New Knowledge

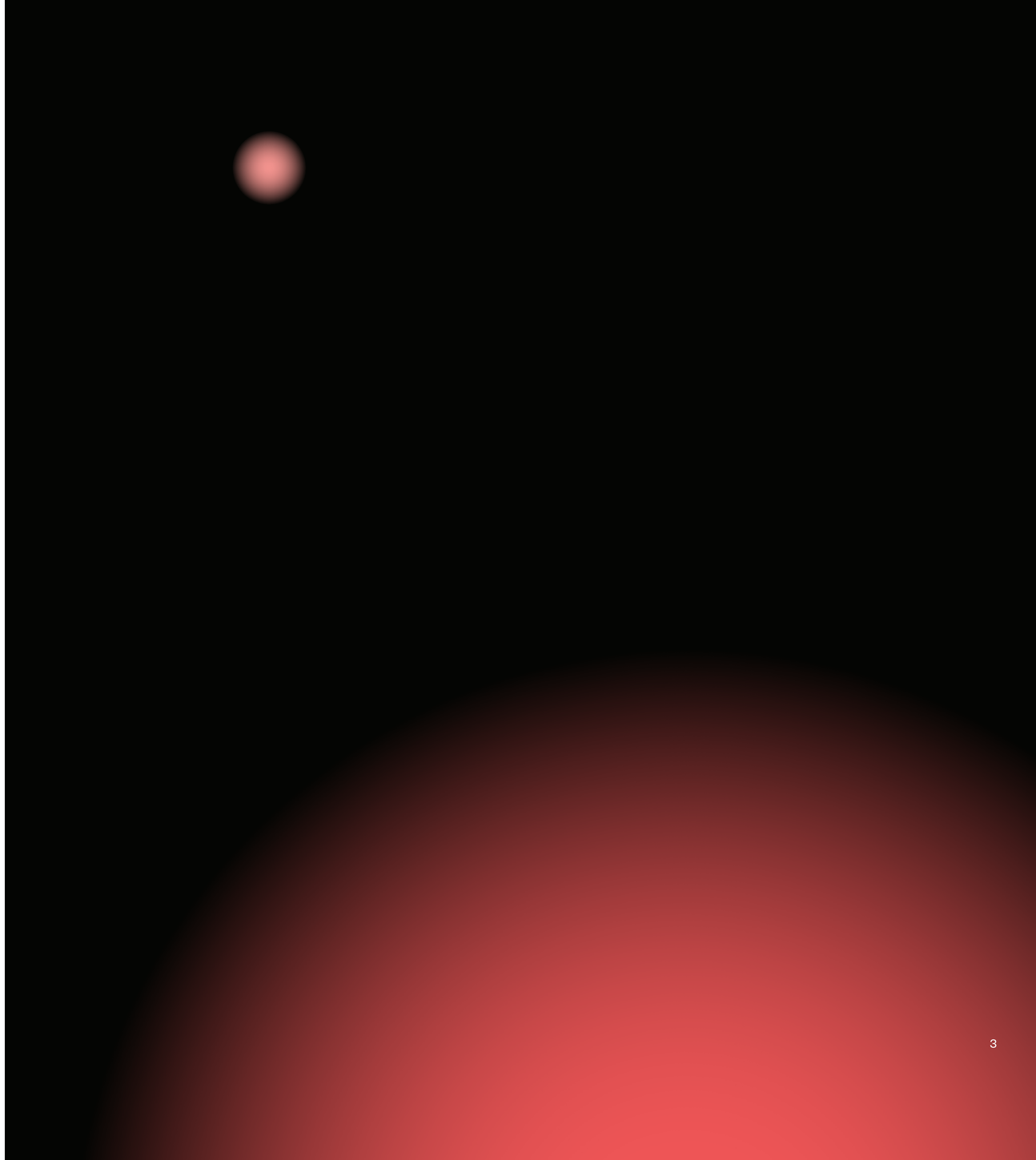
The State of Disinformation 2018

A Next-Gen Cybersecurity Problem

The internet and its capabilities are constantly evolving.

Over the past decade, disinformation, misinformation, and social media hoaxes have evolved from a nuisance into a high-stakes information war.

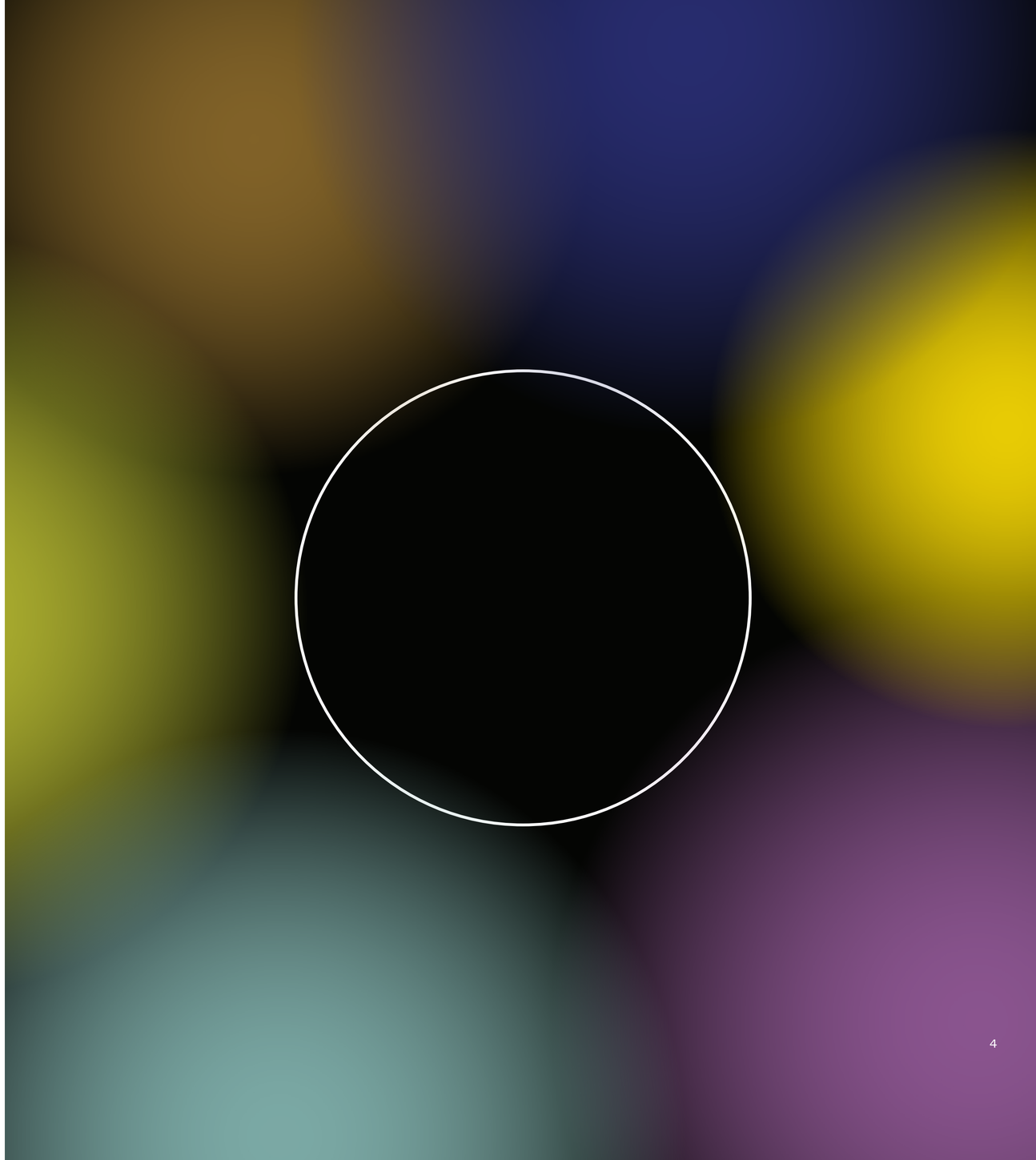
These types of operations are exploiting weaknesses in our online information ecosystem. However, security strategies have not kept up with the changing tactics and landscape. We discuss counter-messaging and counter-narratives, and fall into the trap of treating this as a problem of fakes news rather than an attack on our information ecosystem.



When lawmakers and business leaders discuss “cyber attacks,” they’re generally describing network intrusions and exfiltration of data.

There are best practices and frameworks for tackling and preventing more traditional cybersecurity attacks: identification and management of vulnerable infrastructure, building a defensive environment around that infrastructure, detecting and analyzing all anomalous events on the network, responding to actual attacks, improving those defensive measures, and recovering from successful attacks.

But disinformation does not operate in a way that lends itself to standard preventive measures.



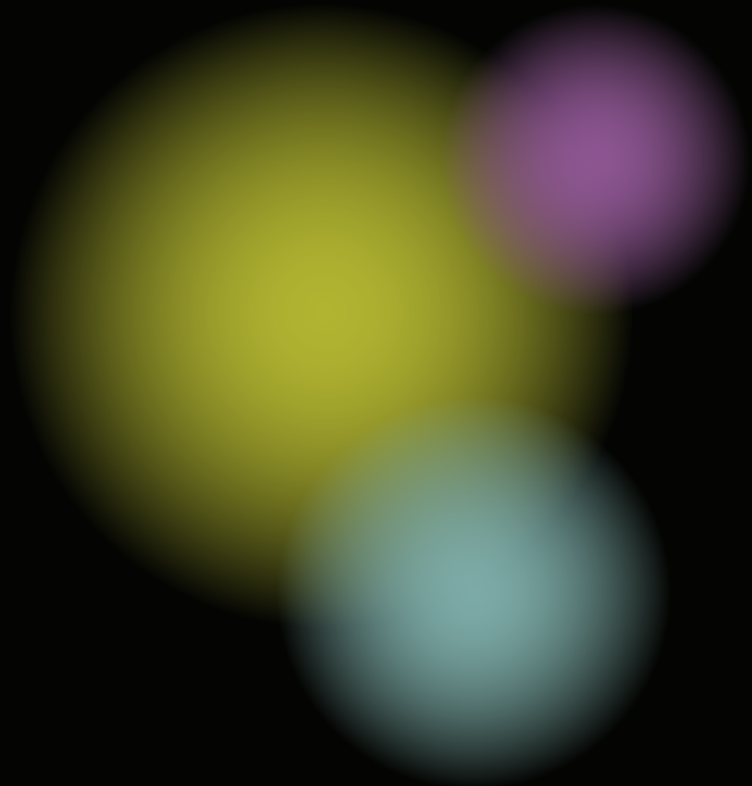
Disinformation, by contrast, is a new breed of cybersecurity threat.

It's an attack on cognitive infrastructure, on people themselves, on society, and on systems of information and belief. Its targets are widespread, making it a large and dangerous problem. Corporations and media have responded by refuting false or misleading information: defending themselves by trying to correct the record.

This is ineffective. By the time a disinformation campaign has reached the public, the damage has often already been done.

Without a next-generation information integrity security strategy, highly visible brands, democratic processes, and the entire information ecosystem are vulnerable. It's time to change how we think about propaganda, disinformation, and false information: it's not about fake news, it's an adversarial attack in the information space.

Disinformation is a cybersecurity problem.

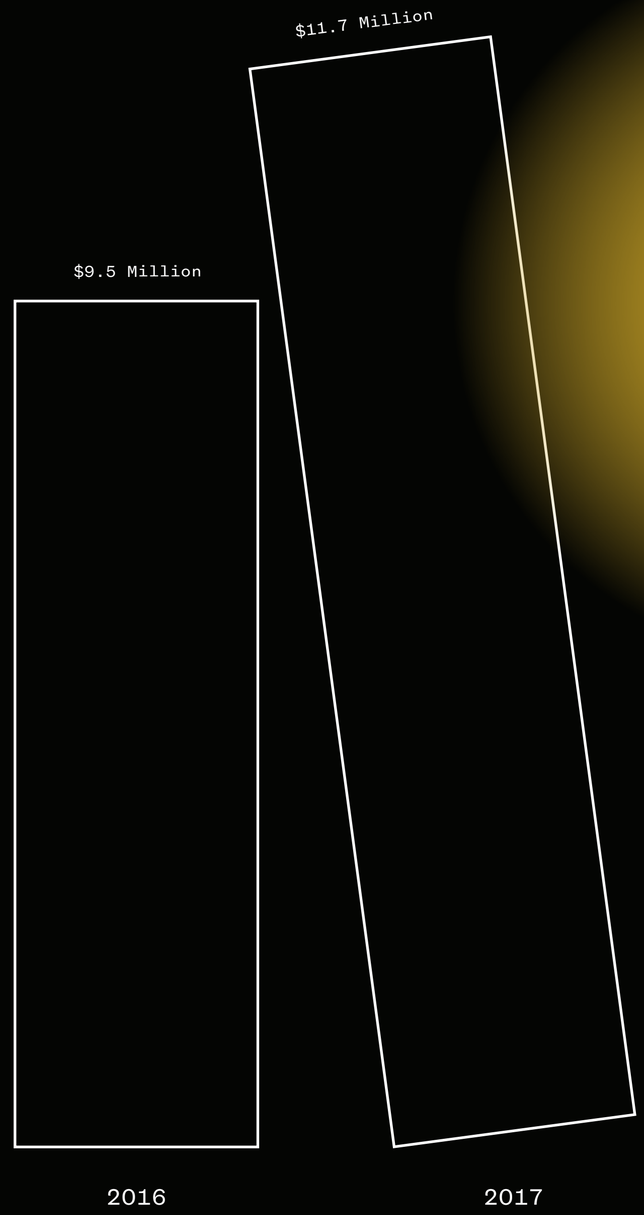


The State of Cybersecurity

Most people, and companies, associate “cybersecurity” with data breaches, device intrusions, malware, and exploits that infiltrate networks or exfiltrate data.

Brands know that breaches can happen to anyone, and they understand the importance of cybersecurity in today’s data-rich and highly connected business landscape. What companies sometimes forget is that cyber attackers adapt, evolve, and execute faster than preventive technology changes, leaving a gap in what is protected.

As a result, brands are reactively increasing their security budgets to ensure that they aren’t the victim of the next big attack. According to Accenture’s annual Cost of Cybercrime Report, in 2017 companies paid on average $11.7 million for cybersecurity, which is up by 23% compared to 2016(1). But as cybersecurity budgets increase and the cybersecurity landscape evolves, brands have to ask themselves if they’re making the right types of investments.



Cybersecurity is ultimately about protection of computer systems to avoid loss of value, either from stolen data, theft or damage to hardware, or disruption or misdirection of services.

Disinformation and information integrity attacks also cause loss of value. The difference between disinformation and other cybersecurity threats, however, is the extent to which it can be contained. There is no patch or firewall that can stop it. Which begs the question: what is the right approach to defending your brand against a new strain of cyber attack?

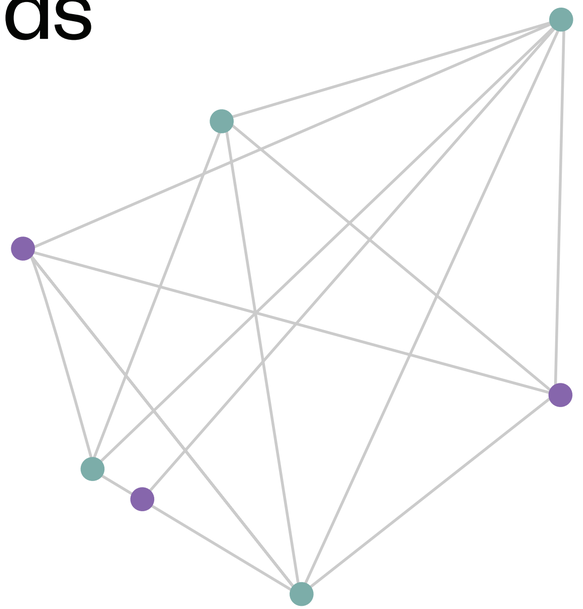
“We tend to think of our cyberdefenses as physical barricades, barring access from would-be perpetrators, and of information campaigns as retrograde and ineffective. In other words, we continue to focus on the walls of the castle, while our enemies are devising methods to poison the air.”

– Phillip Lohaus, American Enterprise Institute (3)

Why Disinformation Is a Growing Cybersecurity Problem

Since the 2016 election, most media coverage of disinformation risk has focused on Russia's interference and mass manipulation of social media in elections. Disinformation isn't just unique to politics though. This problem extends beyond elections, and is a significant problem for brands and other organizations that consumers have come to trust.

But it is not news that social media is being manipulated at a massive scale.

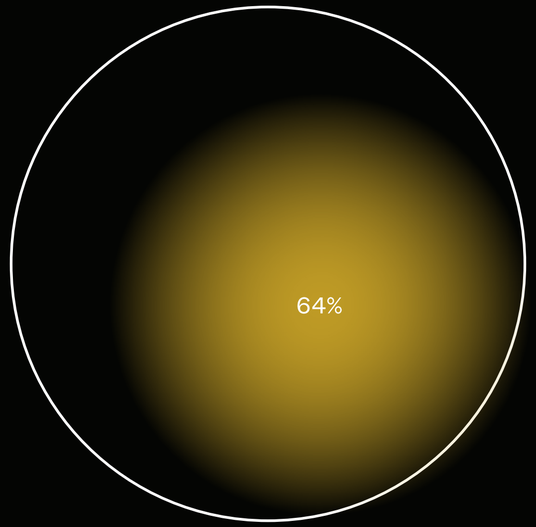


A study from Gallup shows that 64% of Americans think that more than half of the news and information they see on social media is inaccurate(4). And this sentiment is justified.

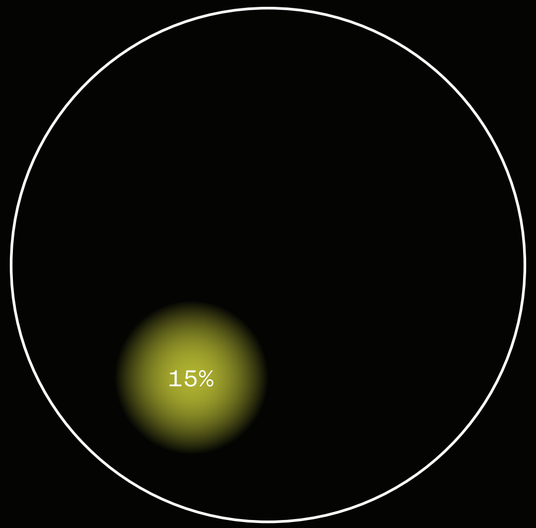
A recent study on botnets found 9-15% of active Twitter accounts are social media bots.(5)

Botnets are just one way that disinformation campaigns can be targeted against brands. But bots are only a small part of the larger threat that disinformation poses. Covert organizations are developing sophisticated tactics that can undermine brand integrity, cost brands money, and jeopardize their external reputation.

In the digital age we live in, where we spread and consume the majority of information online, disinformation is thriving off of a brand's online presences. However, social media companies have been slow to create solutions to protect their users, and in turn this is leaving our entire information ecosystem vulnerable and susceptible to an attack. This requires more than just a fact checking solution, or relying on Facebook and Twitter to ban malicious accounts.



Percent of Americans that think that more than half of the news and information they see on social media is inaccurate(4)



Percent of active Twitter accounts that are bots

Cheap barrier to entry

One of the reasons disinformation can be so damaging is that defamatory campaigns are easy to launch and inexpensive to amplify. All it takes is a small group of people working together to intentionally create a false narrative with social media posts; no coding or hacking required. While more sophisticated campaigns leverage social media advertising and buy bot networks, in general it does not require a big budget to put disinformation campaigns into play.

Social media as an amplifier

Social media has exponentially increased the amount of information we see, as the platforms are designed for virality. In no time at all, a false malicious tweet targeting a brand can be picked up, liked, shared and retweeted by thousands of other users.Before brands have a chance to react, disinformation campaigns can spread and become headlines in coverage from major news outlets.

Jeopardizes brand integrity

Reputation damage can happen in an instant. A social listening tool can tell brands when they receive hundreds of new mentions in minutes, but can’t detect whether the campaign is orchestrated or authentic, or where the narrative originated. Whether it’s fake accounts spreading rumors or coordinated groups leaving fake reviews, disinformation hurts your reputation. A disinformation threat has the ability to undermine a brand’s reputation, sentiment, and most importantly the trust it has built with its consumers over years.

The Cost of Disinformation

A disinformation campaign can be financially devastating for the brand experiencing it. Disinformation does not discriminate.

The goal is to cause most harm to public perception of the brand. Without any form of disinformation defense, the damages done to a brand can be costly.

Disinformation often influences public perception and brand sentiment, and this can have a negative impact on key parts of business like sales, customer retention, and stock prices. This ultimately can cost brands millions of dollars between money lost, and money spent on hiring corporate comms teams, developing a crisis management solution, and running counter campaigns to diffuse the controversy.

But the costs of disinformation aren’t only financial. It also costs brands their time.

Fighting Back

To combat this evolving threat, we have to address those structural weaknesses, but as platform features change and determined adversaries find new tactics, it often feels like whack-a-mole. It's time to change the way we think about disinformation to be more like how we think about cybersecurity, and to take action accordingly.

Emerging technology can play a large role in providing the appropriate defense needed in fighting disinformation. Artificial intelligence can equip brands with sophisticated technologies that can help to proactively monitor ongoing social conversations and detect coordinated disinformation attacks.

The challenge lies in brands adopting these new technologies and utilizing their capabilities.

New Knowledge helps brands defend themselves against disinformation.

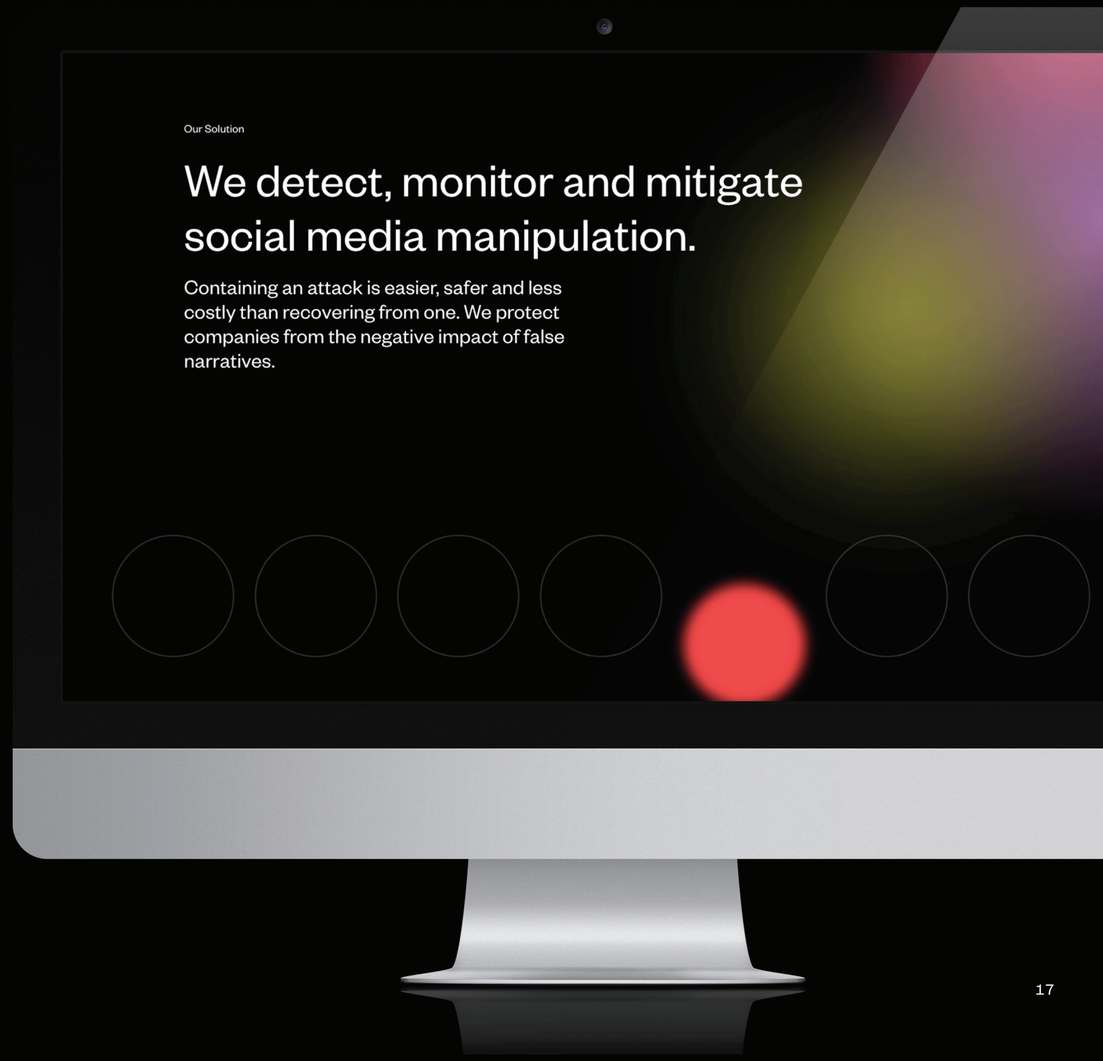
In the age of information warfare, a durable solution that defends companies from disinformation attacks needs to be a part of every brand's cybersecurity strategy. It's up to brands to take action, and make the right investments in robust disinformation defense.

New Knowledge has created the first disinformation defense solution for brands and organizations. By leveraging next-gen technology like advanced AI, New Knowledge can proactively detect, monitor, and defend brands from disinformation attacks before they happen.

The New Knowledge solution provides brands with access to all the resources they need to protect their brand reputation.

With a team of national security, technology, and disinformation experts, we're helping leading brands protect themselves from damaging attacks.

Industries from entertainment to agriculture to energy have become the focus of state-sponsored hostile actors as well as economically or ideologically-motivated networks of anonymous trolls. It's time for companies to move toward embracing new technology, and toward treating disinformation as a part of a comprehensive cybersecurity strategy.



“This will be one of the defining threats of our generation. Influence operations exploit divisions in our society using vulnerabilities in our information ecosystem. They take advantage of America’s commitment to freedom of speech and free flow of ideas.”

– Renee DiResta, New Knowledge Director of Research

About New Knowledge

New Knowledge defends brands against disinformation and protects the integrity of information ecosystems. Our technology monitors the digital landscape to detect subversive campaigns before they can undermine or hijack a brand's narrative. Through advanced machine learning and artificial intelligence, we help our clients protect themselves against disinformation before it can tarnish their brand. We are dedicated to defending public discourse and preventing the manipulation of public trust.

Sources

1. Accenture, Cost of Cyber Crime Study, 2018. Report.
2. Ponemon Institute & HP research, Annual Cyber Security Study, 2017
3. Lohaus, Phillip. From Cybersecurity to Information Warfare, 2017. Article.
4. Statista, Perceived level of accuracy on social media in the U.S. 2018, 2018. Study.