NOTIFIABLE DATA BREACHES (NDB) SCHEME

Preparing for Australia's new privacy Amendment Act 2017

WHITE PAPER

INTRODUCTION

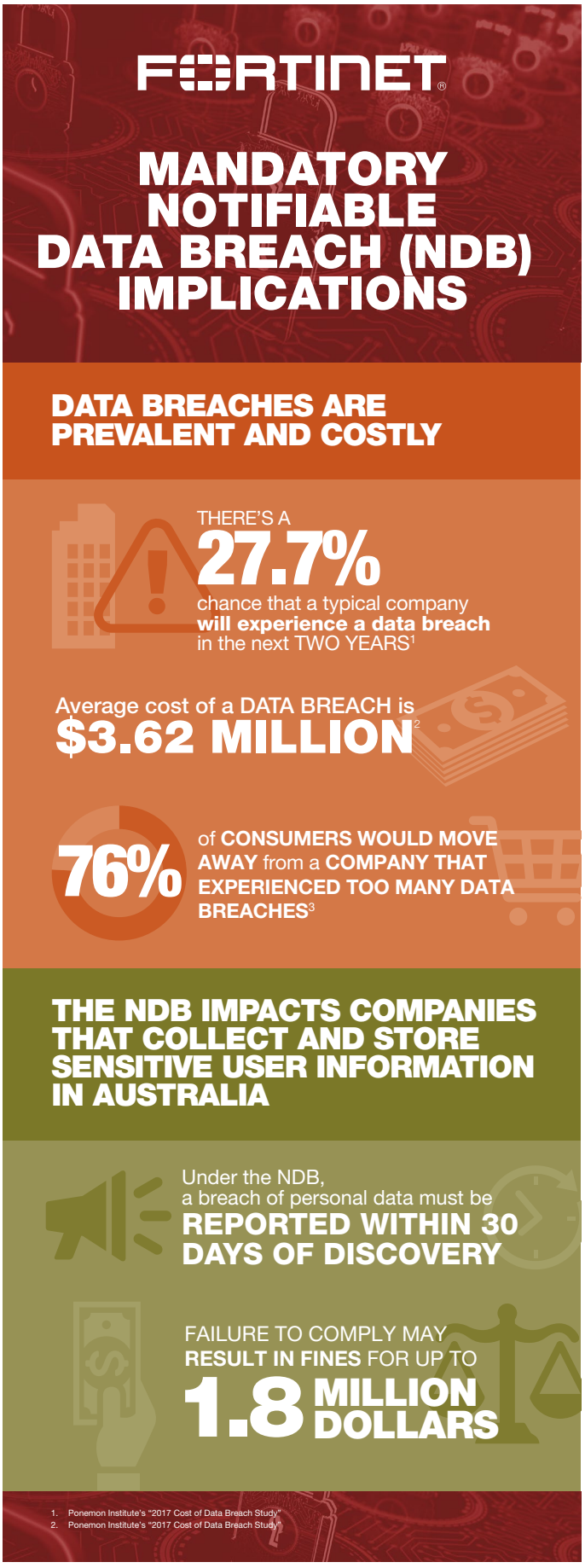
Mandatory notifiable data breach (NDB) scheme will transform how all enterprises prioritise and invest in cybersecurity infrastructure. While Australia's new Data Notification Law directly impacts companies with turnover of $3 million and over. Its implementation will also put pressure on smaller businesses to provide greater transparency to their customers. Research suggests that more than half (55%) of consumers worldwide will abandon online purchases if they harbour privacy concerns about the merchant – no matter its size.[1]

All industries, not just those with traditionally higher compliance burdens like finance and legal, must now comply with the new laws – a nod to the fact that personal and sensitive data is collected in most customer transactions today, irrespective of industry. And with similar laws like the European Union's General Data Protection Regulation (GDPR) coming into play, Australian businesses will require rigorous detection and response to not only comply at home, but also in overseas markets.

Many larger enterprises are already bracing for the significant costs of overhauling their cybersecurity platforms and policies. To do so effectively, however, they will need to focus not just on smarter technology but on a more rigorous methodology around detecting, identifying, and responding to potential breaches. A "security by design" approach, where security is built into all processes and protocols from the ground up, offers the most efficient and cost-effective means for companies to stay compliant and improve their threat readiness levels up to today's speed.

This whitepaper examines the contents and implications of recent Australia's NDB scheme, examining some of the key network security challenges posed by its reporting and regulatory burdens. While IT faces increasing complexity and total volume of potential threats to process, a wisely-architected and well-integrated approach to technology and policy – what we call "security by design" – can not only minimise the risk of noncompliance, but harden defence and detection measures in an efficient and sustainable manner.

A company's ability to report and fix data breaches has always affected its "licence to operate" in the minds of customers. Australia's new legislation only turns that marketplace truth into regulatory fact. Now, more than ever, businesses must invest in strong monitoring and response to thrive and repel any risks to personal data.



[1] https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

WHAT IS NOTIFIABLE DATA BREACHES SCHEME?

The Privacy Amendment (Notifiable Data Breaches) Bill 2016, or NDB bill, requires all organisations covered by the Australian Privacy Act 1988 (Privacy Act) notify any individuals who are likely to be at risk of serious harm in the event of data breach. The NDB bill also recognises the importance of timeliness in any cybersecurity situation: organisations have only 30 days to investigate and notify the public after evidence of a serious data breach has surfaced.

The NDB bill only affects Australian companies of $3 million annual turnover or more, although businesses of all sizes are recommended to abide by the new standards as closely as possible. Ensuring fast, comprehensive data breach notification gives customers a chance to minimise potential damage to their property or person caused by any breach, while also legislating a far higher standard of accountability than Australian industries have provided to regulators and the public alike thus far.

WHAT WOULD CONSTITUTE A NOTIFIABLE BREACH?

Notifiable breaches include any data breach that might result in serious harm to any individual whose data is involved. The Office of the Australian Information Commissioner, the government agency in charge of managing and enforcing notification, has ultimate arbitrage over what constitutes a notifiable breach or not.

DATA BREACHES OCCUR WHEN PERSONAL INFORMATION HELD BY AN ORGANISATION IS EITHER LOST, OR SUBJECTED TO UNAUTHORISED ACCESS OR DISCLOSURE. EXAMPLES OF A DATA BREACH INCLUDE (BUT ARE NOT LIMITED TO):

- Theft or loss of a device containing customers' personal information – even if there is no proof the data has been exploited or accessed;
- Malicious forced access (hacking) of a database containing personal or personally-identifiable information; or
- The incorrect provision of one person's data records to someone else.

ACCOUNTABILITY & GOVERNANCE

To comply with the NDB bill, Australian companies must demonstrate that they have adopted appropriate governance measures including detailed documentation, logging, continuous risk assessment and remediation. Cybersecurity should, as far as possible, be an integral part of all systems from the outset, rather than a measure applied in retrospect.

That, of course, poses obvious challenges to businesses operating legacy systems and infrastructure. For these businesses, network-level security plays an even more critical role in data breach notification compliance. While redesigning legacy systems with inbuilt, native data protection may take a long time, network-level measures can be rolled out relatively quickly – making them the first, and often, in the short-term the last line of defence for these companies.

To maintain "evergreen" relevance as technologies change, the NDB bill makes little explicit mention of any specific technologies required to ensure compliance. Companies should nevertheless focus on the fundamentals of cybersecurity – rigorous monitoring, across as many attack vectors as are known, coupled with processes and platforms for quick response – if they want to maintain their licence to operate in today's increasingly high-risk digital environment. They may face many challenges to doing so, but none are insurmountable.

NETWORK SECURITY CHALLENGES

MAINTAINING 'STATE OF ART' DEFENCES

Keeping pace with the evolving threat landscape has always been a challenge, even prior to the notifiable data breach scheme. Cybercrime's perceived profitability has turned it into a booming worldwide industry, one with resources and innovation that no individual company, nor national governments, can always defeat.

Part of the problem comes from the way cyber security has evolved, with the discovery of each new attack vector spawning yet another security solution to be added into the mix. Although each such addition may fulfil its role as intended, it does so mostly in isolation, with little or no interaction with the rest of the network security infrastructure. This "break-fix" approach to security not only increases IT's management burden, but can easily lead to gaps and inconsistencies in the response to new threats – especially in today's complex multi-vendor, as-a-service infrastructure environments. And as new technologies like mobile and the Internet of Things add to a company's endpoints – and potential vulnerabilities – maintaining an impermeable network border can prove all but impossible.

One response to new threats is to increase visibility, processing and controls. Doing so, however, creates the same issues faced at most passenger airports today: unacceptable chaos, confusion, and delay, even before any incident occurs. Additional processing also adds complexity, multiplying the number of data points to be aggregated and interpreted when evaluating the best response to any detected event.

BREACH MITIGATION – REDUCING THE ATTACKER'S WINDOW OF OPPORTUNITY

Research in 2016 found that it takes organisations an average of five months to discover that a data breach has occurred. Hackers rely on this window between initial intrusion and the eventual breach detection to inflict the most damage (figure 1). The more time an attacker can spend undetected, accessing personal data, the more brutal the eventual impact – both financially and to the company's reputation. The faster an organisation can detect and respond to the initial intrusion, the smaller the effect the hacker will have on the organisation's operations.

FIGURE 1

Although at times it may be impossible to detect the undetectable, security administrators must prepare for the inevitable, occasional intrusion, while striving to minimise such occurrences and hasten their detection through every means possible. As previously noted, the NDB scheme does not require notification of all security breaches – only those that present a "serious" risk to individuals' personal data. Companies can reduce the severity of any breach by rendering their data opaque, whether through encryption or the use of pseudonymous techniques. However, they still have a responsibility to minimise the time between breach and detection (Figure 2) – something that requires more proactive detection and monitoring.

FIGURE 2

[2] 2016 M-Trends Report

THE "SECURITY BY DESIGN" METHODOLOGY

Compliance with the new data breach notification scheme cannot be achieved through technological upgrades alone. To reduce exposure to the potentially crippling implications of a serious data breach, businesses must minimise both the number of network intrusions, and their time to detection – an approach that requires a robust methodology as much as state-of-the-art technology. Adopting a "security by design" methodology, such as that employed by Fortinet, can weave together disparate cybersecurity systems into a single, seamless whole.

There are three key areas where security by design can reduce the threats to any business – and make it more aware when such threats do occur:

1. STRONG THREAT PREVENTION AND DETECTION

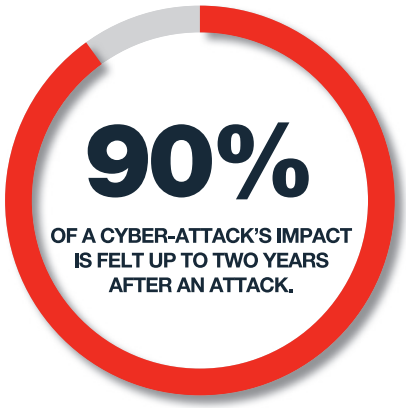
Because an attack can come from a wide range of attack vectors and leverage unknown malware, individual security products and technologies must work together to form a cohesive security fabric that covers the complete network, from the end point to the cloud and beyond. These products must work together collaboratively, eliminating any gaps between products that could be exploited by the hacker or cybercriminal. This multi-layer approach, prevention and detection working together, allows the organization to effectively combat cyber attacks and minimize the occurrence of a data breach severe enough to be reported under the NDB scheme.

2. THE NEED FOR SEGMENTATION

Strong threat prevention and detection are critical components of an organization's cyber security strategy. Another, complementary component should be internal segmentation of the network. Segmentation contains any threat after infiltration, limiting its lateral movement and minimizing the potential damage it can cause prior to detection. Internal segmentation is accomplished by strategically deploying high-performance firewalls as part of the network's internal infrastructure. Such an approach is particularly effective when a user's access rights are enforced by firewall policies: an intruder using compromised login credentials will be blocked by the internal firewall and trigger warning alarms when accessing network areas that the logins aren't authorized for. Internal segmentation also helps to secure sensitive data, keeping it separate from other data stored in the network, which also provides greater visibility.

3. ACTIVE THREAT INTELLIGENCE

A cybersecurity solution can only be effective if it keeps pace with rapid changes in the threat landscape. Due to the rapid change in even existing threats, security systems that cannot keep up will be quickly left behind. Threat intelligence, in the form of continuous and automatic updates, is crucial in maintaining the efficacy of any security system. But threat intelligence cannot be just a one-way flow of information. It must be part of a larger eco-system, incorporating real time attack feedback from field-installed systems along with independent threat research that is eventually redistributed back towards those systems.



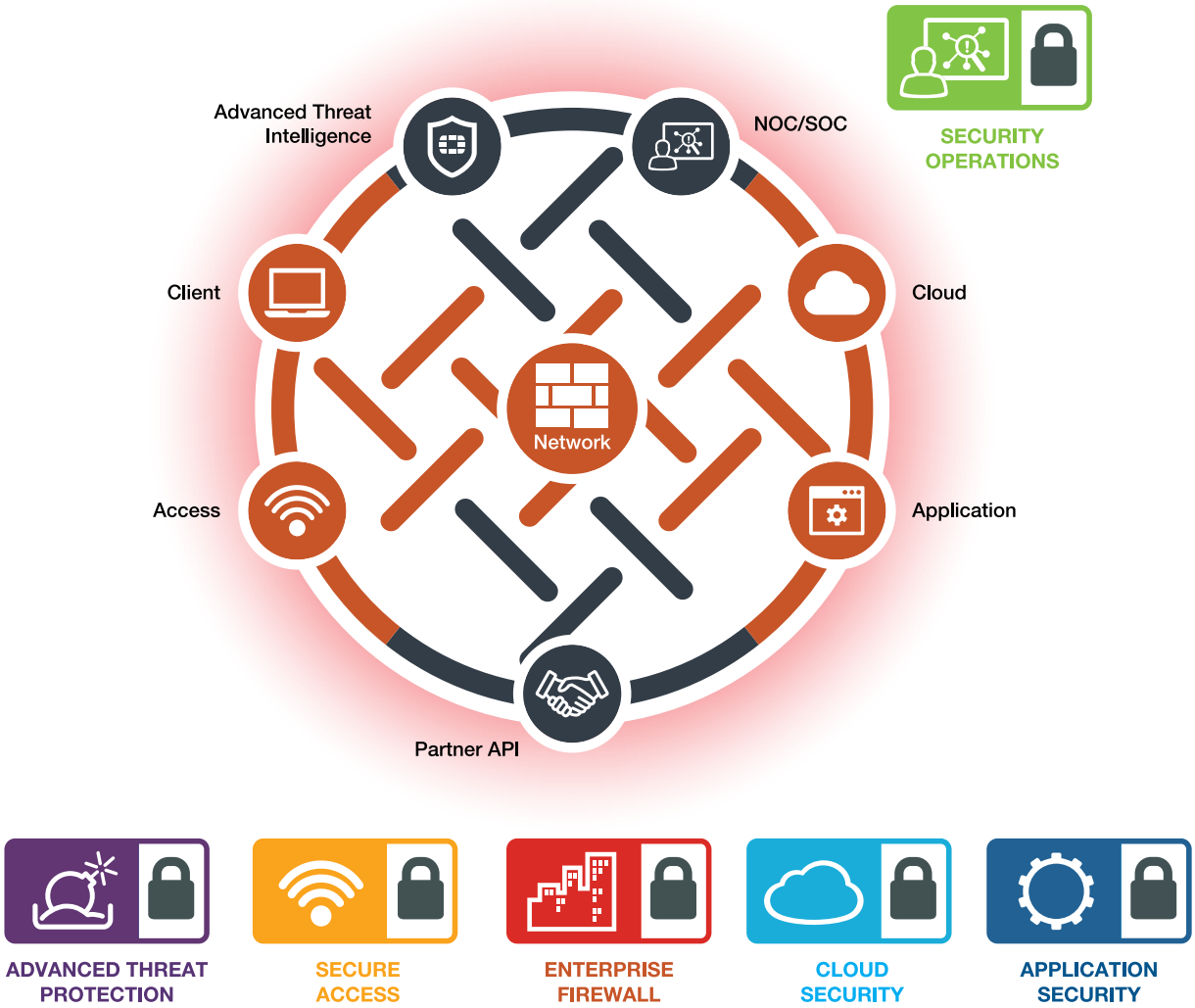
1 https://securityintelligence.com/know-the-odds-the-cost-of-a-data-breach-in-2017/

INTRODUCING THE FORTINET SECURITY FABRIC

As part of their preparations for the upcoming NDB scheme, organisations should be assessing their ability to meet its stringent reporting requirements. They should also take advantage of this internal review to objectively review their overall security posture, identify weak links and plan a strategy to bring their security infrastructure to where it needs to be. And that strategy should include the Fortinet Security Fabric as their security blueprint.

The Fortinet Security Fabric is Fortinet's technology vision for tackling the security problems that enterprises are facing today as well as those of tomorrow. Built upon the tenets of Broad, Powerful and Automated, the Fortinet Security Fabric is comprised of multiple security technologies that work together collaboratively to provide the strong threat prevention and detection capability needed to satisfy the NDB scheme. All of the different technologies in the Fortinet Security Fabric are supported by a single source of threat intelligence ensuring the level of protection is always in step with the threat landscape.

A wide range of product and technologies, organized into logical solution sets provide end to end protection from the desktop to the cloud and beyond.



BROAD

Designed to cover the expanding attack surface of a modem enterprise network, the Fortinet Security Fabric provides protection, visibility and control over every part of the environment, from wired and wireless endpoints, across public and private cloud assets, to the datacentre, and even to the applications themselves.

Combined with dynamic network segmentation that logically separates data and resources, the Fortinet Security Fabric can reach deep into the network to discover new threats as they move from one zone to the next. This broad deployment and deep visibility is a crucial step to compliance, by helping monitor internal traffic and devices, preventing unauthorised access to restricted assets, and limiting the spread of intruders and malware.

Furthermore, the benefits of the Fortinet Security Fabric are not limited to the Fortinet portfolio of security solutions. With open application programming interfaces (APIs), open authentication technology, and standardised telemetry data, a growing ecosystem of Fabric-Ready Partners is emerging, enabling organisations to integrate existing security and networking investments into their own Fortinet Security Fabric.

POWERFUL

With the processing power of many traditional security appliances failing to keep pace with increases in network bandwidth and threat complexity, organisations are often faced with an exponential compromise. Either they must reduce the level of protection, which risks intrusion via an uncovered attack vector or through an unsecured part of the network, or they must accept a drop in application performance across the network.

By offloading security and content processing to dedicated, custom-built Security Processing Units (SPUs) that combine hardware acceleration with highly optimised firmware, Fortinet products have become the fastest in the industry, enabling organisations to establish comprehensive security without compromising on performance.

AUTOMATED

In addition to broad visibility across the entire attack surface and the processing muscle to delve deeper into every packet. the Fortinet Security Fabric can also muster the combined intelligence of its distributed components to rapidly correlate events and coordinate a fast, automatic response appropriate to the level of risk.

As rapidly as new threats are detected, the Fortinet Security Fabric can automatically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware. And as an organization's network grows and adapts to changing business needs, the Fortinet Security Fabric will grow and adapt with it, automatically extending the latest security policies to new devices, workloads, and services as they are deployed, whether local, remote or in the cloud.

SUMMARY

Ensuring compliance to the NDB scheme will take time and investment from most companies. Both are, given the sheer pace of digital transformation and cybercrime's evolution, commodities in increasingly short supply. This compliance journey has no fixed end, but will continue and evolve over the course of any organisation's lifetime. That makes sound fundamentals, like Security by Design, even more important to sustaining compliance and security for the long term.

The Fortinet Security Fabric directly addresses those fundamental questions of policy and technology by harnessing the collective power and intelligence of Fortinet's portfolio of security solutions to deliver benefits greater than those of its parts. Its approach to security revolves around scalable connectivity between solutions, actionable intelligence, and open API standards, giving businesses some of the most comprehensive and responsive end-to-end protection on market today.

Australia's data breach notification scheme have put businesses on notice: they can no longer put security at the back of their priority list. IT should not, however, treat the revised act as yet another burden. Rather, they should view them as an opportunity to gain greater buy-in from the rest of the business on the importance of IT security – and drive further transformation to stay compliant and competitive for the future.

128048 0 1 EN