Removing Encryption as a Barrier to Investigation

Understanding Encrypted Network Traffic Analysis

WHITE PAPER

LiveAction®

Table of Contents

03 Executive Summary

04 Trends in Encrypted Network Traffic

06 Current Approaches to Encrypted Network Traffic

08 New Strategy: Encrypted Traffic Analysis

10 Buyers Guide for Encrypted Network Traffic Solutions

11 Conclusion

Executive Summary

Organizations have a problem they know about **but cannot see**. The majority of modern IT network traffic is now cloaked in encryption. Those with malicious intent are taking full advantage of this trend. Ransomware groups, phishing attack operators, and even insider threats are hiding their actions inside encryption.

Look no further than headline making cyberattacks against companies like Colonial Pipeline, Kaseya, and Equifax.

A recent Gartner note on Emerging Technologies and Trends explains why hiding within encryption is a tactic of choice for attackers: "An embarrassing amount of traffic in organizations today goes uninspected simply because it is encrypted. This is not acceptable."

If it is unacceptable and drives risk, then why is it happening? There are a number of factors.

Due to evolutions in the space, legacy tools for inspecting network traffic are largely obsolete and approaches that decrypt some data are rapidly becoming less effective. Network visibility is declining across the board, making detection and investigation more difficult. Clearly, something must change.

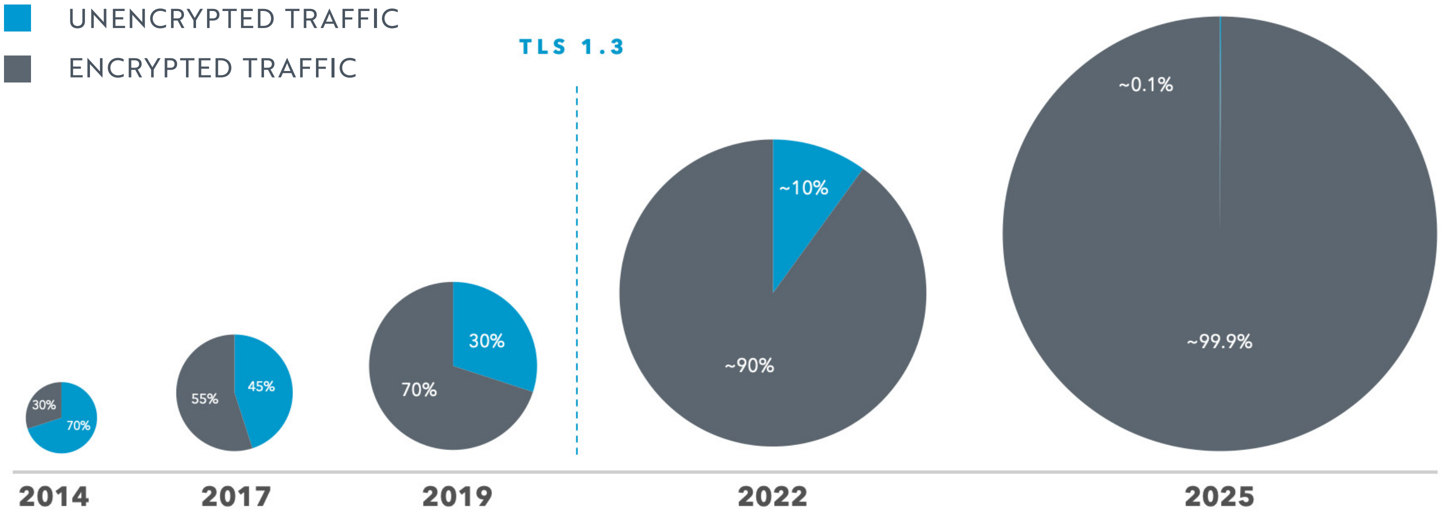
This White Paper examines encryption trends, current approaches to the challenge, and a next generation strategy for detecting advanced cyber threats, regardless of encryption. This new approach is Encrypted Traffic Analysis (ETA) and it allows organizations to maintain **encryption, privacy, and cybersecurity** without compromising one for the other.

Trends in Encrypted Network Traffic

The volume of encrypted traffic is growing rapidly. Many organizations report that 90% of their network traffic is encrypted. Soon, it may all be this way.

Large players like Google are writing about their push for complete encryption. “Security is a top priority at Google… our goal is to achieve 100% encryption across our products and services.”

Encrypted Traffic is a Growing Concern



Network Security Issues

- Declining Network Visibility
- >90% of Malware hides within encryption
- New Protocols: TLS 1.3, QUIC, DoH
- DPI-based tools are going blind

Trends in Encrypted Network Traffic

Clearly, we are headed toward network environments where nearly all traffic is encrypted. And deployment of popular encryption methods is increasing. For example:

Hypertext Transfer Protocol Secure

HTTPS/TLS

The baseline for securing web traffic through encryption, is pushing out unencrypted connections

Virtual Private Network

VPN

Use of these encrypted tunnels to connect to a corporate network via a public network has skyrocketed

SecureShell

SSH

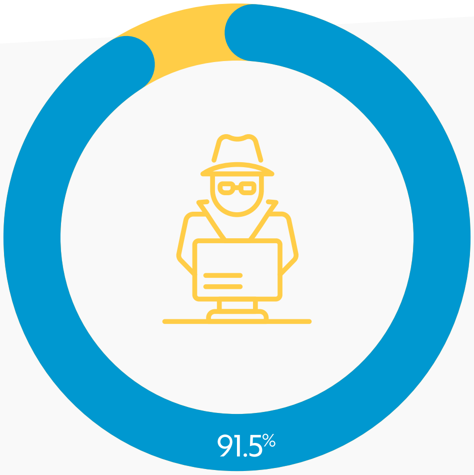
A cryptographic protocol for operating network services securely over an unsecured network

Gartner points out that **increased encryption is a double-edged sword** for organizations and SecOps teams. “While encryption is a great method to protect an organization’s data and communications, it is also a great tool for bad actors to communicate and attack and infiltrate an organization.”

Threat actors understand this and are frequently targeting network visibility blind spots, as DarkReading reports: “91.5% of malware detections in the second quarter of 2021 involved malware arriving over HTTPS-encrypted connections.”

Detection and investigation is becoming more difficult. Encrypted traffic on networks is growing. Cyberrisk is growing right along with it.

> “91.5% of malware detections in the second quarter of 2021 involved malware arriving over HTTPS-encrypted connections.”



Current Approaches to Encrypted Network Traffic

The landscape is shifting, and the challenge of encrypted network traffic is greater than ever. Unfortunately, the effectiveness of some common strategies is decreasing at the same time. Let's look at the reasons for this as we explore common approaches to encrypted traffic on the network.

Rules based approach to encrypted network traffic

In the past, IT and security teams could simply examine data packets. There was an incredible amount of network traffic in plain-text, allowing traditional rule based tools to be quite effective at inspecting data flows. This approach relied on things like next-gen firewalls, data loss prevention (DLP) and intrusion detection (IDPS). With 90% of network traffic now encrypted, these tools are rendered largely ineffective for this purpose.

The European Union Agency for Cybersecurity (ENISA) explains why this legacy approach is no longer satisfactory: "Organizations relying on such controls for their information security lose valuable insight and end up having blind spots in their managed infrastructure."

Decryption based approach to encrypted network traffic

Some organizations utilize a **data decryption** strategy to try and gain visibility into encrypted network traffic. Decryption tools capture certificates, break the encryption, and inspect the data. Then, organizations must re-encrypt and re-certify it. This is sometimes referred to as a 'man-in-the-middle' approach, as you intervene in the middle of the traffic process.

Those taking this approach are partially successful. However, significant amounts of data simply cannot be decrypted. This can be for a variety of reasons, including the growing use of custom and non-standard encryption.

> “Organizations relying on such controls for their information security lose valuable insight and end up having blind spots in their managed infrastructure.”

Current Approaches to Encrypted Network Traffic

Here are some additional challenges to this approach, as reported by those who have tried a data decryption strategy.

- **Added Business Risk & Liability**
  You may be breaking the law or falling out of compliance when you break encryption of some traffic.
- **Complex deployment & management**
  You must properly generate and store private keys, create whitelists of approved applications and more.
- **Not all data can be decrypted**
  Decryption blind spots are increasing with the evolution of encryption tools. Blocking or allowing unreadable traffic is required by this approach.
- **High expense**
  Organizations purchase a full security stack (decryption tools) at every edge in the enterprise; often, these are big boxes for a small interface.
- **Degraded network performance**
  Each stack of decryption tools is a potential choke point on the network. SecOps can cause a NetOps problem.
- **Agents Required**
  Decryption tools are typically limited to Windows & Linux systems.

There is another crucial detail to be aware while considering decryption as a strategy. **It is becoming less effective**. The rapid deployment of encryption protocol TLS 1.3 increases the amount of network traffic that cannot be decrypted, even with the use of decryption toolsets.

Clearly it is time for a new strategy for handling encrypted traffic and securing your organization against it.

ENISA says something called Encrypted Traffic Analysis (ETA) may be the right approach. Let's look at what it is and how it operates.

New Strategy: Encrypted Traffic Analysis

A new approach to detect advanced threats on the network and enable rapid investigation is called Encrypted Traffic Analysis (ETA), and it is unfazed by encryption. Instead of relying on plain-text or data decryption attempts, it looks at traffic behavior on the **network regardless of encryption status**.

The fundamentals of this approach combine data collection, advanced behavioral analysis, and machine learning (ML). Mature ETA solutions analyze traffic in real-time, strictly with flow data, and then aggregate and correlate multiple events to provide the context security teams need. This **complex event processing** is powerful and feeds into SOAR and SIEM.

The strategy gives insights into how encryption is used and misused in your environment. It results in decreased time to detect threats that bypass existing security controls, and accelerated response for SecOps teams. Innovative ETA solutions also enrich the data, threat score it, and deliver it SOC ready with Mitre ATT&CK labeling.

Surprisingly, this approach maintains security and privacy compliance throughout the process.

Andrew Fast, Chief Data Scientist at LiveAction, explains:

"When people think about privacy vs. security, they typically think of tradeoffs. They think that they are conflicting in some way. Some approaches require this. However, you can still have security while maintaining privacy if you take the encrypted traffic analysis approach."

This is possible because you gain visibility into network and device anomalies without decrypting traffic.

Use cases for ETA

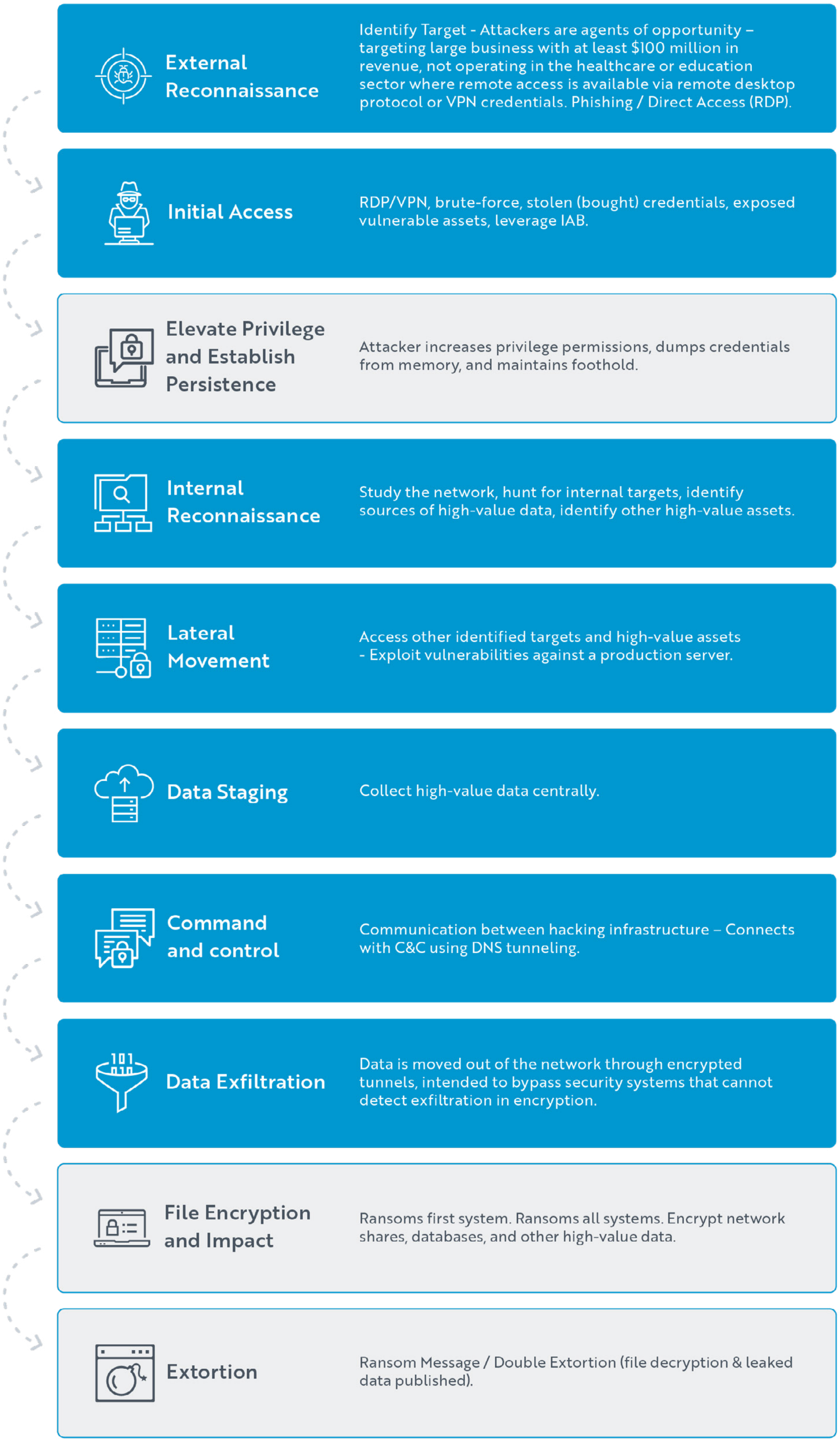
This strategy covers various use cases, ranging from hands-on keyboard attacks to phishing.

In the case of a sophisticated phishing attack, ETA analyzes the packet dynamic structure of legitimate websites, which behave differently than those of phishing sites. This difference and behavior can alert responders if end-users or devices communicate with a malicious site. This is how ETA can rapidly reveal a phishing attack regardless of encryption.

Another way to view the ETA approach is to look at how it can help disrupt a modern cyberattack, like ransomware. The attack unfolds in stages, and network defenders are often left in the dark, as attackers remain cloaked behind the encryption barrier. Not with ETA.

> “When people think about privacy vs. security, they typically think of tradeoffs. They think that they are conflicting in some way. Some approaches require this. However, you can still have security while maintaining privacy if you take the encrypted traffic analysis approach.”
>
> —Andrew Fast, Chief Data Scientist

New Strategy: Encrypted Traffic Analysis



External Reconnaissance
Identify Target - Attackers are agents of opportunity – targeting large business with at least $100 million in revenue, not operating in the healthcare or education sector where remote access is available via remote desktop protocol or VPN credentials. Phishing / Direct Access (RDP).

Initial Access
RDP/VPN, brute-force, stolen (bought) credentials, exposed vulnerable assets, leverage IAB.

Elevate Privilege and Establish Persistence
Attacker increases privilege permissions, dumps credentials from memory, and maintains foothold.

Internal Reconnaissance
Study the network, hunt for internal targets, identify sources of high-value data, identify other high-value assets.

Lateral Movement
Access other identified targets and high-value assets - Exploit vulnerabilities against a production server.

Data Staging
Collect high-value data centrally.

Command and control
Communication between hacking infrastructure – Connects with C&C using DNS tunneling.

Data Exfiltration
Data is moved out of the network through encrypted tunnels, intended to bypass security systems that cannot detect exfiltration in encryption.

File Encryption and Impact
Ransoms first system. Ransoms all systems. Encrypt network shares, databases, and other high-value data.

Extortion
Ransom Message / Double Extortion (file decryption & leaked data published).

Let's consider the 'Initial Access' stage of the attack. With Encrypted Traffic Analysis (ETA) powered by machine learning, network defenders will quickly identify anomalies that could be associated with threat actor initial access. That is because ETA creates behavioral baselines to track expected network behavior. It identifies regularly accessed resources, such as RDP, VPN and SSH and maintains an inventory of communications. It can therefore immediately detect when something unusual is happening.

Next, let's consider the 'Data Staging' part of the attack. Ransomware actors regularly hide within encryption to move and stage data they are about to exfiltrate from your network. However, the ETA approach can detect this and allow a security team to stop it.

ETA will detect a host within your network that has consumed an unusually large volume of asymmetric traffic. This alerts your SOC to a significant change in the behavior of that host, which is often the result of a threat actor staging data before stealing it from your network. These are just two examples.

In all the stages highlighted in blue, ETA gives IT and security teams an opportunity to detect and stop a cyberattack.

Buyers Guide for Encrypted Network Traffic Solutions

Newer approaches to significant cybersecurity problems can sometimes feel overwhelming. To help on your journey, here are 6 questions to ask when you are evaluating a solutions provider in the Encrypted Traffic Analysis space.

- **Is Threat Detection in Real-Time?**

  Tools that can process millions of events per second are considered best in breed, but make sure they are engineered to analyze network traffic **without** multiple passes over the data stream.

- **Will this Secure My Entire Network?**

  Look for something with easy to deploy, lightweight software sensors, that can be used anywhere: from core, to edge, to cloud. Ask: how many attributes are you analyzing?

- **Is Machine Learning a Buzzword or Actually Used?**

  A top tier solution will create a historical inventory of traits and behaviors for fingerprinting, for both encrypted and plain-text traffic. True machine learning **must be applied here** to rapidly identify threat actor anomalies.

- **Does the solution rely primarily or entirely on NetFlow?**

  Although NetFlow increases visibility into network traffic and helps with security analysis, NetFlow data is not enough. NetFlow saves resources by examining only a small fraction of network packets. Many threats can remain undetected as a result.

- **Is the Solution SOC Enabled?**

  A product that correlates and enriches traffic with details, risk scores and MITRE ATT&CK labeling is essential. This qualifies, simplifies, and accelerates investigation and response.

- **Will this Help with Compliance?**

  Best in breed solutions will include specific alerting and reporting for security compliance so staying compliant remains front and center.

In Conclusion

The amount of encrypted traffic on the modern IT network is unacceptable, risky, and increasing.

Rule based approaches are obsolete. Man-in-the-middle decryption techniques are expensive and the amount of network visibility they provide is decreasing, as encryption protocols evolve.

Therefore, a future-proofed approach like Encrypted Traffic Analysis is needed. Organizations no longer must choose **either** encryption and privacy—**or cybersecurity**. They can now maintain all three and remove the barrier of encryption for good.

Connect with LiveAction for a personal demo of ThreatEye NV, a powerful Encrypted Analysis Tool that serves both SecOps and NetOps.

You can also learn more from the company's Chief Data Scientist in this on-demand discussion: Detecting Advanced Threats with Encrypted Traffic Analysis

Sources Cited:
Google Transparency Report, 2022
ENISA Report, Encrypted Traffic Analysis Use Cases
Gartner, Emerging Technologies and Trends Impact Radar

© Copyright 2022 - LiveAction. All Rights Reserved.
960 San Antonio Rd, Suite 200, Palo Alto, CA 94303
+1 (888) 881-1116

About LiveAction

LiveAction's ThreatEye Network Detection & Response (NDR) solutions for enterprise threat detection and encrypted traffic analysis are unfazed by encryption. ThreatEye NV is the only platform that tracks, classifies, and characterizes all use of network traffic regardless of encryption status.