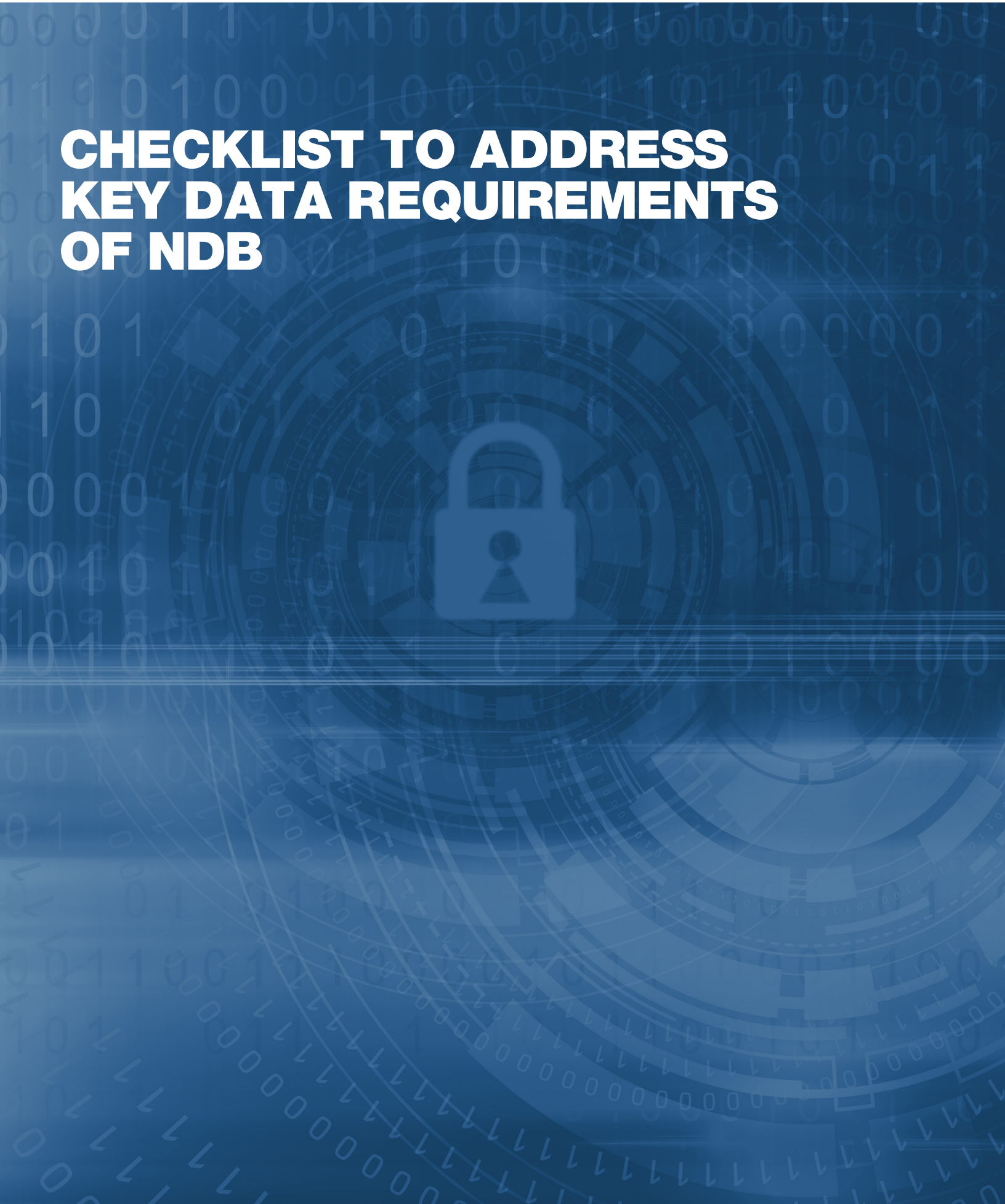
FORTINET

CHECKLIST TO ADDRESS KEY DATA REQUIREMENTS OF NDB



Fines of the Australian Notifiable Data Breach Scheme (NDB) has captured the attention of IT security directors and boards across Australian organisations.

Adherence to the NDB regulations requires state-of-the-art technology for comprehensive data protection—and, in particular, advanced threat prevention and detection—to minimise the possibility of a data breach. According to the nonprofit Center for Internet Security (CIS), most successful attacks exploit poor cyber hygiene.[1] (See call out below for more details.)

In addition to the CIS recommendations[2], businesses affected by NDB need to make sure they have the right technologies in place to protect their environments and detect and mitigate data breaches quickly and effectively, which starts with getting the right security architecture in place.

CIS CONTROLS: 20 ACTION ITEMS

The best starting point for recommendations on thwarting prospective attacks is the 20 CIS Controls. Though tackling all 20 action items in the list of 20 is ideal, organizations can eliminate the "vast majority" of their security vulnerabilities by starting with the top five.

1. Routinely take inventory of company devices, both authorised and unauthorized.
2. Inventory all the authorized and unauthorized software that is in use across the network.
3. Ensure that all hardware and software configurations are secure.
4. Continuously assess vulnerabilities across their network and remediate any problems that they find.
5. Carefully control the use, assignment, and configuration of administrative privileges on all devices and software on their network.

STATE-OF-THE-ART SECURITY ARCHITECTURE

Complexity is the enemy of intrusion prevention and data breach detection and remediation—and, ultimately, an organisation's ability to protect all the personally identifiable information (PII) that it collects and stores. Running an assortment of security technologies from multiple vendors undermines an organisation's ability to detect intrusions. And in the event that an intrusion leads to a data breach subject to NDB, complexity in the security environment can exacerbate the challenge of reporting to the appropriate supervisory authority within 30 days.

To effectively protect the PII it collects and/or stores, an organisation requires a security architecture that is tightly integrated and that includes state-of-the-art systems providing six key capabilities:

1. **Next Generation Firewalls**. The first line of defense against intrusions targeting PII is a Next Generation Firewall (NGFW). Some of the capabilities most relevant to organisations affected by NDB include:

- Multilayered security that uses advanced threat prevention to protect the entire attack surface—all devices, users, and applications. This includes Internet of Things (IoT) devices, many of which were designed with little attention to security (which explains why patch updates are impossible to manage on them), as well as the ever-expanding universe of software-as-a-service (SaaS) and other cloud solutions.
- High-performance security processor (SPU) for application-layer services that protect a corporate network while detecting data breaches hidden in SSL traffic via the industry's fastest SSL inspection engine.
- Single-pane-of-glass visibility and management for simplified deployment and consistent security policy controls. This enables real-time sharing of intrusion information, which accelerates time to detect, neutralise, and stop attempted data breaches.
- Segmentation of network traffic, which minimises the breadth and depth of intrusions and minimises the attacker's opportunity to access protected data.

Fortinet FortiGate NGFWs are the perfect solution for protecting a network against intrusions and preventing data breaches, and they have garnered industry-wide recognition. Gartner placed Fortinet in the "Leaders" quadrant in its 2017 Magic Quadrant for Enterprise Network Firewalls[3], and FortiGate firewalls received a "Recommended" rating for the fourth consecutive year from the NSS Labs NGFW group test.[4]

2. **Endpoint Security.** If firewalls are the first line of defense, endpoint security solutions need to be the second barrier. As corporate networks support increasing numbers—and diverse types—of endpoints, state-of-the-art endpoint security technology becomes crucial for protecting PII and other data. Traditional antivirus and malware systems alone are no longer adequate. The Fortinet FortiClient solution enhances an organisation's ability to stop data breaches from occurring, and moreover to meet NDB reporting requirements in the event of a breach. Relevant capabilities include:

- Protection against advanced threats that could lead to data breaches. Specifically, memory monitoring enables FortiClient to detect and block attacks on unpatched application vulnerabilities.
- Native integration with the Fortinet security architecture, the Fortinet Security Fabric, for real-time updates on emerging threats. Stopping attacks and preventing their intrusion obviates data breaches long before they happen.
- Clear visibility into security on endpoints throughout the company, as well as visibility into any vulnerabilities detected across the organization's attack surface. Updates are available via email alerts and a vulnerability dashboard. The ability to manage endpoint security in real time enables organisations to respond to attacks and prevent and mitigate their intrusions faster and more effectively.

Just like FortiGate NGFWs, FortiClient has garnered industry recognition, including a 2017 "Recommended" rating from NSS Labs for Advanced Endpoint Protection solutions.[5]

3. **Email Gateway Security.** Email security is crucial; a recent report found that two-thirds of malware was installed this way.[6] For companies trying to secure their networks and data against cyber attacks, a secure email gateway (SEG) is a must-have. A sophisticated SEG, FortiMail from Fortinet blocks ransomware, phishing, and other threats to PII using:

- Multilayered antispam technology that uses more than 12 sender, protocol, and content inspection techniques—from IP and domain assessments to recipient verification and sender policy framework (SPF) checks—to shield the network and users from unwanted bulk emails. As these often include embedded exploits for intrusion, organisations can stop them before they enter their email network.
- Anti-malware capabilities that combine static and dynamic technologies, including signature, heuristic, and behavioral techniques. The same applies here; ensuring that malware does not make it to user mailboxes stops attacks before they enter your network.
- A robust set of data protection capabilities, including data loss prevention, email encryption, and email archiving technologies. Ensuring your users are not sending out confidential and private data, as well as encrypting emails with PII, is critical to any organisation seeking to prevent data breaches.

FortiMail is recognized for its superb threat detection efficacy. For example, after blocking nearly 750 different unique new and little-known threats in a laboratory test, it was awarded "Advanced Threat Defense (ATD) certification by ICSA Labs.[7]

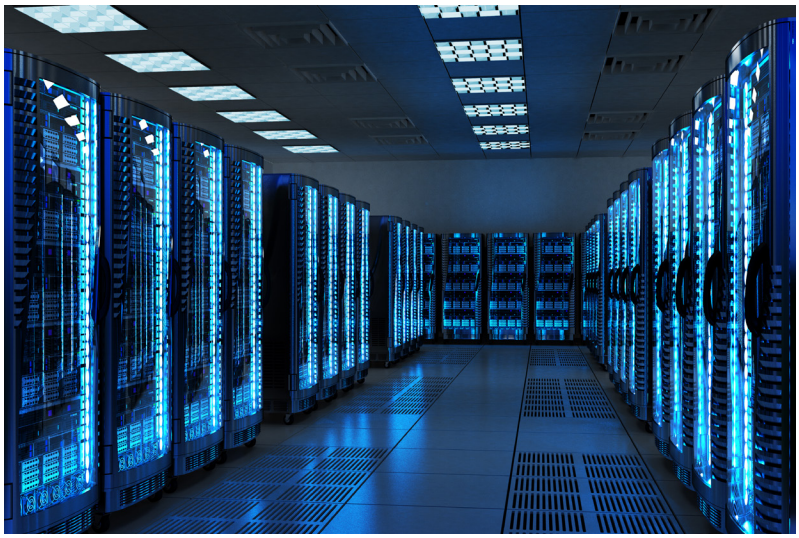
4. **Web Application Security.** Hackers may use sophisticated techniques, such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning, to turn web applications into an access gateway. Protecting PII against these threats requires a multilayered approach to web application security. Some of the key ways in which FortiWeb web application firewalls enable organisations to protect against malicious intrusions include:

- Multiple layers of technology that identify threats through techniques such as IP reputation analysis, DDoS protection, protocol validation, examination of attack signatures, antivirus, and data loss prevention capabilities. Once again, stopping intrusions before they occur eliminates the possibility of data breaches.
- A behavior-based detection engine that intelligently identifies any threats that stray from typical patterns of web traffic. This is particularly important in identifying unknown threats.
- Native integration into the Fortinet Security Fabric that enables regular updates on emerging threats and the ability to share information about any exploits they detect. As discussed earlier, cyber hygiene is a foundational element in any intrusion prevention and detection strategy.

Like the other Fortinet solutions discussed, FortiWeb also received a "Recommended" rating from NSS Labs in its 2017 Web Application Firewall Test.[8]

5. **Comprehensive Management and Reporting.** In 2016, cyber attackers who successfully entered a corporate network had on average,107 days to wreak havoc before the intrusion was detected.[9] Reducing the length of time an intruder can explore the network limits their opportunity to initiate a data breach. Thus, the speed with which an organisation can detect and mitigate intrusions is crucial to preventing data loss.

   To effectively shrink a prospective criminal's window of opportunity, an organisation must ensure that all its security devices are performing at all times. For this purpose, Fortinet offers a suite of products for security solution management—FortiManager, FortiAnalyzer, FortiSIEM, and FortiCloud—which, when combined, centralise the management of security devices across the network. Some of their core capabilities include:



- Streamlined visibility into security policy and device management. FortiManager enables network and security operations staff to initiate and synchronise a coordinated response to detected threats, and to manage security policies across all Fortinet devices and third-party solutions that are part of the Fortinet Security Fabric. It also offers the industry's best scalability, managing up to 100,000 Fortinet devices—not including third-party devices that are part of the Fortinet Security Fabric—through a single pane of glass. Here, rapid incident response is often critical in stopping or minimising data breaches, which is key when it comes to NDB.
- Centralised visibility into log and event data from security solutions companywide. FortiAnalyzer automatically retrieves and scans security logs, notifying the IT security team via dashboards and alerts anytime they detect a sign of compromise. Once again, rapid incident response is critical to NDB.
- Analytics technology that aggregates and cross-correlates information from diverse sources, such as logs, performance metrics, and SNMP traps. FortiSIEM dynamically auto-discovers physical and virtual systems attached to the network and pulls information about these systems' configurations into a centralized management database (CMDB). By cross-correlating performance, event, and log data in real time, FortiSIEM provides a holistic view of threats across the organisation's entire attack surface.
- Visibility into security systems from anywhere in the world. FortiCloud provides a web-based console that can be used to centrally control, and even deploy, all Fortinet Security Fabric devices—Fortinet and third party. This rapid management and deployment of devices can mean the difference between a successful or unsuccessful intrusion or data breach.

6. **Secure Access Layer.** The number and types of devices connecting to corporate networks continue to grow exponentially. Further, users want fast Wi-Fi, but organisations must also secure wireless access to their networks in order to minimise the chance of an intrusion and subsequent data breach. Fortinet Secure Access solutions include the ability to:

- Centralise identity management and user identification. FortiAuthenticator utilises a range of user identification methods to ensure that devices connecting to the corporate network receive only the appropriate role-based access privileges.
- Secure access switches for an added layer of security. FortiSwitch products use device detection, DHCP snooping, and syslog collection that augment intrusion prevention and data protection within FortiGate NGFWs.
- Solutions in the FortiToken line generate OATH-compliant, time-based one-time password (TOTP) tokens, an affordable second factor for companies moving to two-factor authentication. This enables organisations to ensure that only those who are authorised have access to specific applications.

ADVANCED THREAT PREVENTION AND DETECTION

To be successful in intrusion prevention and detection, as well as data breach incident response, organisations require advanced threat protection and detection capabilities. These fall into two buckets:

- **Threat Intelligence.** Organisations require advanced security intelligence to stay on top of incoming threats. Using this industry-leading research, FortiGuard pushes out real-time updates about emerging exploits. Fortinet maintains regular product updates and patches, prioritised for specific attacks, that quickly close the gap when new vulnerabilities are identified.
- **Sandboxing.** Identifying previously unknown attacks is a requirement, and sandboxing techniques are becoming increasingly prevalent as part of the security strategy to stop them. FortiSandbox enables organisations to not only receive automated updates about emerging security concerns but also share their own discoveries as real-time updates sent to their other security products. The inclusion of FortiSandbox infuses a layer of advanced threat protection throughout the Security Fabric. And as with other solutions from Fortinet, FortiSandbox is at the top of the options, recognised, as an example, with a “Recommended” rating by NSS Labs for Breach Detection Systems.[10]

FINAL CHECKLIST ITEMS

If you are impacted by NDB, then you have no time to wait. Point products and security platforms are not your answer when it comes to comprehensive, end-to-end intrusion prevention and detection and data breach prevention and detection solutions. This is where the Fortinet Security Fabric excels. The upside is that the different pieces are best in class, with the aggregate adding up to more than the sum of the parts.

Beyond the real-time visibility and controls that organisations get from the Fortinet Security Fabric, they also get a follow-the-sun model with FortiCare 360, both advanced technical services and rapid hardware replacement when failures do occur. This is particularly important when you are talking about data breaches underneath the umbrella of NDB.

[1] John M. Gilligan, "It Is Time to Get Serious About Securing Our Nation's Critical Infrastructure," Center for Internet Security blog, October 30, 2017.

[2] "CIS Controls," Center for Internet Security, accessed December 5, 2017.

[3] Adam Hils, Jeremy D'Hoinne, and Rajpreet Kaur, "Magic Quadrant for Enterprise Network Firewalls," Gartner, July 10, 2017.

[4] "Next Generation Firewall," NSS Labs, accessed December 5, 2017.

[5] "Advanced Endpoint Protection," NSS Labs, accessed December 5, 2017.

[6] "2017 Data Breach Investigations Report," Verizon, accessed December 5, 2017.

[7] "Advanced Threat Defense Certification Testing Report," ICSA Labs, October 2, 2017.

[8] Matthew Chips, "Web Application Firewall Test Report," NSS Labs, April 11, 2017.

[9] "2017 Trustwave Global Security Report," Trustwave, June 2017.

[10] "Breach Detection System," NSS Labs, accessed December 5, 2017.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

150565-A-0-EN December 15, 2017 12:29 PM
checklist-gdpr-121517-1229pm