HOW THE NEXT-GENERATION SECURITY PLATFORM CONTRIBUTES TO GDPR COMPLIANCE

The General Data Protection Regulation is the European Union's forthcoming personal data protection law. In May 2018, the GDPR will replace the 1995 Data Protection Directive, significantly changing the rules surrounding protection of personal data of EU residents. The GDPR is much stricter than its predecessor, with greater scope of coverage – including companies outside the EU – as well as new data breach notification requirements and administrative fines. While the vast majority of GDPR requirements center around data management, data security is also a pillar of GDPR: the law requires security of data processing, accounting for the state of the art. The Palo Alto Networks Next-Generation Security Platform can help with organisations' security and data protection efforts related to GDPR compliance by assisting in securing personal data at the application, network and endpoint level, as well as in the cloud. It can also assist in understanding what data was compromised in the unfortunate instance of a breach, but first and foremost it will help organisations prevent data breaches from happening at all.

OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION

What is the law? The General Data Protection Regulation is the European Union's forthcoming personal data protection law. In May 2018, the GDPR will replace the 1995 Data Protection Directive, significantly changing the rules surrounding protection of personal data of EU residents. The GDPR aims to provide Europeans with greater say in how their personal data is collected and managed, particularly in light of technological advances over the last 20 years. Under the GDPR, individuals have many rights, including access, rectification and erasure of personal data held on them (the so-called right to be forgotten), and the right of data portability. The GDPR also introduces data breach notification requirements and large administrative fines, up to 4 per cent of companies' annual global turnover.

To whom does it apply? The GDPR applies to entities that control or process personal data on EU residents. Personal data is defined in the law quite broadly. In general, it is data that identifies or can be used to contact a person (e.g., name, email address, date of birth, user ID); identifies a unique device (potentially) used by a single person (e.g., an IP address or unique device ID); or reflects or represents a person's behaviour or activity (e.g., location, applications downloaded, websites visited, etc.).[1]

The GDPR applies to entities that are established in the EU, as well as entities established outside the EU if they 1) offer goods or services to EU residents or 2) monitor the behaviour of EU residents that takes place within the EU. In practical terms, this means that any provider of services that process EU residents' personal data must be compliant.

Compliance date:
Entities must comply by 25 May 2018.

A fundamental shift for personal data protection in the EU: New data breach notification requirements and fines

The GDPR represents a fundamental shift for personal data protection in the EU. It is much stricter than its predecessor, with greater scope of coverage – including companies outside the EU – as well as new data breach notification requirements and administrative fines, as described below.

The GDPR introduces mandatory breach notification requirements for personal data. Supervisory authorities must be informed, in most instances, if personal data is lost, stolen or otherwise compromised without undue delay and, where feasible, not later than 72 hours after having become aware of it. In certain cases, individuals must be notified as well. Notifications must describe a range of details about the breach, such as its nature, categories and number of personal data records concerned, likely consequences, and measures taken to address the breach and mitigate its effects.

Finally, the GDPR introduces administrative fines. The consequences of noncompliance (whether egregious or accidental) are severe: a potential maximum fine of 4 per cent of annual global revenue (or maximum €20,000,000, whichever is higher) for noncompliance with many of its collection, processing and administrative obligations (such as the requirement to get consent, or various rules regarding data transfers to third countries), and 2 per cent (or maximum €10,000,000, whichever is higher) for security and data breach notification-related obligations, amongst others.

The General Data Protection Regulation is a complex data protection law that includes numerous obligations regarding data management and data protection. Palo Alto Networks Next-Generation Security Platform can contribute to an organisation's overall efforts to comply with GDPR, namely those efforts related to data security and protection. Palo Alto Networks will not address all aspects of GDPR compliance, but our security platform should be considered an essential component of GDPR compliance.

The GDPR's mandatory data breach notification mandate, with potential resulting reputational harm, regulators' investigations and significant administrative fines, has firmly placed personal data protection as a board-level concern.

Significant impact on organisations, including the CISO and security teams

The GDPR is likely to require substantial technology and personnel investments and business process changes for companies to come into compliance. The GDPR will impact different groups within an organisation, including the legal department and chief information security officer, as well as business teams and product engineers that must implement 'privacy-by-design.'

[1] GDPR Article 4 (1): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

It is important to note that the GDPR provides principles for the protection of data, such as transparency, accountability, lawfulness, right to be forgotten, privacy by design, etc., but it does not prescribe the exact technologies organisations must use to protect the data. This sets a high bar for protection and requires the CISO and security teams to determine and apply the right approach to protect the information covered within the scope of the GDPR.

HOW THE PALO ALTO NETWORKS PLATFORM CONTRIBUTES TO GDPR COMPLIANCE

Cybersecurity is an essential investment to protect personal data and comply with the GDPR.

The vast majority of GDPR requirements center around data management, namely data collecting and processing. There are obligations to provide notice when collecting personal data, prohibitions on unauthorized data processing, requirements to keep records of data processing, a duty to appoint a data protection officer in certain instances, and rules regarding transfer of personal data to third parties and third countries, amongst others.

But this should not overshadow the fact that data security is also a pillar of GDPR. GDPR has specific security-related language, as described in detail below. Further, a key component of protecting personal data is keeping it secure – both from exfiltration by cyber adversaries and from internal leakage. Thus, as they prepare for the GDPR, it is imperative that organisations' investments in compliance activities and information management processes and technologies be complemented with appropriate investments in cybersecurity.

Summary of relevant provisions from the GDPR (see this link to the GDPR for full text)

Topic	Summary of provisions
Security of data processing	Organisations must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Those measures must account for the state of the art. **[Article 32]** Personal data should be processed in a manner that ensures appropriate security and confidentiality of the data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing. **[Recital, paragraph 39]** In assessing data security risk, consideration should be given to risks presented by personal data processing. Risks that should be considered include accidental or unlawful destruction, loss, alteration, and unauthorised disclosure of, or access to, personal data. **[Recital, paragraph 83]**
Data breach notification	Supervisory authorities must be notified if personal data is lost, stolen or otherwise compromised, unless the breach is unlikely to result in a relevant risk to the individual. Notification must happen without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. In certain cases, individuals must be notified. Notifications must describe a range of information about the breach, such as its nature, categories and number of personal data records concerned, likely consequences, measures taken to address the breach and mitigate its effects, and other items. **[Articles 33 and 34]**
Administrative fines	Supervisory authorities are to impose administrative fines for GDPR infringements, on a case-by-case basis. When deciding whether to impose a fine and the amount, the authorities are directed to consider many factors, including the degree of responsibility in implementing technical and organisational measures, taking into account the state of the art as per Article 32. **[Article 83]**

Palo Alto Networks® can help with organisations' security and data protection efforts related to GDPR compliance by assisting in:

1. Securing personal data. The GDPR requires security of data processing, accounting for the state of the art. Our Next-Generation Security Platform provides just that: security at the application, network and endpoint level, as well as in the cloud.
2. Data breach prevention. Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR. Proper cybersecurity is essential to ensure your organisation's personal and business-critical data and applications remain protected. Our Next-Generation Security Platform is built for prevention.
3. Data breach notification. In the unfortunate instance of a data breach, it must be reported. Our Next-Generation Security Platform can help determine what personal data was compromised, and contribute key facts about measures taken to address the breach.

Many parts of our product portfolio have capabilities and features that meet these needs. These are described herein.

Securing Personal Data

The GDPR requires security of data processing, accounting for the state of the art. Palo Alto Networks platform secures data at the application, network and endpoint level, as well as in the cloud.

Truly reducing cyber risk and protecting data, including personal data, requires integrated, automated and effective controls in place to detect and prevent known and unknown threats at every stage of the attack lifecycle. Built from the ground up for prevention, the Palo Alto Networks Next-Generation Security Platform allows organisations to confidently pursue a digital-first strategy as they implement key technology initiatives within the cloud and, increasingly, mobile networks to protect their most valued data assets from exfiltration by cybercriminals and accidental data leakage.

The Palo Alto Networks Next-Generation Security Platform combines network and endpoint security with threat intelligence to provide automated protection and prevent cyberattacks – not just detect them. Our platform natively brings together all key security functions – including firewall, URL filtering, IDS/IPS, and advanced endpoint and threat protection. Because these functions are purposefully built into the platform with cyberthreat prevention in mind, and natively share essential information across the respective disciplines, our platform ensures better security than legacy firewalls and antivirus, UTMs, or point threat detection products. In short, better security supports better data protection.

State-of-the-Art Technology

The GDPR calls for technical and organisational security measures that account for the state of the art. Legacy security systems, made up of cobbled-together point products, have proven inadequate to prevent the rising volume, automation and sophistication of cyberattacks. CISOs should review these legacy products carefully to determine if they meet the state of the art.

The threat landscape is constantly evolving, and as such, state of the art technology must evolve to prevent new threats. The Palo Alto Networks Next-Generation Security Platform combines network and endpoint security with threat intelligence to provide automated protection and prevent cyberattacks, not just detect them. Contrary to legacy point products, our platform leverages the network effects of thousands of customers, technology partners and researchers sharing threat information. We build technology that prevents attacks at the key tactical and strategic places where cyberattackers need to take action to be successful, and we update our global customer base with the latest protections in as few as five minutes. As a matter of scope, we generate more than one million new preventive measures each week as we identify new, or 'zero-day', cyberthreats. With our platform, organisations can safely enable the use of all applications critical to running their business, confidently pursue new technology initiatives, and protect the organisation from both basic and complicated, multifaceted cyberattacks. For CISOs who want to say they have accounted for the state of the art, Palo Alto Networks should be among the security elements considered.

Complete Visibility
Reduce Attack Surface
Prevent Known Threats
Prevent Unknown Threats

Data Breach Prevention

Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR. Proper cybersecurity is essential to ensure your organisation's personal and business-critical data and applications remain protected.

Our platform enables four key prevention techniques relevant to data security, simultaneously contributing to GDPR compliance.

- **Complete visibility.** Our platform offers visibility into all traffic – across the network, endpoint and the cloud – classified by application, user and content. You can't stop or protect against what you can't see. Complete visibility provides the context to enforce dynamic security policy.
- **Reduce the attack surface.** The attack surface is expanding rapidly as companies' use of applications and devices (e.g., SaaS, cloud and IoT) proliferates. The more avenues available to infiltrate an organisation, the more opportunities for a cyber adversary to exfiltrate personal data. We enforce a positive security model, reducing the attack surface by enabling only the allowed applications for the right users and denying everything else.
- **Prevent known threats.** Many data breaches result from known threats, such as commodity information-stealing Trojans, malware and application exploits. On the perimeter, our platform controls the threat vectors themselves through the granular management of all types of applications. This immediately reduces the attack surface of the network, after which all allowed traffic is analysed for exploits, malware, malicious URLs, and dangerous or restricted files or content. On the endpoint, Palo Alto Networks combines threat intelligence from our global community of customers with our unique multi-method prevention approach to block known malware and exploits before they can compromise endpoints.
- **Prevent unknown threats.** Our platform goes beyond stopping known threats to proactively identify and block unknown malware and exploits, which are often used in sophisticated and targeted attacks. When a novel malware or exploit is seen, the WildFire™ cloud-based threat analysis service automatically creates and shares a new control to your prevention devices, like next-generation firewalls and Traps™ advanced endpoint protection, in as few as five minutes, without human intervention. In addition, Traps deploys a unique, multi-method approach to block the core techniques used by zero-day exploits and identify and block unknown malware from compromising endpoints.

> *To further alleviate data transfer and privacy concerns, WildFire EU, a localised cloud deployment, is available to analyse data without ever transferring it from regional boundaries.*

These prevention techniques are powered by WildFire, the industry's most advanced analysis and prevention engine for highly evasive zero-day malware and exploits. The cloud-based service employs a multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats. WildFire goes beyond legacy approaches used to detect unknown threats, bringing together the benefits of four independent techniques for high-fidelity and evasion-resistant discovery:

- **Dynamic analysis:** Observes files as they detonate in a custom-built, evasion-resistant virtual environment, enabling detection of zero-day malware and exploits using hundreds of behavioural characteristics.
- **Static analysis:** Effectively detects malware and exploits that attempt to evade dynamic analysis, as well as instantly identifying variants of existing malware.
- **Machine learning:** Extracts thousands of unique features from each file, training a predictive machine learning classifier to identify new malware and exploits in a way not possible with static or dynamic analysis alone.

- **Bare metal analysis:** Automatically sends evasive threats to a real hardware environment for detonation, entirely removing an adversary's ability to deploy anti-VM analysis techniques.

Together, these techniques allow WildFire to discover and prevent unknown malware and exploits with high efficacy and near-zero false positives.

Managing Security Processes Centrally

The GDPR applies to any organisation that processes personal data on EU residents, regardless of where the organisation is physically located. For many large or multinational organisations, personal data processing might take place in multiple locations, all of which must be compliant. Panorama™ network security management empowers organisations with easy-to-implement, consolidated policy creation and management of our next-generation firewalls. With Panorama, you can implement both centralised and regional policy, and easily delegate to regional admins as needed or preferred. The key is the flexibility to implement policies according to business needs and specific regional laws. For example, a Panorama admin can enforce security policies for firewalls located in a branch in Singapore or Brazil, even though the regional admins in those locations may be unaware of a compliance need to protect data subject to the GDPR.

Preventing Data Exfiltration or Leakage

Data breaches can result from data exfiltration or leakage, and our platform can contribute to preventing both.

With our Next-Generation Security Platform, each critical stage within the attack lifecycle is met with a defence model to prevent data exfiltration – from the attacker's initial attempt to breach the perimeter, to delivering malware or exploiting the endpoint, to moving laterally through the network until the attacker reaches the primary target and attempts to exfiltrate personal and sensitive data.

Organisations operating within Europe can select the regional EU-based Aperture data center to meet their data location preference.

To maintain compliance with GDPR, it's critically important to prevent accidental data leakage/sharing by your internal and partner communities of users across the entire infrastructure. End users are amongst the most common risks, particularly when using SaaS applications. Often untrained and unaware of the risks they bring, their actions can result in accidental personal data leakage.

Our security platform prevents data exfiltration and leakage in several ways:

- **Security at the network.** To protect data within your organisation, built-in data filtering profiles on the next-generation firewall help prevent accidental data leakage – at the network layer. System administrators can apply policies to inspect and control content traversing the network to help limit unauthorised transfer of sensitive data, such as credit card numbers.
- **Security at the SaaS level.** Organisations need to control access to SaaS applications, enforce policy controls on information sharing and stop data leakage.
    - These capabilities are delivered through our platform using the next-generation firewall (e.g. User-ID™, App-ID™ and Content-ID™ technologies) and Aperture™ SaaS security service. The next-generation firewall analyses all traffic from your network to SaaS applications and back. However, certain cloud-based activity can be invisible to in-line security services, such as data sharing permissions or accessing cloud-based data from outside the network (without VPN). In this case, Aperture complements the next-generation firewall, using SaaS APIs to connect directly to the SaaS applications themselves. This makes it possible to see everything users have uploaded or shared. With Aperture, users can view and monitor file uploads across all assets in enterprise SaaS applications, such as Box, Microsoft® Office, Dropbox®, Salesforce®, Secure Data Space and more. Policies can then be applied to monitor and enforce responsible use of assets (including personal data) and protect against accidental data leaks caused by human errors, such as promiscuous or inadvertent sharing, and sharing content using links that may be exposed to the internet. If a policy violation is detected, an alert is generated. If configured, Aperture takes automatic action to remediate the risk.
- **Security at the endpoint.** Traps advanced endpoint protection employs a multi-method approach to preemptively block known and unknown threats, including zero-day exploits and unknown malware, from compromising endpoints.

- **Stopping credential theft.** Stolen credentials are a common threat vector for data breaches, given it is relatively simple to steal a password and gain the level of access desired.
    - Our platform provides the capabilities to break up credential-based attacks across the attack lifecycle. Often, attackers will use credential phishing attempts, sent via email or social media, to trick users into submitting corporate credentials in a fraudulent form. Our platform stops credential leakage by preventing users from submitting credentials to unknown and unauthorised sites. Because stolen credentials are typically used to access critical systems inside the organisation, we also establish protections against lateral movement by enforcing multi-factor authentication (MFA) policies that govern access to these critical applications where sensitive data is contained.

In addition, AutoFocus™, our contextual threat intelligence service, can ingest third-party threat intelligence sources and turn them into prevention across our security platform through our MineMeld™ application. Once indicators of compromise are collected, MineMeld can filter, de-duplicate and consolidate metadata across all sources, allowing security teams to analyse a more actionable set of data, enriched from multiple sources, for easier enforcement.

Data Breach Notification

In the unfortunate instance of a data breach, it must be reported.

In the unfortunate event of a personal data breach, the GDPR requires notification to supervisory authorities, unless the event is unlikely to result in risk to individuals' rights or freedom. Notification must include a range of information, including what data was impacted and what measures were taken.

Our platform can help maintain compliance with this GDPR requirement in the event of a breach. For example, AutoFocus provides the analytics details needed for remediation, helping to understand who the user was, what the threat was, the impact and the level of risk. All of this can help with notification requirements.

In addition, the next-generation firewall can be used to educate users via custom notification pages. System administrators can add their desired education message to the notification pages so that whenever an accidental data leak is prevented, the end user is served that message. For example, the message can include a link to the corporate data policies and best practices. This helps with overall prevention, as well as education efforts that support notification.

Additional Materials

The following resources are available in case you would like to learn more about how the Palo Alto Networks Next-Generation Security Platform can help you maintain compliance with the GDPR:

- Questions about how Palo Alto Networks products approach data privacy? Product-specific data privacy sheets are available here: https://www.paloaltonetworks.com/resources/datasheets.html
- Appendix (on page 8) – an overview of the different components of the Next-Generation Security Platform, including specific data security and protection features and capabilities.

> *Processing personal data to ensure network and information security – for instance, through the Palo Alto Networks Next-Generation Security Platform, and WildFire service specifically – is broadly recognised as a legitimate interest and specifically called out as such in the GDPR.* ***[Recital, paragraph 49]***

APPENDIX – PALO ALTO NETWORKS PRODUCTS AND FEATURES

- **Next-generation firewall**
  - Provides visibility into and control over all applications within the network perimeter and enforces granular security policies – across physical networks and public and private clouds.
  - Inspects files and URLs for known and unknown threats.
  - Policy-based multi-factor authentication (MFA) prevents access to sensitive resources leveraging potentially phished/stolen credentials.
  - Insight gained from App-ID, User-ID and Content-ID can help educate your organisation, especially executives, about who is using what on the network, and its effect on the organisation's risk profile. This insight also helps you set the right policies to enhance security and prevent breaches.
  - Protects against the credential theft and abuse.

- **GlobalProtect network security for endpoints**
  - Extends the safe enablement and protection of next-generation network security to the mobile workforce.
  - Maintains the visibility of traffic and the enforcement of security policy for protection against known and unknown threats.
  - Contextually controls access and enforces security policies based on application, user and device state.
  - Inspects business traffic and protect business data whilst respecting the user's privacy.

- **Panorama network security management**
  - Facilitates intuitive and powerful policy control with a single security rule base.
  - Supports enterprise-class management capabilities, hierarchical device groups, template stacks and more.
  - Provides actionable insight into traffic and threats with the powerful Application Command Center.
  - Enables scalable and flexible deployment options.
  - Maintains aggregated logging and event correlation across next-generation firewall and Traps advanced endpoint protection.

- **Aperture SaaS security service**
  - Provides complete visibility across all user, folder and file activity, providing detailed analysis that helps you transition from a position of speculation to one of certainty about what's happening at any given point in time.
  - Conducts retroactive analysis of data exposure not just of data in-line, but also from the creation of the SaaS account itself, no matter how long ago that was.
  - Runs deep analytics into day-to-day usage that allow you to quickly determine if there are any data risks or compliance-related policy violations.
  - Enables granular, context-aware policy control that allows you to drive enforcement and quarantine users and data as soon as a violation occurs.
  - Blocks known malware, and identifies and blocks unknown malware, with advanced threat protection.

- **Traps advanced endpoint protection**
  - Replaces traditional antivirus with multi-method prevention – a unique combination of malware and exploit prevention capabilities that preemptively blocks known and unknown threats from compromising endpoints.
  - Automates breach prevention by autonomously reprogramming itself to block malware identified by other components of the Palo Alto Networks next-generation security platform, no matter where they are deployed.
  - Delivers breach prevention, in contrast to breach detection and incident response after critical assets have already been compromised.
  - Enables security event identification, correlation and response through integration with Panorama.

Threat Intelligence Cloud

- **Threat Prevention** *(includes intrusion prevention, network anti-malware, and command-and-control (C2) protection)*
    - Keeps up to date on new threats and blocks known malware, exploits and C2 activity.
    - Detects and blocks threats on any and all ports, instead of invoking signatures based on a limited set of predefined ports.
    - Provides advanced C2 prevention by introducing end-to-end automation of the generation, delivery and enforcement of payload-based C2 protections, based on data from WildFire customers.
    - Helps you to never lose sight of a threat, regardless of the evasion technique. User-ID and App-ID technology within our next-generation firewall identify and contextualise all traffic on all ports.

- **URL Filtering with PAN-DB**
    - Enables safe web access, protecting users from dangerous websites, malware sites, credential-phishing pages and attacks attempting to leverage web browsing to deliver threats – with updated protections in near real time.
    - A native component of the Next-Generation Security Platform, providing best-in-class security without adding operational burden.

- **WildFire cloud-based threat analysis service**
    - Identifies and automatically prevents unknown threats in as few as five minutes, without the need for manual response.
    - Detects evasive zero-day exploits and malware with a unique combination of dynamic and static analysis, novel machine learning techniques, and an industry-first, bare metal analysis environment.
    - Builds collective immunity for unknown malware and exploits with shared real-time intelligence from more than 15,500 subscribers.

- **AutoFocus contextual threat intelligence service**
    - Extends WildFire with rich threat analytics and correlation capabilities.
    - Moves away from legacy approaches that rely on aggregating detection-focused alerts and post-event mitigation with local, industry and global threat intelligence with attack context to accelerate analysis, forensics and prevention workflows.
    - Automatically prevents attacks with proactive threat analytics and hunting enabled.
    - Integration with MineMeld enables security teams to aggregate, correlate and automatically turn any third-party threat intelligence source into prevention across the entire platform.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com