EXTRAHOP

WHITE PAPER

Encryption vs. Visibility: Why SecOps Must Decrypt Traffic for Analysis

Research shows that enterprises are increasingly encrypting traffic inside corporate networks (the east-west corridor), on the public internet, and in the north-south channel between them. Studies also indicate that attackers are intentionally using encrypted traffic to hide their malicious acts more than ever before. In this paper, you'll learn about several options for retaining the needed visibility to detect and respond to threats in encrypted traffic. You'll also learn how ExtraHop decrypts critical traffic in real time, out of band, with no performance penalty, to enable SecOps to see and fight threats that are hiding in the encrypted dark space.

TABLE OF CONTENTS

Why Enterprises Are Rapidly Enabling Strong Encryption

In the past, and even today, many enterprises neglected to encrypt the traffic traversing the east-west corridor inside their network. Encrypting data takes work, introduces complexity and cost, and reduces the visibility that security operations teams have into their business's critical systems and data. SecOps teams need this visibility to do their jobs, and for this reason, may feel conflicted about encrypting data in flight inside the network.

However, as general concerns about data privacy grow and new regulations like the EU's General Data Protection Regulation (GDPR) have come into effect, the adoption of in-flight data encryption on the web and inside the enterprise has dramatically increased. Today, the majority of traffic — in the datacenter and across the internet — is encrypted, and this is unlikely to change.

But application traffic isn't the only thing being encrypted. Zscaler's ThreatLabz threat research team reported a huge surge in encrypted attacks last year (in 2024), over 32 billion blocked attacks. In fact, over 87% of all blocked attacks used some form of encryption — which is an increase of 10% from the previous year. So, a higher percentage of ALL attacks are encrypted, and there are more overall encrypted attacks than ever before. **Now is a good time to review your decryption strategy**.

Why Decryption Is Necessary for SecOps Success

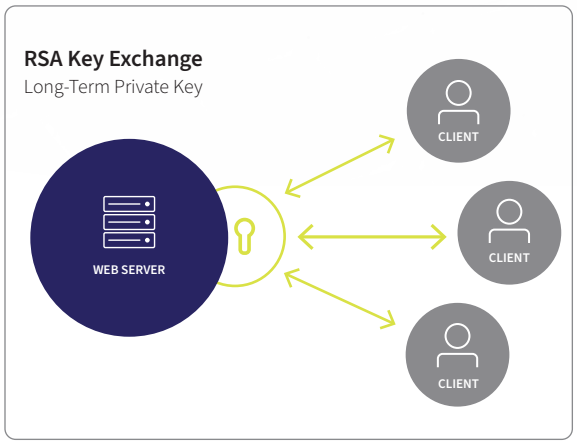
Encryption is on the rise, and it's a good thing for privacy. But it's also a boon to hackers. Encryption, both inside corporate networks and on the public internet, creates blind spots that attackers use to hide their activities from security teams.

Cybercriminals have taken the cue and are increasingly hiding their malicious activities inside encrypted traffic. Malware continues to be the most prevalent form of attack that leverages encryption. In 2024, over 84% of blocked attacks were malware that leveraged encryption for C2, privilege escalation, and lateral movement, according to Zscaler's Threat Labz. Encryption makes it easier for attackers to mask payloads and evade many traditional security measures. Furthermore, attackers are learning to "live off the land" by using existing systems and technology inside their target networks to move laterally and escalate privileges. RMM tools are becoming infamous as legitimate tools for malicious hackers. Encryption is vital for security and privacy, but it can be a double-edged sword when attackers are able to hide their malicious actions in legitimate-seeming encrypted traffic using approved capabilities in their target networks.

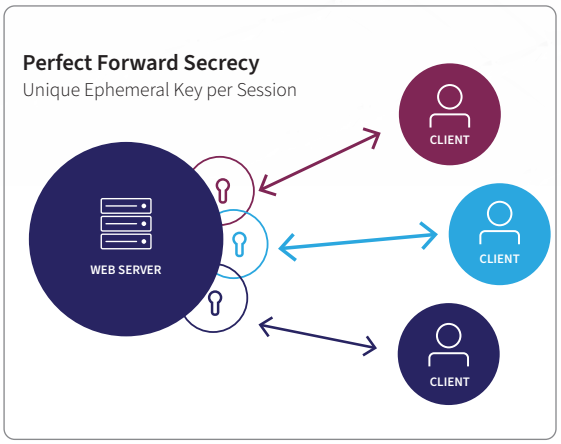
For all these reasons, visibility into encrypted communications is essential for detecting malicious access patterns to databases, storage, and APIs, as well as internal authentication activity associated with lateral movement, data staging, and privilege escalation. Analyzing the decrypted contents of transactions across the network allows for faster identification and remediation of threats before a headline-making data breach happens. On the other hand, decrypting traffic indiscriminately can introduce the risk of having sensitive data in cleartext, making it easier for hackers to steal, and may violate regulations for businesses that handle PCI or HIPAA-regulated data, or businesses subject to GDPR.

The Evolution of Ciphers and Standards: Perfect Forward Secrecy & TLS 1.3

Not only is encryption growing more prevalent, but encryption itself has changed in ways that introduce challenges for visibility. In March of 2018, IETF ratified TLS 1.3 as the new standard encryption protocol for network communications. The most impactful aspect of this update is the requirement of Perfect Forward Secrecy (PFS). Previous versions of TLS allowed the use of the now-deprecated RSA ciphers for key exchange, and allowed servers and clients to use long-term private keys from which individual session keys could be derived. This meant that if the private key for a server or client was compromised at any point, all of that device's communications over the period of time the key was in use would be vulnerable to malicious actors. PFS, using Elliptic Curve Diffie-Hellman Encryption, creates an ephemeral session key, or "secret," for each conversation. The ephemeral secret is only used for that conversation and cannot be derived from the private key of either the server or the client. Even if an attacker compromised a session secret, it would only decrypt that session. Other sessions with the same server would still be secure. For hackers trying to steal large databases of intellectual property or millions of credit card numbers, this presents a significant challenge.



RSA key exchange, now deprecated, used a long-term private key that meant if the key was compromised, many communications over a long period of time could be decrypted.



With PFS, standard in TLS 1.3, every session is encrypted with a new ephemeral session secret, so that any compromised key can only decrypt a single session.

Unfortunately, the same challenge is presented to SecOps teams, which need visibility into their traffic in order to detect and investigate threats. This challenge is not limited only to TLS 1.3. Any environment with perfect forward secrecy enabled, regardless of TLS version, will potentially experience this loss of visibility.

How to Decrypt Traffic for Analysis: A Tale of Two Methods

There are two models for accessing and decrypting data for security analytics:

1. Interception/Man-in-the-middle
2. Out-of-band monitoring and decryption

The interception, or man-in-the-middle (MitM), model requires placing a device in-line on the network so that all messages passing across the network are captured by the MitM device, decrypted, analyzed, and then re-encrypted and sent along to their final destination. Though this model is widely used, recent research has shown that it introduces more security risks than it solves. Because MitM devices decrypt data in line, they have to at least temporarily store

cleartext data, making them a juicy target for hackers. Research also shows that up to 60% of MitM solutions increase risk by re-encrypting messages using a weaker cipher suite than the original message had used. Additionally, MitM solutions inherently introduce network latency, and none are architected to perform well at the scale and throughput levels required by today's enterprise networks.

Therefore, the out-of-band monitoring and decryption method is preferable for SecOps teams monitoring internal (east-west) traffic for hidden threats. Out-of-band solutions acquire a copy of network traffic from a network tap or port mirror. Since they're not preventing the original communications from going through, they do not introduce any network latency, nor do they need to re-encrypt the communications, which eliminates the risk of using lower-quality encryption algorithms.

How ExtraHop Out-of-Band Decryption Works

ExtraHop is an out-of-band solution that conducts all decryption and analytics "on box." This means it never needs to send any cleartext data across the network or re-encrypt any messages. This approach means that ExtraHop introduces no risk to the traffic it monitors, unlike MitM solutions.

Data Acquisition

For hardware-based out-of-band solutions, acquiring data via a network tap or port mirror is a fairly straightforward process. ExtraHop appliances can ingest, decrypt, and analyze up to 100 Gbps of traffic in real time. In cloud environments, ExtraHop uses either Microsoft Azure vTAP or Amazon VPC Traffic Mirroring to acquire the packets.

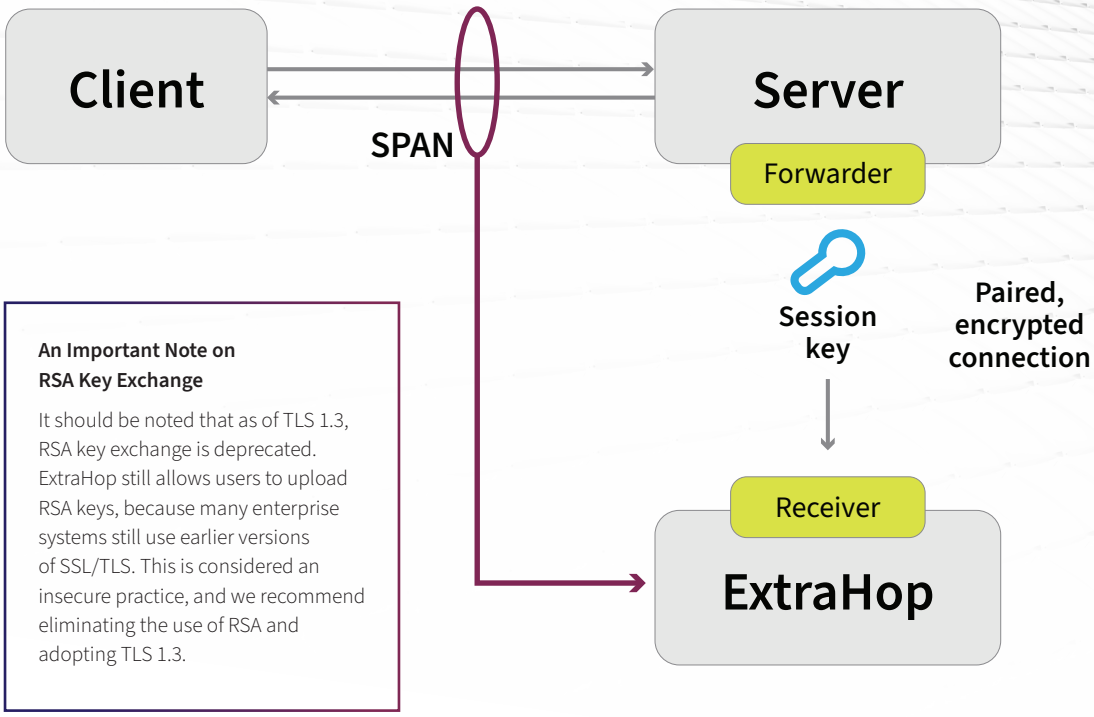
Taking Advantage of Decryption While Still Protecting Sensitive Data

ExtraHop is designed to provide users with deep, meaningful network traffic analysis while protecting the privacy of sensitive data, personal identifiers, or data regulated by various industry standards such as HIPAA, PCI, SOX, GDPR, and others. Customers choose exactly which traffic to send to ExtraHop for analytics so they can avoid analyzing sensitive or regulated data. However, it is unnecessary to completely ignore sensitive traffic this way because ExtraHop, by default, does not expose data that is in scope for the above-listed regulations. The platform provides customizable controls for data access using **Application Inspection Triggers** and **Role-Based Access Controls (RBAC)**, so SecOps teams can get the visibility they need while staying fully compliant.

Using and Protecting Your Private Keys in TLS 1.3

ExtraHop accesses the ephemeral session secrets for each conversation with a lightweight secret-sharing agent installed on each server whose communications need to be decrypted.

The agent securely transmits session secrets from each server across a PFS-encrypted channel to the ExtraHop appliance, where they are securely stored and only accessible to users with the highest level of administrative privilege.

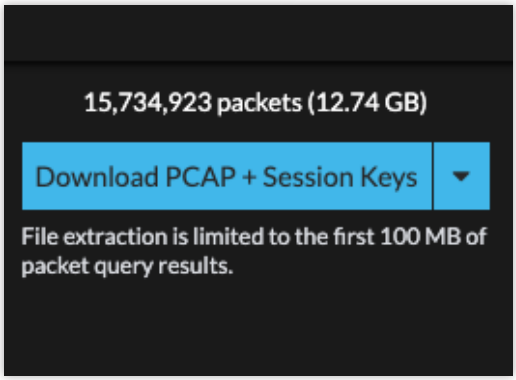


An Important Note on RSA Key Exchange

It should be noted that as of TLS 1.3, RSA key exchange is deprecated. ExtraHop still allows users to upload RSA keys, because many enterprise systems still use earlier versions of SSL/TLS. This is considered an insecure practice, and we recommend eliminating the use of RSA and adopting TLS 1.3.

Accessing Critical Data With Need-to-Know Decryption

Normally, you can get all the information you need for incident investigation and response from the metrics provided by ExtraHop without needing any person to lay eyes on unencrypted data. However, sometimes seeing the packets themselves is the only way to prove exactly what happened. Whether you're proving to a third-party vendor that their action constituted an SLA violation or providing evidence of regulatory compliance, sometimes you need access to cleartext packets.



RevealX™ makes it simple to download precise packet captures and TLS 1.3 session keys for immediate forensic investigation or encrypted data.

ExtraHop is able to provide highly granular, role-based access to the decryption keys for specific sessions. We've covered how the data and PFS session keys are acquired in earlier sections. Here's what the experience is like for individual users:

ExtraHop users may be assigned one of three levels of access:

1. No Access
2. Access to Packets Only
3. Access to Packets and Secrets

Users with access to packets and secrets will see a new "Download Session Keys" button when looking at packets in ExtraHop. This will enable those users to download the asymmetric key to decrypt the packets transmitted between the specific clients, during the specific time window of their search. The nature of asymmetric key encryption means that the keys accessible by highly privileged ExtraHop users can only decrypt the exact packets the user selects. Even if the asymmetric key was compromised, it could not be used on anything beyond that narrow range of packets.

Diving Deep With Wireshark

While ExtraHop uses its decryption capabilities to provide the richest data for real-time analysis and metrics, and to provide data for machine learning behavioral detection, the product does not provide the capability, on-appliance, to manually examine individual packets that have been decrypted using PFS session keys. To decrypt and examine downloaded packets, users with the highest level of privilege need to **download the session keys and the relevant PCAP files and use Wireshark to open and examine them**.

How Hackers Hide Their Tracks With Encryption

The visibility challenges for security operations teams will only grow more pressing as hackers get better at using encrypted channels inside target networks to conceal their reconnaissance, privilege escalation, data staging, and lateral movement activities. By decrypting all TLS traffic between critical assets inside the network, SecOps teams can more easily distinguish normal, benign TLS communications from those being used by bad actors to conceal recon, lateral movement, unauthorized database access and authentication transactions, and more.

Attackers often take advantage of the encryption already in place inside the target network. For example, if an attacker has compromised an internal client and is using that machine to attempt to log into a sensitive database, those communications are likely already encrypted. An analytics tool without decryption capabilities would see that some communication had happened between the compromised machine and the database, but not much else. An analytics tool with L7 visibility and PFS decryption would be able to see that the compromised machine was repeatedly trying and failing to log in to the sensitive database — or worse, that they successfully logged in, retrieved sensitive data, and then dropped the audit table to erase their tracks. The added context and detail offered by both L7 visibility and decryption can make a material difference in the SecOps team's ability to understand the level of risk and react appropriately.

A third, less common scenario occurs when attackers actively encrypt their own communications using different methods or protocols than those present on the target network. If these communications are observed by an analytics tool without decryption capability, they may appear as benign network traffic. However, if the SecOps team is decrypting all of their other network traffic, and they encounter a conversation that can't be decrypted, that provides a strong, immediate signal that the traffic is malicious and should be investigated.

Is Decryption Necessary for Detection and Investigation?

Many vendors of monitoring and analytics products make the claim that it is unnecessary to decrypt traffic for analysis. They believe SecOps teams can get enough information out of limited data, such as NetFlow and log analytics, or by analyzing still-encrypted traffic. For the reasons listed in this brief, they are wrong. Decrypting and analyzing packets all the way down to the application transaction payload at Layer 7 frequently provides a level of definitive insight that allows SOC analysts to prioritize their actions and respond confidently before damage is done, in a way that simply isn't possible with encrypted data limited to L4 flow communications.

What About TLS Fingerprinting? Don't JA3 Signatures Work?

Yes! In fact, we love fingerprinting methods, and we were thrilled to build support for JA3 and JA3S into ExtraHop.

TLS fingerprinting absolutely has a place in the SecOps toolbox. JA3 signatures are a great way to tell when new applications show up on your network, and even tell when a novel application starts communicating with a new endpoint. The combination of JA3 and JA3S is particularly good for detecting stealthy command & control traffic. This approach of analyzing encrypted traffic can provide a valuable puzzle piece, but not a complete picture. ExtraHop supports JA3 and

JA3S fingerprints for all TLS traffic, and also provides real-time TLS decryption for critical assets, even when perfect forward secrecy (PFS) is used, allowing complete visibility and end-to-end investigation and forensics into threats against essential infrastructure.

What Is "Encrypted Traffic Analysis" and Does It Work?

This one is a little more complicated. When vendors say "encrypted traffic analysis," they often mean that they are inferring malicious behavior by looking at the sequence of packet lengths and times (SPLT) in observed transactions.

For example, after an adversary compromises a machine inside the target network, they are likely to try to move laterally to find and access databases containing valuable data. An encrypted traffic analysis vendor might see the related database traffic and might be able to see that the cadence of the compromised machine's interactions with the database doesn't look the same as usual interactions with that database. There is some truth to this claim, but the approach is akin to a signature-based approach. Attackers can always change their patterns of behavior to avoid detection through these mechanisms. Signature-based detection, whether the signature is a hash of a specific malware, or a behavioral fingerprint, will always require constant upkeep because adversaries adapt.

A product that decrypts this traffic and inspects the payload itself would be able to see whether the actual methods being used look malicious. For example, seeing a series of SELECT* methods followed by a DROP TABLE would be a much clearer signal of malicious activity than a change in timing or volume of transactions. Decrypting traffic for analysis is often the only way to confidently differentiate legitimate use of a protocol from malicious tunneling by an attacker living off the land.

ExtraHop is the only network traffic analytics product capable of decrypting PFS traffic at line rate at sustained 100 Gbps of throughput to provide complete visibility, real-time detection, and guided investigations about the things that matter most to the SOC.

Learn More About Why SecOps Needs Decryption to Succeed

www.extrahop.com/resources/papers/encryption-weaponized-ebook

www.extrahop.com/blog/detect-malware-in-encrypted-traffic

www.extrahop.com/blog/why-decryption-is-neccessary-for-security

Already a Customer and Want to Get Started?

Here are some handy links to ExtraHop documentation about how to get started with decryption in ExtraHop Network Traffic Analytics:

1. Decryption Concepts in ExtraHop
2. Perfect Forward Secrecy Basics (Windows)
3. TLS Decryption

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com