proofpoint.

SOLUTION BRIEF

Proofpoint Threat Response and GDPR

Achieve Compliance with Security Automation and Data Privacy Best Practices

KEY BENEFITS

Embrace Security Best Practices

- Resolve targeted threats faster and more efficiently
- Unburden your IT team with automated incident response
- Reduce alert fatigue
- Collect and prioritize data from disparate security devices
- Get a context-rich view of all threats

Comply with GDPR

- Prevent sharing of personal data with external third parties
- Integrate with internal control systems
- Add to internal data processing records
- Provide proof of compliance backed by Proofpoint

Most successful organizations today are using automation technology to handle security incidents. What's behind this trend? And what should you consider when adopting security automation to help you comply with regulations, follow best practices, and achieve long-term business benefits?

THE DRIVE FOR INCIDENT AUTOMATION

Today's cybersecurity landscape requires rapid response. But security teams face many challenges that prevent them from responding to targeted threats quickly and efficiently. These include:

- **Staff shortages:** Incident response can be a slow process that requires a lot of work. Certain tasks take a great deal of time and create bottlenecks. And repeating the same tasks for every incident can overwhelm your already stretched security team.
- **Alert fatigue:** The more security devices you rely on, the greater the number of alerts. Your security team is then left to triage alerts manually. What's the problem with this? It is subject to human error. And real incidents are often neglected.
- **Disparate security devices and data:** Incident response investigation requires information from multiple, disconnected sources. Each data point is one piece of the puzzle. Like many organizations, you're increasingly facing targeted threats, where responding within minutes is essential. Too much disconnected information can slow down your incident response.

Security orchestration, automation and response (SOAR) solutions can help solve these problems. They ingest alerts from various sources and add workflows to automate incident response. By leveraging a SOAR solution, you save time. You also limit or reduce the number of full-time employees it takes to deal with the security incidents by automating the incident response process. This reduces mean time to respond, contain and remediate threats.

Proofpoint Threat Response is a SOAR solution that takes the manual labor and guesswork out of incident response. It helps your security team resolve threats faster and more efficiently. Threat Response collects alerts from various sources and automatically enriches and groups alerts with vital context from Proofpoint Threat Intelligence—in seconds. It provides the "who, what and where" of attacks, user IP mapping, and external threat intelligence, such as industry-standard STIX and TAXII feeds. Your analysts can quickly triage security incidents. Based on the context and forensics collected and analyzed, Threat Response presents a context-rich view of that threat. Your analysts can take automated response actions, such as:

- Retract delivered email from users' mailboxes
- Add users to low-permission groups
- Update block lists of firewalls and web filters
- Contain the threat by blocking/quarantining threats across Microsoft Exchange, firewalls, endpoint detection and response (EDR), web gateway, Microsoft Active Directory, network access control (NAC) and other solutions

DATA PRIVACY AND SECURITY OPERATIONS

GDPR and the "Lawfulness of Processing"

According to the European Union General Data Protection Regulation (GDPR), processing personal data is a legitimate function for relevant data controllers. This is true where personal data is necessary for ensuring network and information security. It's also legitimate to process personal data when preventing unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data. These "legitimate interests" are defined in GDPR Article 6 "Lawfulness of processing." Legitimate interest can be asserted legally. But that is only possible if you can justify processing. Processing needs to comply with the principles of proportionality and subsidiarity. These exceptions to the use of personal data for IT security are defined in GDPR Article 6(1)f and in GDPR recital 49.

When it comes to GDPR compliance, extending and securing your infrastructure with security services like Threat Response is a big advantage. This solution is an essential part of a modern IT architecture. Configuring Threat Response can include processing data in external security architectures, such as a threat intelligence provider or security services. Threat Response does not provide any data to external parties. It only uses this data for agreed purposes described in the written service agreement between you and Proofpoint. Threat Response is available on premises only—without any external data transfer by default.

Add Threat Response to Records of Processing Activities

According to GDPR, the proper settings and integration into other systems is important for compliance. You can add Threat Response to internal data processing records, as required by GDPR Article 30 "Records of processing activities."

Internal Exchange of PII Data

GDPR Article 47, "Binding corporate rules," allows internal international information sharing. These corporate rules should include all essential data privacy principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

To guarantee GDPR compliance, you need to perform implementation through an internal control system (ICS). This means establishing an ICS. A compliant ICS consists of elements of the internal control system and monitoring system. The control system provides ways to control your organization's activities. It ensures proper recording of business transactions and compliance with GDPR principles.

EXCHANGING DATA WITH THIRD PARTIES[1]

To achieve an adequate level of protection, GDPR allows organizations to engage external experts, tools or services to support internal security measures. There are stringent GDPR regulations to ensure that third-party providers (processors) support your data protection level. These are defined in Article 28 "Processor." The controller should only use processors that provide sufficient guarantees to implement technical and organizational measures in ways that meet the GDPR requirements. Processers must ensure protection of the rights of the data subject.

To meet this strict requirement, Proofpoint offers various documents for your records for all related products to help you achieve compliance. This includes the data processing agreements (DPAs) you need for your process directory.

Built with industry and compliance best practices in mind, Threat Response automates and speeds up incident response. It also helps ensure that your use of personal data in a security context complies fully with GDPR. As an added benefit, Proofpoint provides defensible documentation to help you demonstrate proof of compliance.

1 This applies when configuring external data exchange or external services (example: Proofpoint Targeted Attack Protection).

LEARN MORE

For more information, visit **proofpoint.com**.