GLASSWALL

A LOOK AHEAD

10 CYBERSECURITY PREDICTIONS FOR 2019

INTRODUCTION

2018 was a year of major cyberattacks, from all-too-common hacks, ransomware and phishing to new, sophisticated crypto-jacking. The year also brought dramatic privacy developments through enactment of the European General Protection Regulation (GDPR) and passage of the California Consumer Privacy Act, both of which are sure to bring major changes to data handling practices the world over. As artificial intelligence and machine learning advance, bad actors develop increasingly sophisticated and stealthy attacks that go undetected for longer periods of time.

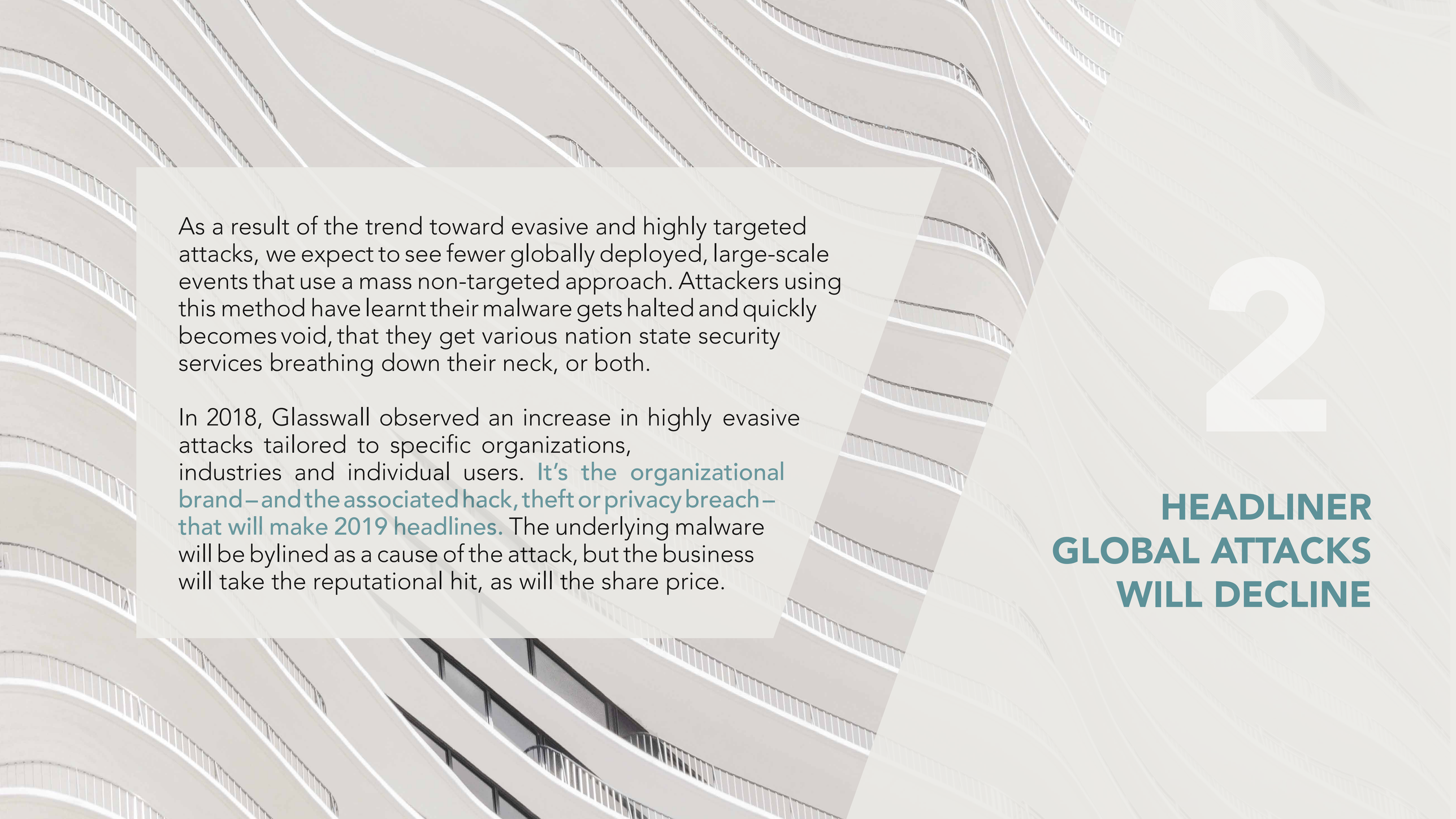
The digital landscape is becoming ever more challenging. Based on what we're already seeing first-hand with our customers and in the market, we've developed some thoughts on what 2019 likely has in store.

IF IT ISN'T BROKEN, DON'T FIX IT!

1

Malicious actors know that sending weaponised email attachments is their most successful payload delivery method – because it gets results – and they will continue to use it as their weapon of choice in 2019. Weaponized email attachments such as PDFs and Microsoft Office documents will continue to trick even savvy users because of the sophisticated customisation and targeting capabilities attackers now utilize.

Stolen personal and company data, when combined with advanced social engineering tactics, will make it ever more challenging for users to distinguish malicious from harmless content, especially when it convincingly references relevant business information or actions, and appears to come from trusted sources.



As a result of the trend toward evasive and highly targeted attacks, we expect to see fewer globally deployed, large-scale events that use a mass non-targeted approach. Attackers using this method have learnt their malware gets halted and quickly becomes void, that they get various nation state security services breathing down their neck, or both.

In 2018, Glasswall observed an increase in highly evasive attacks tailored to specific organizations, industries and individual users. It's the organizational brand – and the associated hack, theft or privacy breach – that will make 2019 headlines. The underlying malware will be bylined as a cause of the attack, but the business will take the reputational hit, as will the share price.

2

HEADLINER GLOBAL ATTACKS WILL DECLINE

CYBERSECURITY WILL SHIFT UP THE LIST OF BUSINESS RELATIONSHIP PRIORITIES

Malicious actors' use of supply chain partners and vulnerable or poorly secured third-party products and services will escalate as an attack vector. That will escalate the importance of building business relationships and reputations that focus on mutually protective cybersecurity. Attackers will increasingly exploit vulnerable down-chain business partners (who may not have large cyber security budgets) to penetrate up-chain targets, through disguising their activities as normal-course-of-business communications that carry less suspicion; a malicious file hidden amongst millions of emails is a perfect weapon.

For instance, a manufacturer might work with a supply chain partner who regularly submits machine-generated reports as spreadsheets, sent unencrypted. Attackers who notice the predictable patterns, workflows, source and recipient of documents can use that information to slip under the radar and reach their victim organization – the manufacturer. The same could apply to other industries that rely on the flow of certain document types, such as Word documents between law firms or PDFs in financial services for T&C's. Identifying malicious files in these kinds of situations is extremely challenging, requiring a proactive, not reactive, approach.

4

ATTACKS WILL BE DYNAMIC, BROADER, AND HARDER TO DETECT

Malicious actors' will continue using evasive methods, such as a single email sent from a single email address to a single user, **but will also employ a highly dynamic and broad range of techniques within a single attack that could last for days.** For instance, using multiple file types like PDF and Microsoft Office, alternating between document features like macros and DDE, and utilizing a broad spectrum of malware, ransomware or embedded phishing links – all add up to cyber threats that are extremely challenging to detect and prevent. That can easily leave cybersecurity teams chasing multiple events that at first glance do not appear related.

These evasive techniques will ultimately lead to an increase in post-penetration dwell time, bucking the trend of recent modest declines. The massive Marriott breach announced in late 2018 perfectly embodies this situation. Sophisticated techniques enable attackers to stay undetected longer, gather intelligence, delay payload launch and then simply leave no trace through the use of 'file-less' malware. This elusive type of malware typically allows total control over an end point, and in a highly innovative move removes its existence from memory without leaving traditional host artifacts for discovery. The result is maximized reconnaissance and theft opportunities while ensuring the malicious actor is nowhere near the crime scene.

5

SECURITY AUTOMATION WILL TAKE CONTROL OF SIMPLER TASKS, WITH A CAVEAT

The persistent global shortage of information security professionals will accelerate broader adoption of automation and seamless orchestration (ASO) in a rush to normalize lower-level processes. However, customers will demand that these products *do not fail* at their primary task of preventing cyber-attacks.

In turn, instead of today's dominance of proprietary protocols, **customers will demand seamless integration across platforms and among security point solutions.** They will move away from point technologies that offer little to no integration, and migrate to those that deliver seamless access to structured and unstructured Threat Intelligence data.

2019 WILL BE THE YEAR OF GOVERNANCE

6

Successful and smart security investments that leverage the aforementioned ASO will depend on a robust governance structure that ensures cybersecurity supports the business or mission needs. Realistically, ASO will only be successful if defined by good processes, which is especially important with regard to cloud computing: Cloud providers do not, contractually or otherwise, assume any liability for your risk, as is the case with violations of GDPR.

Successful ASO places significant importance on the why, what and how for organizations using third parties such as cloud services, and drives correct governance, policy, process, procedure and cybersecurity measures accordingly.

TRUTH WILL MAKE A COMEBACK

Citizens will demand a reckoning between themselves, social media providers and their respective political leaders as to what is true information, who is considered the voice of the “press” and what can be done to regulate it. In light of mounting corporate and political scandals, public pressure may lead to increased regulation, as the effects of the GDPR ripple beyond Europe to demonstrating the power of the citizen overshadowing those organizations who store, and profit from, their personal data.

This shift will also positively affect the ways that social media and large data companies monetize customer data; more savvy citizens will ensure that privacy starts making a gradual comeback.

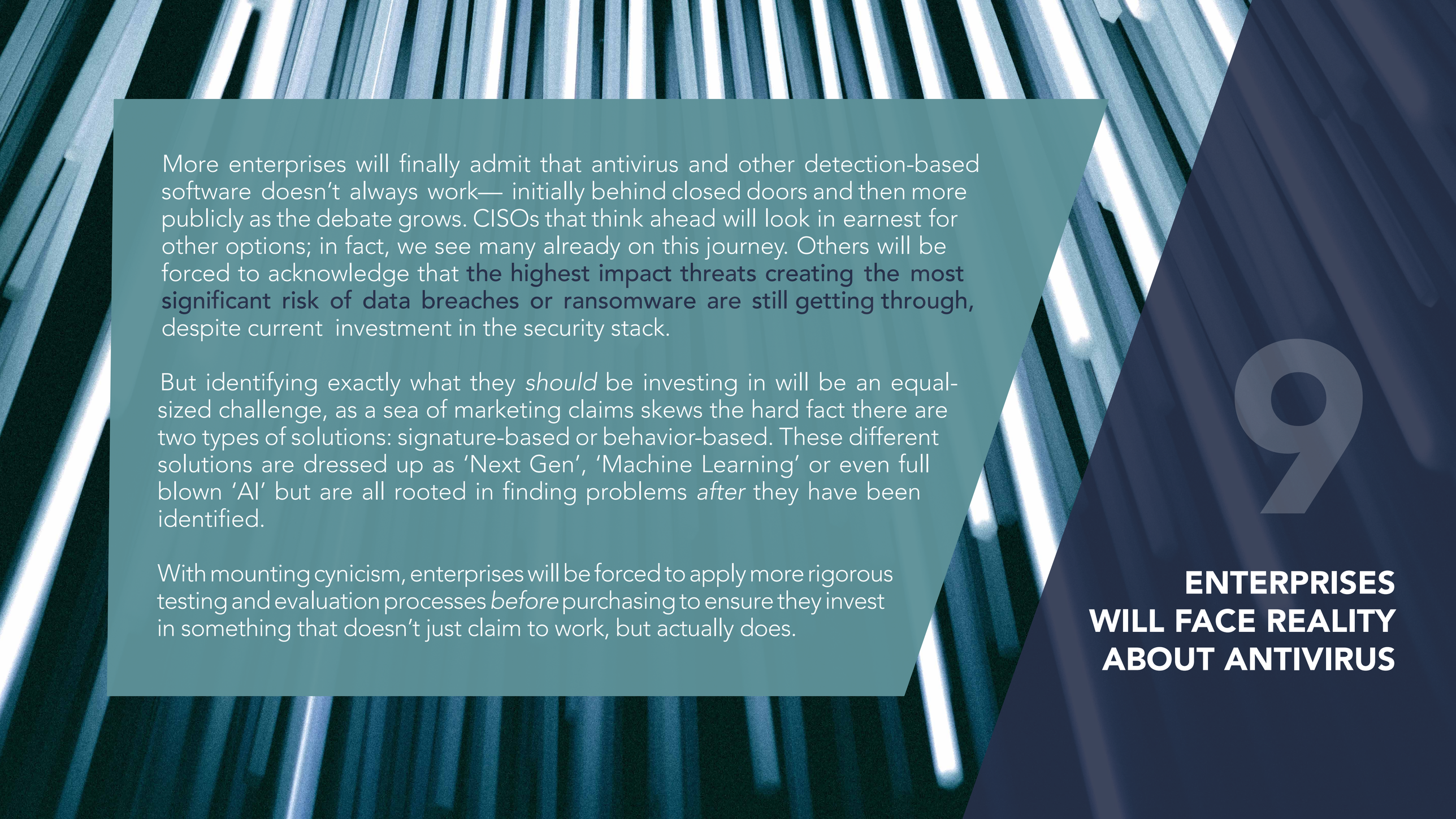
Beyond social media, democratic institutions will be put at risk if fact and opinion, already blurred within mainstream media outlets, cannot be differentiated across social media platforms.

CUSTOMERS' SECURITY DEMANDS WILL FORCE A SHIFT IN DATA PROTECTION

Use of data encryption and sanitization will increase as more savvy consumers understand that the infrastructure of the internet is inherently untrustworthy, and that the 'smart' products and services they consume are equally exposed to trust issues. The move to encryption and sanitization will compel organizations to change their approach to digital security, having it built-in rather than bolted-on to avoid as many risks as possible.

A good example of this practice is train tunnels, with their various signals, circuit breakers and safety features built-in to avoid every possible catastrophic scenario. They're carefully designed from the start with safety as the top priority. Now consider web cameras, built to lowest cost, yet deployed by the hundreds of millions and exploited in the wild to massive effect; we can only imagine security being a cursory mention during development.

With most products and projects that are powered or enhanced by Information Technology, security still follows the original requirement but it never truly catches up.



9

ENTERPRISES WILL FACE REALITY ABOUT ANTIVIRUS

More enterprises will finally admit that antivirus and other detection-based software doesn't always work— initially behind closed doors and then more publicly as the debate grows. CISOs that think ahead will look in earnest for other options; in fact, we see many already on this journey. Others will be forced to acknowledge that **the highest impact threats creating the most significant risk of data breaches or ransomware are still getting through,** despite current investment in the security stack.

But identifying exactly what they *should* be investing in will be an equal-sized challenge, as a sea of marketing claims skews the hard fact there are two types of solutions: signature-based or behavior-based. These different solutions are dressed up as 'Next Gen', 'Machine Learning' or even full blown 'AI' but are all rooted in finding problems *after* they have been identified.

With mounting cynicism, enterprises will be forced to apply more rigorous testing and evaluation processes *before* purchasing to ensure they invest in something that doesn't just claim to work, but actually does.

10

WE'LL SEE A MAJOR CYBER ATTACK ON CRITICAL NATIONAL INFRASTRUCTURE

Across 2018, there has been increasing media focus on news that Critical National Infrastructure (CNI) across the globe is significantly vulnerable and at risk. In the last decade, attacks on CNI have already been used in politically motivated or defensive nation state retaliation situations, such as with the Stuxnet worm and, more recently, the attack on Ukraine's power grid that used weaponized email attachments to cripple the system for days.

Operators of CNI have for years been squeezed on profit margins; seeking efficiencies, they've started to leverage third party cloud services to assist in running the systems that manage the CNI infrastructure, opening up a new set of cybersecurity challenges in an already high-risk scenario.

With the combination of highly complex and sometimes aging environments, third-party cloud services and known vulnerabilities across multiple legacy systems, 2019 will likely see another significant cyber-related attack on CNI that will make everyone, regardless of country, feel very vulnerable indeed.

ABOUT GLASSWALL

Glasswall has offices in London and across the United States, and provides organizations and governments with unique protection against advanced and unknown cyberthreats in documents through its innovative, ground-breaking security technology. The forensic data that Glasswall provides delivers an essential insight into threats already within networks and through its Glasswall FileTrust™ for Email security platform and SDK, provides fresh insight into unknown and as yet undetected cyberthreats. With Glasswall, key cybersecurity decision-makers are better equipped with actionable intelligence to immediately act, respond and set compliance standards to meet crucial data security requirements.

GLASSWALL

TELEPHONE
UK: +44 (0) 203 814 3890
USA: +1 (866) 823 6652

EMAIL
sales@glasswallsolutions.com

WEBSITE
www.glasswallsolutions.com