STATE-OF-THE-ART DATA PROTECTION FOR GDPR

7 Considerations and Where Fortinet Can Help
The extensive requirements and substantial fines of the European Union’s (EU’s) General Data Protection Regulation (GDPR) have captured the attention of IT security directors around the world. For companies that do business in the EU, now is the time to shore up security processes.

Adherence to the GDPR regulations requires state-of-the-art technology for comprehensive data protection—and, in particular, advanced threat prevention and detection—to minimize the possibility of a data breach. According to the nonprofit Center for Internet Security (CIS), most successful attacks exploit poor cyber hygiene.¹

Businesses affected by GDPR 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.
1. First Line of Defense. The first line of defense against intrusions targeting PII is a Next Generation Firewall (NGFW). Some of the capabilities most relevant to organizations affected by GDPR 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, neutralize, and stop attempted data breaches.
- Segmentation of network traffic, which minimizes the breadth and depth of intrusions and minimizes 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, and FortiGate firewalls received a “Recommended” rating for the fourth consecutive year from the NSS Labs NGFW group test.
2. Protect the Endpoint. 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 organization’s ability to stop data breaches from occurring, and moreover to meet GDPR 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 organizations 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.4

3. Secure Your Email. Email security is crucial; a recent report found that two-thirds of malware was installed this way.5 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 antispm 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, organizations 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 organization 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.6
4. Guard Your Web Applications. 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 organizations 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.

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. 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 organization can detect and mitigate intrusions is crucial to preventing data loss.

To effectively shrink a prospective criminal’s window of opportunity, an organization 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, centralize 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 synchronize 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 minimizing data breaches, which is key when it comes to GDPR.
- Centralized 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 GDPR.
- 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 organization’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 organizations must also secure wireless access to their networks in order to minimize the chance of an intrusion and subsequent data breach. Fortinet Secure Access solutions include the ability to:

- Centralize identity management and user identification. FortiAuthenticator utilizes 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 organizations to ensure that only those who are authorized have access to specific applications.

7. **Advanced Threat Prevention and Detection.** To be successful in intrusion prevention and detection, as well as data breach incident response, organizations require advanced threat protection and detection capabilities. These fall into two buckets:

- **Threat Intelligence.** Organizations 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, prioritized 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 organizations 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, recognized, as an example, with a “Recommended” rating by NSS Labs for Breach Detection Systems.³
FINAL CHECKLIST ITEMS

If you are impacted by GDPR, 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 organizations 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 GDPR.


