and activities or shows any signs of depression, act immediately to limit long-term emotional damage. Make sure your child feels safe and knows that he will receive unconditional support no matter what.

In response to most cyberbullying behaviors, kids should:

- Never retaliate or respond negatively – block and report the person instead
- Take screenshots of negative behavior, threatening messages or mean comments and report them to the social media platform or police, depending on the situation
- Max out privacy settings for all social media accounts and platforms and make sure your kids' profile is set to private

Talking with adults, mainly teachers or parents, should always be the first step when something bad happens. And that's true whether it's a matter of direct bullying or something your kids see online that was targeted at somebody else.

If kids feel uncomfortable or threatened by any online interaction, it's important to remain calm and discuss the problem.

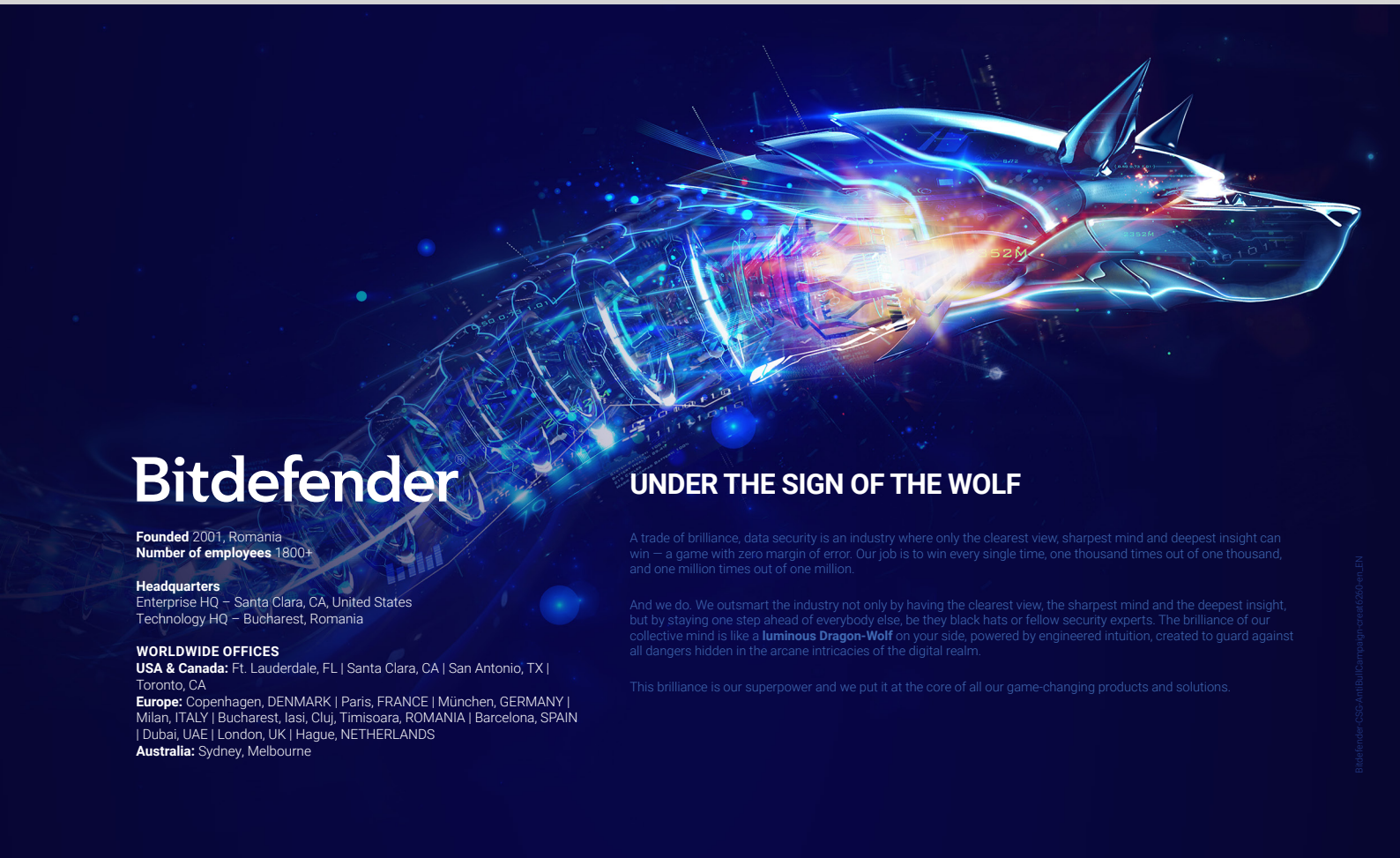
The things we say and do online have a lot of power and always leave a trail. What kids and teenagers share in the digital world will positively or negatively impact their lives.

Being good cyber citizens and leaving a positive digital footprint can give them an advantage later in life, whether it's for education or career opportunities.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.



Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-CSO-AntiBullCampaign-creat4220-en_EN