ESG WHITE PAPER

Exploring Decryption in the Context of Privacy Regulations

How Centralized Decryption Can Help Meet Compliance Requirements

By John Grady, ESG Senior Analyst

January 2021

This ESG White Paper was commissioned by Symantec, a Division of Broadcom, and is distributed under license from ESG.

Contents

Executive Summary

The rapidly expanding digital economy has generated many benefits for consumers, but its emphasis on data has sparked an increasing focus on privacy and the rights of the consumer. As a result, regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), among others, have been introduced to ensure that individuals retain a level of control with regard to the collection and use of their personal information. Yet at the same time, some of the developments helping to facilitate user privacy have been co-opted or exploited by bad actors.

In fact, encryption, which has been broadly adopted to protect the information of internet users and ensure the security of their communications, has been increasingly utilized by attackers to conceal their activities. Additionally, the ability of organizations to decrypt and inspect encrypted traffic for malicious activity has become less clear due to privacy laws such as GDPR and CCPA. However, when applied in a measured and risk-balanced way, implemented following the proper procedures, and supported by specific policies and safeguards, decryption can occur under existing privacy regulations, helping to improve enterprise security and protect sensitive data. Further, the decryption and inspection of enterprise network traffic is not only justifiable, but in many regards necessary to maintain the visibility needed to comply with key aspects of current privacy regulations, including the obligations for implementing effective security and fulfilling breach notification requirements through the timely detection of incidents.

The decryption and inspection of enterprise network traffic is not only justifiable, but in many regards necessary to maintain the visibility needed to comply with key aspects of current privacy regulations.

Encrypted Network Traffic Complicates Both Cybersecurity and Compliance

As the underlying composition of web traffic has changed over the years from basic browsing to a more application-centric, user-specific experience, the need to protect the privacy of individuals has increased. This has led to a dramatic rise in the amount of encrypted web traffic. In fact, the percentage of encrypted webpages Windows users load in Chrome has risen from 39% in 2015 to 81% in 2020.[1] These figures are applicable to the enterprise as well, where web application traffic is even more prevalent and typically encrypted by default. While this shift toward security and anonymity is certainly a positive development for individual users, the prevalence of encrypted traffic has complicated cybersecurity for enterprise organizations. Specifically, security teams often face the choice between having reduced visibility into network traffic that may be masking malicious content entering the network or enterprise data being exfiltrated when not decrypting, or the complexity of managing siloed decryption across multiple tools.

Attackers Use Encrypted Traffic to Their Benefit

Attacks continue to grow in sophistication and frequency, pushing cybersecurity teams to their limits. Ransomware, file-less malware, remote access trojans, and other malicious code can be delivered through a variety of channels, creating numerous attack vectors security teams must defend against. Unfortunately, attackers are all too aware of the trend toward encrypted traffic and have increasingly used encryption to further obscure their actions, including:

- Malware delivery. Attackers can compromise legitimate websites to serve malware and other exploits; use common business applications that utilize encryption such as OneDrive or Box to deliver malicious code; and procure SSL certificates for spoofed or fake sites to send malware via encrypted connections as part of phishing or other attacks.

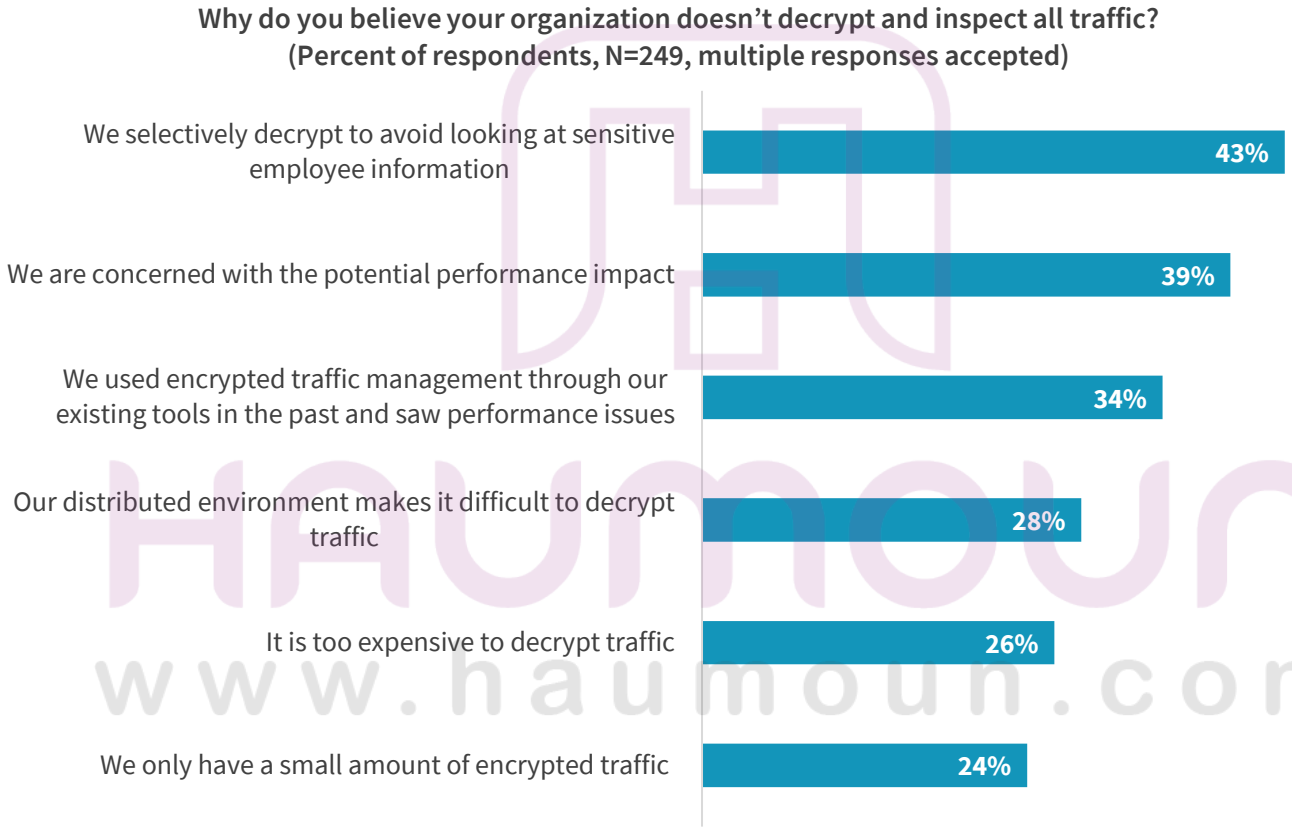
[1] Source: Google Transparency Report, *HTTPS Encryption by Chrome Platform*, September 2020.

- Command and control traffic. Once a machine is compromised, the command and control traffic attackers use to escalate privileges and move laterally within the network is typically encrypted to obscure the attacker's actions.
- Data exfiltration. Once the attacker has access to sensitive business data, it is exfiltrated via encrypted channels, preventing data loss prevention solutions from detecting the data leakage.

Legacy Decryption Approaches Have Not Solved the Problem

The ability to decrypt and inspect encrypted network traffic has existed for many years. Some security tools offer native decryption capabilities, and dedicated decryption solutions exist as well. Yet despite the need for visibility into encrypted traffic, and the presence of tools to facilitate this, many organizations continue to forgo decryption. ESG research has found that the main drivers of this gap in decryption are privacy and performance concerns (see Figure 1).[2]

Figure 1. Reasons Organizations Forgo Decryption



Source: Enterprise Strategy Group

Organizations do not want to decrypt all network traffic. Employees often access their personal financial accounts and healthcare information on the enterprise network, and there is no compelling reason the company should have visibility into those transactions. As these websites are typically among the most well protected, the risk of compromise is minimal and does not outweigh the privacy considerations of the user. Further, decrypting network traffic is computationally intensive, potentially impacting the user experience when performed on security tools such as next-generation firewalls (NGFW), secure web gateways (SWG), or other general-purpose tools. These considerations have historically led some

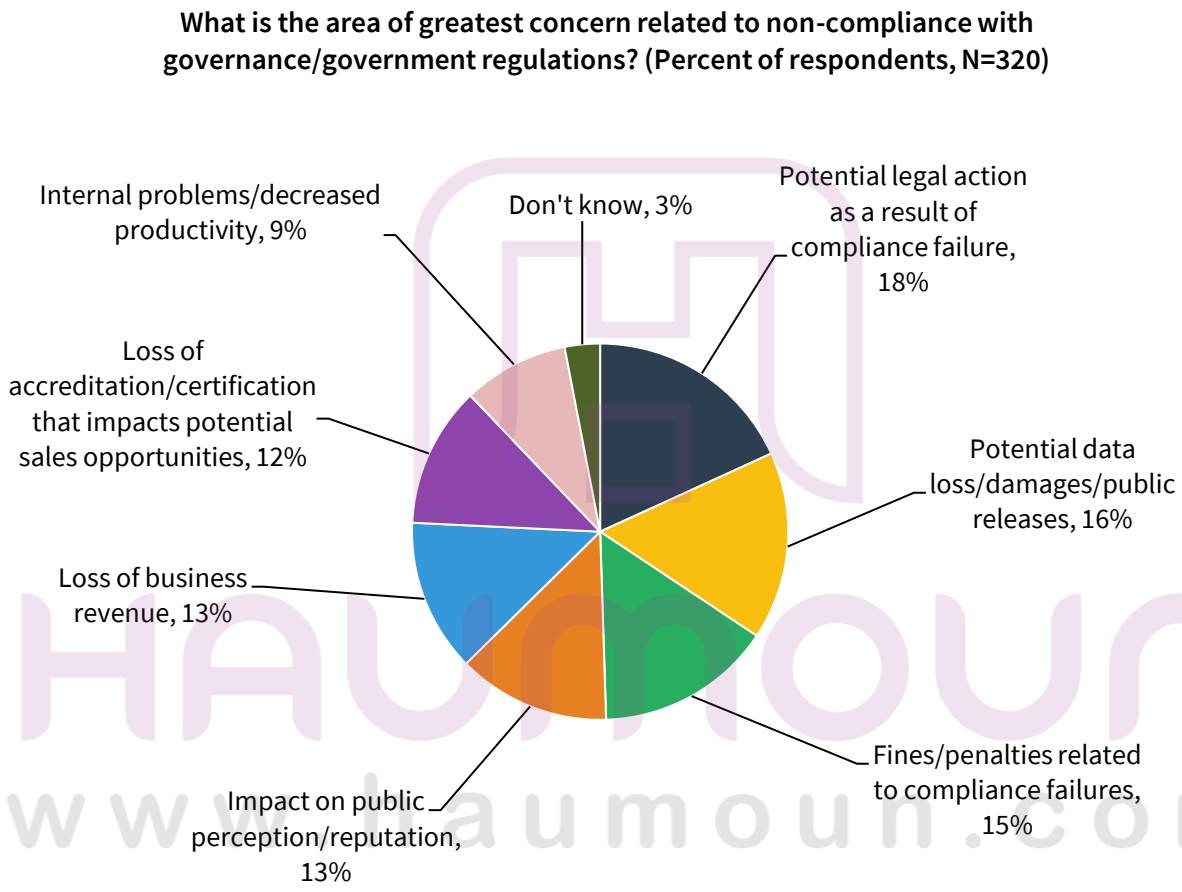
[2] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

organizations to broadly forgo decryption, which significantly hampers the security organization's ability to maintain visibility into network activity, protect the enterprise from modern attacks, and prevent data loss.

The Regulatory Environment Complicates the Issue

While general privacy considerations have always been top-of-mind regarding decryption, recent regulations have amplified the concern. In fact, 30% of organizations report new data security and privacy regulations as one of the biggest reasons IT has become more complex.[3] This should not come as a surprise, as the result of non-compliance can lead to a variety of undesirable consequences ranging from fines and legal action to lost revenue and reputation (see Figure 2).[4]

Figure 2. Impacts of Non-compliance with Regulations



Source: Enterprise Strategy Group

Specifically, the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronic Documents Act, and other existing and proposed privacy regulations have fundamentally changed how organizations must think about collecting and managing personal information. Because of the widening definition of personal information and the broad applicability of these regulations, it is not only customer data, but also employee data that fall under the coverage of these laws.

[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[4] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.

Decryption Is Often Justifiable, But Privacy Must Be Weighed and Balanced

As these new regulations have come into existence, organizations have struggled with how to ensure the privacy of employee information and meet compliance requirements while maintaining the visibility required to protect the enterprise from modern cybersecurity threats. Specifically, questions such as whether looking at encrypted traffic is allowed, under what conditions it may be permissible, whether it represents too great an invasion of privacy to the employee, and if it is ultimately worth the effort to implement have generated consternation for enterprises of all types.

A decision on whether and how to decrypt network traffic requires a detailed assessment to establish why it is justified, how it is risk-balanced, and what safeguards will be implemented to minimize intrusiveness and limit privacy risks for users.

The short answer is that decryption is often not only a defensible practice under GDPR and other privacy acts but can also serve as an enabler toward maintaining compliance with these regulations. However, reaching a decision on whether and how to decrypt network traffic requires a detailed assessment to establish why it is justified, how it is risk-balanced, and what safeguards will be implemented to minimize intrusiveness and limit privacy risks for users.

The following recommendations are meant as a guide to help organizations understand some of the key considerations when deciding whether to decrypt network traffic and developing the supporting policies and procedures to implement the practice. GDPR is used as the reference point because of its significance in modern privacy law and the fact that many subsequent regulations have borrowed heavily from it. It is critical to note that these recommendations should be considered in conjunction with the input and guidance of legal and compliance departments to ensure adherence to local and industry-specific regulations. Any organization considering decryption must fully account for the particularities of their company, employee agreements, industry, country, and the specific regulations to which they are subject.

Key Considerations for Implementing Decryption

The justification for organizations to decrypt and inspect network traffic with regard to GDPR is found within Articles 6, 32, and 33. Articles 32 and 33 lay out the obligation for securing the processing of personal data, including the "appropriate technical and organizational measures to ensure a level of security appropriate to the risk," as well as the notification requirements following a data breach of personal information. Article 6 provides the specific conditions under which data processing is lawful, with the following two being relevant to decryption:[5]

- "Processing is necessary for compliance with a legal obligation to which the controller is subject."
- "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

To establish justification, an organization must assess its risk in conjunction with the invasiveness of the protections it is seeking to put in place. For example, a bank or retail organization collects a significant amount of sensitive personal information and, as a result, is frequently targeted by malicious actors—in many cases using the types of encrypted attacks previously discussed. With this being the case, the organization may not be able to meet its obligations under Article 32 or

[5]Source: Art. 6, GDPR, Lawfulness of processing.

33 to protect its sensitive data and detect and disclose data breaches in a timely manner due to its limited visibility into encrypted traffic. These facts would then be used to establish justification under the legal obligation.

Additionally, Recital 49 specifically calls out the processing of personal data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" as a legitimate interest of data controllers, further validating decryption resulting in the processing of personal data as justified given the circumstances. However, the justification is only the beginning of the process and does not provide unchecked latitude for organizations to utilize invasive measures. Rather, intrusions to employee privacy must be minimized while managing the risk established in the initial justification. This requires a broad, cross-functional effort to ensure the proportionality of the approach, mitigate privacy risks that exist, and develop specific policies to support the initiative.

Involve the Right Teams from Across the Organization

As a starting point, it is critical to involve the correct stakeholders from across the organization. Typically, the cybersecurity team serves as the genesis of a decryption initiative; however, these projects ultimately require input across compliance, risk, legal, human resources, and data protection officers. These stakeholders should have input into the decision to decrypt, the development of the supporting policy, and the ongoing compliance of decryption initiatives relative to industry regulations.

Table 1. Roles and Responsibilities for Implementing Decryption

Group/Role	Key Responsibilities

Cybersecurity	▪ **Provide context from a security perspective** around the threat landscape the organization faces, the impact of encrypted traffic on visibility, and examples of encrypted threats that have impacted the business.
	▪ **Generate the initial recommendation of decryption policies** including but not limited to:
	  ▪ The groups and roles subject to this type of inspection.
	  ▪ Indicators triggering or forgoing the decryption on network traffic.
	  ▪ Roles and individuals with access to decrypted traffic data.
	  ▪ The retention period and location for decrypted traffic data.
	  ▪ Potential purposes for decryption beyond cybersecurity and how to limit if appropriate.

Compliance	▪ **Review initial recommendations and indicate specific compliance concerns** to develop the initial boundaries for security, risk, and legal to work within across all relevant regulations (such as GDPR, CCPA, HIPPA, and PCI). ▪ **Ensure approved policies meet the applicable requirements** under all regulations to which the organization is subject.
Data Protection Officer	▪ **Set policy governing the use of decryption tools and associated controls** by working with the cybersecurity and compliance teams. ▪ **Provide guidance on the balance** of organizational risk and employee privacy. ▪ **Monitor the implementation** to ensure it remains within the predefined guardrails. ▪ **Receive and respond** to complaints and data subject access requests. ▪ **Document the data processing activity** within the company record of processing activities. ▪ **Conduct the data privacy impact assessment.** ▪ **Represent the company** with trade unions and regulators as required.

Group/Role	Key Responsibilities
Risk	▪ **Provide inputs into the risk analysis** from a cybersecurity, compliance, legal, and business perspective. ▪ **Help weigh the proportionality** of the invasiveness of proposed decryption measures versus the risk of not decrypting network traffic.
Legal	▪ **Advise on employment matters** including external engagement with trade unions and internal communication to employees. ▪ **Coordinate with risk and compliance** to minimize the potential for litigation.
Human Resources	▪ **Advise on groups and roles** excluded from decryption policies. ▪ **Assist in translating legal and technical policies** into actionable employee communications. ▪ **Participate in discussions** with employee trade union representation.

Source: Enterprise Strategy Group

Create Detailed, Documented Policies for the Collection of Decrypted Data

With the correct stakeholders engaged and initial justification established, creating proportionality becomes critical. Delineating inbound versus outbound traffic may be the first step, where the vast majority of inbound traffic is designated as suspicious and subject to decryption more broadly, while outbound traffic is treated as less hostile and only decrypted in a narrow set of circumstances. Teams must identify the types of financial, healthcare, ecommerce, and other websites employees send outbound requests to that should remain exempt from decryption.

Conversely, they also must identify traffic flows that are most likely to include sensitive corporate data to ensure data loss prevention solutions have the visibility they require to prevent data leakage. Policies may dictate that decryption is handled differently for certain groups or roles (such as those in HR and those with elevated privileges that may be targets for cyberattack) to ensure sensitive data is not compromised. Finally, local regulations may vary on the question of decryption, making the location of the source and destination of the request key inputs to the policy matrix.

Establish Stringent Controls for the Management of Decrypted Data

Because decryption will inevitably result in the collection of personal information, strong controls must be put in place to secure the processing of this data. Encryption should be used both for data at rest and in motion to secure information where it resides and when it is sent to other tools for analysis. Ideally, data collected should be obfuscated by default to protect the anonymity of the individuals subject to the processing from internal teams. This data should be available to a limited group of roles and individuals, only under very specific conditions, and with strong and auditable access controls in place to prevent unauthorized usage. Security administrators should not be able to access data identifying individuals unless there is a valid need—specifically, an attack was detected that requires remediation or data exfiltration was observed that warrants an investigation. In certain jurisdictions, it may be necessary to involve employee representation in cases where the individual is unmasked. Policy should be very clear on the circumstances and process required for individual identification to occur.

Because decryption will inevitably result in the collection of personal information, strong controls must be put in place to secure the processing of this data.

Further, organizations must specify the retention period and location of collected data, as well as the analysis processes that will be used. Organizations may decide to set different retention timeframes for different types of sessions, dependent on a host of factors. Local retention is often more straightforward, while cloud storage may generate additional requirements as a result of the July 2020 Court of Justice of the European Union decision, which invalidated the EU-U.S. Privacy Shield framework. For processing, it must be decided if artificial intelligence (AI) will be used for anomaly detection,

and if so, specified to exclude the profiling of individuals to ensure the scope is limited solely to identifying relevant cybersecurity patterns and deviations.

With these controls determined, a data privacy impact assessment must take place (DPIA), the format of which may vary based on the jurisdiction under which decryption will be implemented. These assessments describe the purpose of data processing and operations to support data processing; provide an assessment of the necessity and proportionality of the processing as well as the risks to the rights of data subjects; and outline how the personal data collected will be protected and the measures taken to protect them effectively. Especially given the requirements of Article 6 to demonstrate the balance of interests between the legitimate interests of the data controller and of the data subject, the DPIA will become a key statement of record on how that balance was determined and the steps taken to manage the different interests. As a result, the DPIA ultimately serves as the official record for the regulator of how the decision to decrypt was reached, how proportionality was assessed, and most importantly, how identified risks have been mitigated.

Maintain Transparency Through Clear and Specific Communications

After establishing policy and completing the required assessments, organizations must engage with the users of the network to communicate the established policies to ensure transparency. In European countries, coordination with workers councils and trade unions will likely take place. Many organizations build on established acceptable use policies to disseminate the details of decryption initiatives. The business must clearly state how decryption is used and why, what data is captured, if AI is used and for what reasons, what traffic is exempted, the parameters of the processing that have been established to safeguard data that is collected, and the rights of the employees. Employee rights should specify how data subject access requests, including erasure and rectification, will be handled, and that data collected will not be used for purposes outside cybersecurity, such as employee management or profiling. It should also be highlighted that these communications may be relevant not only to employees, but also to guests, contractors, customers, and any other users of the corporate network.

How Centralized Decryption Solutions Can Help

To support the policies and procedures required to ensure decryption remains justified and proportionate, technology that can enable the initiative is required. While individual security products such as next-generation firewalls and secure web gateways do support decryption, managing the breadth of policies required to limit decryption to the established parameters at scale often requires a centralized approach. As such, centralized decryption solutions can help organizations seeking to selectively decrypt and inspect network traffic while maintaining compliance with GDPR and other privacy regulations by combining granular policy enforcement, centralized management, and strict security controls. Specifically:

- Granular policy enforcement. To support the selectivity with which decryption must be implemented, the policy engine in a decryption solution must be extremely granular. While the initial factor in a decryption decision may be the destination website to prevent sensitive personal information from being collected, additional considerations including geography, data streams, and user roles, among others, quickly complicate the process.

- Centralized management. Similarly, to ensure the security of the data collected, a centralized solution can provide a streamlined approach to create access, encryption, logging, and retention policies with the specificity required to support decryption while maintaining privacy. Further, these solutions provide a clear audit trail showing network activity and administrator actions to identify if data has been improperly accessed.

- Strong security. Centralized decryption solutions can help improve employee privacy by enforcing strict encryption policies. Personal information is put at risk when attackers set up spoofed sites using weak SSL certificates, or

legitimate sites cut corners through subpar encryption standards. In either case, a centralized decryption solution can improve visibility to ensure the connection is not malicious, or simply block traffic to the site altogether based on predetermined encryption standards.

The Bigger Truth

The conversation around privacy and security is more relevant than ever given the increasingly digital and interconnected nature of most people's lives whether at home, at work, or in public. However, the saying "you can't have privacy without security, but you can have security without privacy" is testament to the fact that striking a balance between the two is a complex task. Organizations face an increasingly difficult challenge to protect their users, infrastructure, and data from cyberattack. Yet, this does not provide free rein to shift the balance further toward security at the expense of privacy. Rather, organizations must target proportionality by focusing not only on the greatest risks to their business, but also the most critical risks to user privacy. Decryption is a perfect example of why this balance must be struck. There is no one-size-fits-all approach to this process, and every organization must assess its situation specifically to determine the best course of action. However, all successful initiatives will seek to emphasize transparency, minimize invasiveness, and limit risk to both users and the organization.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188