PALO ALTO NETWORKS TRAPS: A KEY TOOL FOR THE ROAD TO GDPR COMPLIANCE

The General Data Protection Regulation is a new data protection regulation from the European Union that aims to improve controls for protecting the personal information of individuals in the EU. It is stricter and simultaneously broader in scope than the 1995 Data Protection Directive, which it replaces. The GDPR went into effect in May 2016, giving organizations time to achieve compliance by the deadline of May 25, 2018.

Although the GDPR is an EU law, it applies to entities around the world: any organization that controls or processes personal data on individuals in the EU, as well as companies that provide goods or services to individuals in the EU or monitor their behavior, must comply. A recent study showed that 92 percent of U.S. companies consider the GDPR a top data protection priority.[1]

This complex law covers both data management – that is, collection and processing – and data protection. Keeping personal data secure is a key element of data protection, and the GDPR includes specific security-related language in certain articles and recitals. Because endpoints play a key role in organizational security, this paper focuses on how Palo Alto Networks® Traps™ advanced endpoint protection can enable security, risk and compliance teams to protect data in their efforts towards GDPR compliance.

Five Key Security Provisions Related to Endpoint Protection

Several sections of the GDPR speak to security. The most important sections relating to endpoint security are the following:

a. Recital 39: "Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of the personal data …"

b. Article 5(f): "Personal data shall be … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

c. Recital 78: "The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organizational measures be taken … The controller or processor should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default."

d. Recital 83: "In order to maintain security … the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks … Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation …"[2]

e. Article 32: "Taking into account the state of the art … [organizations] shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

Important GDPR Definitions

Personal data: Any information relating to an identified or identifiable natural person, or "data subject." This includes:

- Data that identifies a person or can be used to contact a person.
- Data that identifies a unique device potentially used by a single person, e.g., an IP address or unique device ID.
- Data that reflects or represents a person's behavior or activity, e.g., location, apps downloaded, websites visited.

Processing: Any operation or set of operations performed on personal data, whether automated or manual. This includes:

- Collection, recording, organization, structuring, storage, adaptation or alteration.
- Retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available.
- Alignment, combination, restriction, erasure or destruction.

How Traps Helps Security Teams in Their Journey to GDPR Compliance

Traps can assist in the journey to GDPR compliance in five ways that address the aforementioned provisions: preventing unauthorized access; preventing unauthorized or unlawful processing and accidental loss, destruction or damage; applying data protection by design and by default; facilitating risk mitigation; and accounting for state-of-the-art technology.

Preventing Unauthorized Access

Traps ensures unauthorized processes, such as those initiated through malware or exploits, cannot be launched and gain unintended access. This includes protection from executable files, DLLs and malicious macros, as well as prevention of script-based attacks. The security of the Traps agent itself is assured by requiring, by default, users and administrators to enter a password to uninstall it.

Preventing Unauthorized or Unlawful Processing and Accidental Loss, Destruction or Damage

Traps secures personal data at the endpoint by preventing malware and exploit attacks. It uses multiple methods of prevention to pre-emptively block known and unknown threats, including zero-day exploits and unknown malware. The Traps approach is based on four key principles:

1. Traps provides complete visibility into endpoint application activity along with context to enforce dynamic security policy. This includes providing event information about malicious application activity on endpoints and servers, enabling rapid response to alerts and incidents.
2. Traps reduces the attack surface. Restriction rules limit the attack surface area on endpoints, proactively maximizing coverage from attacks by defining where and how your users can run executable files.
3. Traps prevents known threats with multiple methods of prevention, combining threat intelligence from a global community of customers, partners and third-party feeds to block known malware and exploits before they can compromise endpoints.
4. Traps prevents unknown threats. Using exploit prevention techniques, it targets software vulnerabilities in processes that open non-executable files, blocking the core techniques used by zero-day exploits. It employs malware prevention techniques to prevent malicious executable files from compromising endpoints. Traps uses local analysis via machine learning to determine whether an unknown file is likely to be malicious or benign, without reliance on signatures, scanning or behavioral analysis. In addition to local analysis, Traps sends unknown files to WildFire® cloud-based threat analysis service to rapidly detect unknown malware and automatically reprogram itself with relevant protections.

Applying Data Protection by Design and by Default

Default settings have been designed into Traps to protect users against privacy risks, with granular control over service protection settings and security of the agent itself. This default protection prevents attempts to disable or make changes to Traps processes, services, registry keys and values, and files. Especially relevant to GDPR, customers can determine by policy which types of files to transmit to WildFire for analysis and can choose between the U.S.- and EU-based WildFire clouds if they want to further limit the geographic location to which unknown files are transmitted for analysis.

Facilitating Risk Mitigation

Traps is a certified[3] replacement for traditional antivirus software. Since AV does not sufficiently mitigate security risks, many AV users have to deploy additional technologies and products to mitigate what their AV cannot address, imposing additional costs on their organizations. Traps enables threat protection technology on infrastructure and connected systems to protect against known and unknown malware and exploits, and is continuously updated to prevent the download and execution of malicious files.

Accounting for State-of-the-Art Technology

GDPR requires technical and organizational security measures that account for the state of the art. An evolving threat landscape calls for constantly evolving technology, yet many products are cobbled together and rapidly become outdated. Traps, in contrast, combines endpoint security with threat intelligence to provide automated protection and prevent cyber-attacks. The innovative technology is constantly evolving to stay ahead of rapidly changing threats. Traps is integrated with WildFire to automatically create and share new controls with all users, worldwide, in as few as five minutes, without human intervention. More than 1.5 million new preventive measures are generated each week as zero-day threats are identified.

Mapping Traps Capabilities to GDPR Recitals and Articles

Traps can support the road to GDPR compliance through its endpoint security capabilities. This table maps these Traps capabilities to specific controls that address GDPR recitals and articles.

GDPR REQUIREMENT: **Recital 39 – Unauthorized access** ***Ensure appropriate security and confidentiality of personal data, including preventing unauthorized access.***	
Control	
Prevent access by unauthorized users	Traps ensures only authorized users can access applications and data on the endpoint. Traps may not be uninstalled without entering authorized credentials.
Prevent access by unauthorized or unwanted processes	Traps prevents unauthorized processes against launching and gaining unwanted access. This includes protection from malicious macros and prevention of script-based attacks.
GDPR REQUIREMENT: **Article 5(f) – Unauthorized processing** ***Ensure protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage.***	
Control	
Protect against known threats	Traps prevents known threats via a multi-method approach combined with threat intelligence from a global community of customers.
Protect against unknown (zero-day) threats	Traps prevents unknown threats by blocking the core techniques used by zero-day threats. It provides protection against both malware and exploits.
Provide continuous endpoint visibility and monitoring	Traps provides full visibility into all endpoint activity and a recorded history of all endpoint and server activity.

GDPR REQUIREMENT: **Recital 78 – Data protection by design and by default** ***Adopt internal policies and implement measures that protect data by design and by default.***	
Control	
Ensure privacy and data protection by design	Privacy features have been built into Traps throughout the design process. For example, customers can determine which types of files to transmit to WildFire for analysis as well as choose between the U.S.- and EU-based WildFire clouds if they want to further limit the geographic location to which unknown files are transmitted for analysis.
Ensure privacy and data protection by default	Default Traps settings protect users against privacy risks, with granular control over service protection settings and the security of the agent itself. This default protection prevents attempts to disable or make changes to Traps processes, services, registry keys and values, and files.
GDPR REQUIREMENT: **Recital 83 – Mitigate risks** ***Evaluate the risks inherent in the processing and implement measures to mitigate those risks.***	
Control	
Implement threat protection technology to protect from known and unknown threats	Traps protects against known and unknown malware and exploits. Unlike AV products, Traps does not require a host of additional security products to mitigate risks.
Continuously update threat protection	Traps provides continuous updating to prevent against the download and execution of malicious files.
GDPR REQUIREMENT: **Article 32 – Security of processing** ***Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (state of the art).***	
Control	
Employ state-of-the-art technology	Traps continuously evolves to stay ahead of threats. The entire Palo Alto Networks portfolio is based on state-of-the-art technology and is constantly enhanced to provide comprehensive protection.
Provide automated protection	Traps is integrated with WildFire to automatically create and share new protection against zero-day threats with all users in as few as five minutes, globally, without human intervention.

How Traps Provides Assurance to Risk and Compliance Officers

Risk and compliance teams need to feel confident that the measures taken in their organizations will support compliance with GDPR requirements. Traps helps them avoid the onerous notification requirements that would stem from a personal data breach, not to mention the hefty administrative fines that could be levied.

Security Commensurate With Risk

Organizations that use legacy systems and a hodgepodge of point products have no way of assuring this. Products may interoperate poorly, provide inadequate protection or focus solely on detection rather than protection, leaving openings for unauthorized users to access, destroy or disclose personal data. Traps prevents breaches from happening in the first place, thus avoiding accidental or deliberate loss, destruction, or damage of personal information. This gives risk and compliance officers confidence that they are taking steps aligned with the risk.

Prevention of Unauthorized Access

If an organization uses an endpoint security product that protects against unauthorized individual access but does not stop rogue processes from accessing personal data, this could leave the organization open to personal data breaches that could trigger the GDPR's breach notification requirements – and, potentially, hefty fines. Traps ensures no unauthorized users or processes, such as those initiated through malware or exploits, can access applications and data on the endpoint. This helps risk and compliance teams feel confident they are preventing both types of unauthorized access.

State-of-the-Art Technology

Many legacy systems and point products become stagnant over the years and cannot hope to keep up with constantly evolving malware and attacks. Traps is a constantly evolving, machine learning-based offering that stays ahead of data security threats and potential breaches, epitomizing the state-of-the-art technology risk and compliance officers need to take into account to address GDPR requirements.

Data Protection by Design and by Default

Data security products purchased and implemented piecemeal can introduce serious gaps in security design, and weak default settings can open the door to hackers and eventual breaches. This leaves the organization with the possibility of violations and out-of-compliance status. Traps employs multiple methods of prevention in data protection, with strong default settings and administrator control, ensuring risk and compliance teams can feel confident their endpoint protection measures align with GDPR requirements.

Appropriate Levels of Security

Endpoints represent significant risk as vulnerable points in overall organizational security. When an organization relies on loosely coupled point products or simple antivirus, the gaps can be so great as to render security measures ineffective. Simply using static analysis to find known threats is insufficient in a world where cyberattacks evolve daily. Traps employs a combination of static and dynamic analysis, machine learning techniques, and more to help risk and compliance officers adopt GDPR-appropriate levels of security for endpoints.

Conclusion

The GDPR requires organizations to take adequate steps to ensure the highest level of protection for the personal data of individuals in the EU. Data visibility, data security and risk reduction are key elements of GDPR compliance. Although no security vendor can make an organization GDPR-compliant via a single tool or service, Traps can help organizations take confident steps on the road to GDPR compliance. Traps helps security teams ensure strong protection for endpoints, as required by risk and compliance officers. With Traps, organizations can pre-emptively block known and unknown threats from compromising their endpoints.

1. GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey. Jan. 2017. Retrieved from https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html

2. Regulation (EU) 2016 … of the European Parliament and of the Council. April 2016. Retrieved from http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

3. AV-TEST Full Product Test of Palo Alto Networks Traps. July 2017. Retrieved from https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Palo_Alto_Traps_Full_Product_Test_July_2017.pdf

   Traps Advanced Endpoint Protection PCI Validation. Coalfire, Oct. 2016. Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/traps-advanced-endpoint-protection-pci-validation

   Traps Advanced Endpoint Protection HIPAA Validation. Coalfire, Oct. 2016. Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/traps-advanced-endpoint-protection-hipaa-validation/

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com

traps-a-key-tool-for-the-road-to-gdpr-compliance-wp-051018