DARKReading

WHITE PAPER

Stopping the New Breed of Advanced Encrypted Threats

Close the Visibility Gap with Microsoft and TLS Protocol Decryption

Sponsored by

ExtraHop

Table of Contents

Encryption: The Double-Edged Sword

Broad adoption of encryption technologies is causing major shifts in the security operations and cyber threat landscape. This has led to changes in attacker techniques, creating fertile ground for the evolution of a new breed of sophisticated attacks.

In an effort to ensure that data within their environment remains secure and confidential, more and more organizations are enabling encryption across their network and application protocol portfolios. This is especially true in Active Directory environments where Microsoft has begun simplifying the process due to the many protocols handling credentials and sensitive data. The shift in organizational security posture is long overdue, and almost certain to pay dividends in organizations savvy enough to complete the transition.

Unfortunately, encryption also brings new challenges. While reducing an organization's exposure to a wide variety of vulnerabilities, encryption also negatively impacts visibility into much of the data that security teams traditionally rely on to detect and respond to advanced attackers. As a result, the increasing use of encryption simultaneously improves an organization's security posture while providing attackers new avenues for remaining hidden.

We are only beginning to see the ways in which attackers are capable of turning encryption against security teams, and already the evidence is chilling. Encryption, then, is a double-edged sword that must be wielded carefully.

It's critical to understand why encryption has become standard in the protection of data in transit, and how that encryption can also be abused by advanced attackers to infiltrate, persist, and covertly move laterally within the very networks encryption is designed to protect.

As attackers grow more sophisticated, and regulations require tighter security and privacy measures, there is no escaping the decision to encrypt. Organizations must find a way to balance the increasing expectations for data security and data privacy, against the necessity of maintaining visibility to ensure operational security.

Strategic decryption is emerging as the best way to approach the challenges posed by encryption for SecOps teams. This whitepaper clarifies the risks and rewards of implementing strategic decryption and offers specific guidance for security teams to retain the visibility they need for threat detection, investigation, and response — without compromising on business requirements.

Why Advanced Attackers Love Encryption

More and more businesses have begun to adopt encryption to protect network traffic within their organizations as an enhanced layer of security against malicious attackers. The question, then, is how to minimize the ability of advanced attackers to abuse encryption for their own ends.

Infiltration

Initial access methods remain familiar: phishing emails, compromised credentials, and malicious payloads are common approaches to bypassing perimeter security. However, once attackers gain a foothold within an organization, their tactics shift to focus on expanding their foothold and reconnaissance.

Lateral Movement

Once ensconced safely within a network, advanced attackers turn their attention to reconnaissance, expansion, exploitation, and privilege escalation with the goal of identifying critical systems and valuable data. Often, this includes using Living-off-the-Land techniques to reduce the likelihood of detection.

Living-off-the-Land (LotL)

As the name suggests, LotL techniques focus on utilizing native tools and protocols to achieve a goal. Many native tools such as Powershell, WMI, and MS-RPC have the option to utilize encryption as a security measure. This encrypted East/West traffic is the perfect vehicle for advanced attackers, allowing them to move unseen and undetected in what appears to be legitimate traffic. By enabling encryption, areas that were once fully monitored can become blind spots for cybersecurity teams. Savvy attackers seek out these blind spots to stay concealed while digging deeper into the organization's network.

Although LotL techniques have been a central component of the advanced attacker playbook for some years now, security teams continue to struggle to identify these threats and take remediative action in a timely and effective manner. The addition of encryption to these techniques only increases the difficulty of identifying malicious activity. Attackers have time to establish redundant means of command and control, gain administrator access, and identify an organization's critical data and most valuable assets.

Combating an attacker's ability to leverage encryption for malicious purposes, is critical to maintaining operational security. Without a plan to regain visibility into encrypted network traffic, SecOps will remain blind, and advanced attackers will be able to continue exploiting vulnerabilities, infiltrating or manipulating sensitive systems, and exfiltrating valuable data.

Examples of Malicious Misuse of Encryption

Attackers are using encryption to remain covert, extending dwell times and leading to more devastating impacts. Longer dwell times result in larger quantities of data being stolen, longer and more expensive remediation, and damage to corporate reputation.

- Attackers hiding in encrypted traffic can launch malicious attacks without security teams being aware of them.
- Malware can spread undetected throughout a network, identifying and infecting more endpoints.
- Ransomware can be distributed more broadly in a target network and impact more data, justifying greater payment demands.

The Power of Encryption When Leveraged by an Advanced Attacker

The blind spots created by encryption can be used to carry out advanced attacks while delaying detection for weeks or months.

- PrintNightmare attacks are conducted over an encrypted protocol leaving most network defensive systems blind to attempted exploits.
- ProxyLogon and ProxyShell are vulnerabilities in Microsoft Exchange servers, these vulnerabilities are accomplished by sending encrypted traffic to the server and leaving many organizations completely blind to the attempts.
- Lack of visibility into encrypted traffic allowed the Colonial Pipeline ransomware attack to be carried out successfully.
- Lateral movement was key to the LockBit ransomware attack, allowing attackers to identify and access multiple systems while moving undetected through the network.

These examples showcase the downside of encryption. To make matters worse, logging is only partially effective even when fully enabled, leaving even the most scrupulous security teams with only hypotheses and guesswork when it comes to identifying malicious activity within an environment, or trying to establish a blast radius.

The answer? An ability to identify malicious traffic and activity, using strategic decryption, enables organizations to take back the advantages encryption is intended to deliver. Unfortunately, decryption possibilities are highly misunderstood across the industry, and compliance requirements for heavily regulated industries leave many organizations operating from a position of mistrust.

Encryption — Business Needs vs. Security Necessity

The need to balance business needs with security operations creates conflicts that lead to difficult choices. SecOps teams are often forced into taking on increased risk in one area to decrease risk in another.

For example, encrypting all internal network traffic reduces the risk of data theft or manipulation. However, downgraded visibility increases the risk of failing to detect a cyberattack before an event occurs that results in loss of data. Loss of data, in turn, leads to direct and indirect financial costs, and/or degradation of business value, reputation damage, and loss of public trust.

Vendors looking to address this visibility gap have provided two primary approaches to solving the visibility issue. While these solutions have historically aided many organizations, both technical approaches utilized in the past have suffered from a variety of shortcomings.

- **Encrypted Traffic Analysis (ETA)** is a relatively cost-effective approach which allows traffic to be evaluated and statistically modeled to identify threats. However, ETA implementations have suffered from a lack of forensically actionable data and limited detection capabilities.
- **Traditional Decryption**, sometimes called bump-in-the-wire, middlebox, or the man-in-the-middle approach. This method relies on routing traffic through appliances that decrypt the traffic for security analysis, then re-encrypt the traffic before sending it to its destination. This "in-line" approach has well established negative impacts on network performance and can raise concerns related to user privacy.

There are many cost concerns related to security requirements and resolving "the encryption problem" only adds to this burden. Security costs have been steadily rising across the board as companies are forced to invest in more security tools, more staff, and expensive cyber-insurance.

Traffic visibility solutions often require purchasing larger firewalls, solution-specific hardware, and expensive licenses. This is quickly leading to the relegation of these solutions to organizations with sizable security budgets, leaving smaller organizations uncomfortably exposed.

The Struggle to Maintain Visibility

Security teams are struggling to maintain the visibility needed to detect threats as organizations work to enable additional encryption features. The broad adoption of encryption for East/West traffic is significantly reducing the visibility SecOps teams have historically relied on for post-compromise security detections. Without this visibility, vulnerabilities are magnified, allowing attackers to:

- Target multiple vulnerabilities while remaining covert once infiltration is achieved
- Setup persistence and expand using LotL techniques to move laterally
- Put malware, such as ransomware, in place for eventual execution

In addition, the current trend of attackers leveraging encryption as part of the standard toolkit, puts security teams in a particularly difficult position. Firewall, Proxy, and IDS/IDPS solutions (the most mainstream approaches for the detection of malicious activity) are typically:

- Positioned to monitor North/South traffic, which is a small fraction of the area where attackers abuse encryption
- Not designed with encrypted traffic in mind
- Reliant on easily evaded signature-based detection approaches

Many organizations have turned to ETA as a means of restoring some visibility and detection capability to these encrypted traffic streams. However, while ETA has seen limited success in identifying malicious activity, it is inherently less effective than decryption solutions as it relies on inference rather than definitive evidence.

At best, ETA-based solutions offer a stopgap solution that:

- Meets only bare minimum requirements for data security and detections
- Is often incorporated into existing security tools (such as firewalls) leaving East/West traffic unmonitored
- Makes identifying and investigating detections slow, and based on guesswork
- Does not provide sufficient insight or protection against encrypted advanced threats

Decryption solutions offer an alternative to ETA, providing better visibility and higher quality data for incident investigation. However, traditional in-line decryption solutions suffer from their own set of limitations.

Limitations of Traditional Decryption

Traditional decryption is positioned "in-line", meaning it performs traffic decryption in real time, in the middle of the traffic flow. It is analogous to your mailman opening every piece of mail you send and receive and performing some kind of analysis before sealing the mail back up and delivering it.

In-line decryption has significant security and performance implications which have limited industry

adoption of such solutions. This approach is typically relegated to organizations featuring highly secure environments with experienced SecOps teams and a significant budget to allocate to the process. Common challenges include:

- **Increased security exposure**
  In-line decryption solutions typically introduce appliances to intercept data in-line, which also introduces another point of vulnerability for attacks on the decryption appliance.
- **Impacted network performance**
  Due to the cost of in-line decryption solutions, they are usually purchased with current network performance in mind. As organizations grow, in-line decryption solutions can create traffic bottlenecks and latency issues resulting in poor network performance and unacceptable downtime.
- **Enhanced vulnerability to attack**
  In-line solutions are also subject to MitM (man-in-the-middle) downgrade attacks, forcing servers to downgrade to a less secure encryption protocol. Additionally, many in-line options do not support TLS with PFS, due to the way PFS keys are handled.
- **Limited visibility**
  In-line decryption solutions are typically designed to monitor North/South traffic, looking for malware with known signature sets and providing only cursory log data for forensic investigations.
- **Certificate exposure**
  Finally, in-line decryption poses certificate management and certificate exposure issues, creating the potential for exposure of sensitive information.

In summary, traditional decryption solutions promise improved security and visibility, but only deliver partial results.

Historical Business Concerns with Decryption

There have been two primary concerns with decryption from a business standpoint: legal compliance with data regulations, and the cost of decryption solutions.

Data Privacy Compliance

Organizations have been deluged with new regulatory information over the past few years, leading to heightened concerns over data privacy in relation to decryption. The overarching fear is that decrypting user traffic may result in the interception of private user data such as confidential or protected financial, health, or legal information.

For years, governmental regulations such as GDPR, PCI-DSS, HIPAA, and others have put in place binding requirements for what data can be collected and how it can be transmitted, stored, and shared with other organizations.

These regulations have also outlined the requirement for encrypting data at rest and in transit as a means of protecting sensitive data from prying eyes. In response, many organizations in the EU and US, (or outside but seeking to do business in those regions) have adopted these requirements as a sort of de facto standard for organizational security posture.

While these regulatory frameworks have provided measurable benefits to the security posture of most organizations, there are significant drawbacks to their security teams in terms of visibility into potential malicious behavior. Operations must take into account business needs and security necessities while remaining compliant.

Increased security costs

It is also the perception of many organizations that decryption requires expensive hardware/licenses in addition to increased operational costs. These concerns place a massive obstacle in the way of decryption adoption, especially for smaller companies that don't have a large budget, and worry about the impact of decryption on their limited time, resources, and their bottom line.

Fortunately, there is a solution that both answers privacy concerns and minimizes out-of-pocket costs while delivering a robust decryption solution to increase visibility for SecOps teams: strategic, out-of-band decryption.

Strategic Out-Of-Band Decryption Is the Answer

Overcoming the limitations of in-line decryption solutions requires a significant re-evaluation of the existing threat landscape, and the role of decryption as it applies to an organization's security posture. The result of this re-evaluation is strategic decryption, which leverages an out-of-band approach coupled with enhanced detection capabilities and support for a broader suite of encrypted protocols.

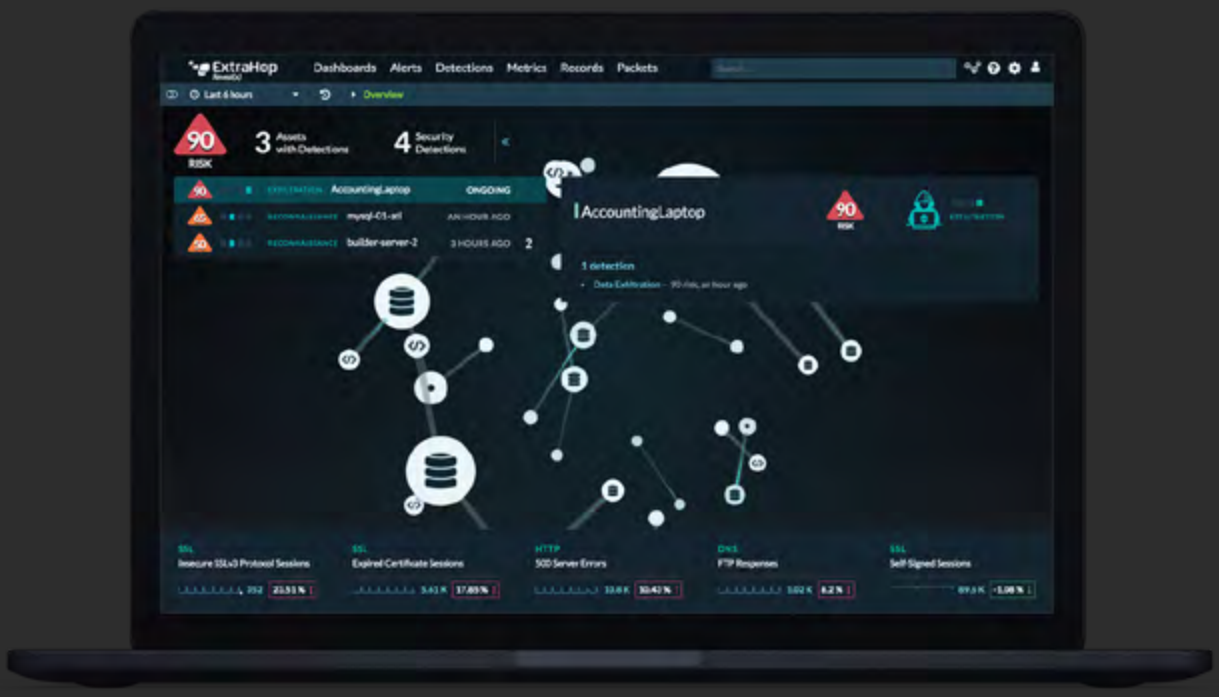
An out-of-band approach is accomplished by creating a mirror copy of traffic provided by an organization's switching and routing infrastructure. This mirror copy of traffic is sent to the decryption solution using traffic aggregation techniques eliminating any impact to an organization's operational network.

Benefits include:

- **Reduced security exposure**
  Out-of-band decryption can be carried out strategically, targeting network pathways where attacks are the most likely, and looking for inconsistencies or signs of irregularities that might warrant closer examination.
- **No negative impact on network performance**
  Encrypted traffic handled by an out-of-band solution is decrypted, analyzed, and then discarded, with no need to re-encrypt and forward the traffic to its final destination. This means there are no bottlenecks — effectively eliminating concerns related to network performance.
- **Minimized vulnerability to attack**
  Since the decrypting appliance is not accessible and has no visible footprint in the operational network that is visible to users and attackers, there is no way for attackers to directly target the appliance as a means of stealing the decryption keys.
- **Improved visibility into East/West traffic**
  An out-of-band decryption solution allows you to easily target and decrypt East/West traffic, giving your SecOps teams a faster path to identifying threats moving laterally within your organization.
- **Less exposure for sensitive data**
  Strategic decryption of East/West traffic is the most secure way to identify lateral movement techniques; you're only decrypting traffic for which you already hold the keys, and the decrypted copy is never stored.
- **Reduced cost of implementation**
  Solutions that offer strategic decryption, such as ExtraHop Reveal(x), address a wide range of security and operations use cases. This broad applicability enables tool consolidation in both the performance and security monitoring toolkits. The result of this, is that strategic decryption is much less expensive than traditional decryption, reducing the impact on budgets while providing a powerful effective solution that addresses far more than just the inherent problem associated with encryption.

INTRODUCING

ExtraHop Reveal(x)



Security teams need a solution that can safely inspect all traffic, including traffic that is trusted and encrypted, and can quickly respond to modern attacks.

ExtraHop Reveal(x) is the ideal out-of-band solution for resource-strapped security teams struggling with the rising challenge of encryption.

The solution provides:

- Comprehensive East/West and North/South visibility
- Real-time threat detection both at the perimeter and inside it
- Fast, intelligent response at scale to minimize impact of an advanced attack
- Simplified certificate and key management

Reveal(x) 360 is a SaaS-based network detection and response platform that automatically discovers and classifies every transaction, session, device, and asset connected to the network. Reveal(x) 360 leverages the power and capability of the cloud to provide uses machine learning capabilities that scale to any size organization. Reveal(x) machine learning is designed to decode and parse more than 70 enterprise protocols and extract over 5,000 features at sustained speeds up to 100Gbps.

In addition Reveal(x) 360 includes 90 days of integrated historical records. The Threat Reports feature alerts analysts to new threats as they emerge providing automated historical investigations, streamlining the investigation of new threats as they emerge.

With Reveal(x) your organization can:

- **Improve overall security hygiene**
  Address activity that represents risk, including cryptographic compliance, misconfigurations, protocol abuse, and vulnerable or non-compliant services.
- **Identify known attacks**
  Swiftly surface malicious behavior, providing analysts in-depth contextual and forensic data including IP addresses, domains, file names, payload strings, and anomalous behaviors identified during past attacks, or from threat intelligence feeds.
- **Flag anomalous behaviors**
  Alert SecOps teams to attacks that may not have a previously known identifier, but are exhibiting anomalous behavior linking back to attack lifecycles.
- **Deliver comprehensive visibility**
  Watch traffic traveling along both North/South and East/West corridors and strategically decrypt based on specific needs and security concerns.
- **Strategically decrypt on demand**
  Depending on the industry and the type of protected data, organizations can customize their decryption approach to the needs of the moment, balancing privacy and protection for optimal results and compliance.
- **Eliminate manual encryption key and certificate management**
  Direct integrations ensure secure and automated transfer of keys to Reveal(x), eliminating time-consuming and error-prone manual key and certificate business practices.

This out-of-band strategic decryption approach eliminates the concerns raised by traditional in-line decryption techniques, while providing a robust solution to the issue of encrypted traffic visibility.

Is Reveal(x) 360 Right For You?

Reveal(x) 360 is designed for organizations of any size to use with ease, and scales effortlessly as you grow to deliver comprehensive, cost-effective cybersecurity with forward and backward compatibility with most security platforms, tools, and protocols.

Reveal(x) supports:

- **SaaS Platforms Including:**
  - » Google Compute Cloud (Google Traffic Mirroring)
  - » Amazon Web Services (VPC Traffic Mirroring)
  - » Microsoft Azure (Rpcap agent)
  - » Most third-party hosting services
- **Strategic Decryption**
  - » Strategically decrypt traffic from specific subnets and hosts
  - » Target specific applications for decryption
- **Support for Modern Encryption Protocols Including:**
  - » TLS 1.3 and below, with or without PFS
  - » Microsoft Protocol Decryption (Kerberos, MS-RPC, SMBv3, and more)
  - » Secure Key Escrow
- **Need-To-Know-Access**
  - » Role Based Access Controls (RBAC)

Reveal(x) gives SecOps teams one-click access to contextual evidence and intelligent response recommendations. Teams will be able to automatically detect new, rogue, and unmanaged devices as well as late-stage attack activities, then validate and remediate threats swiftly.

Reveal(x) integrates with solutions like CrowdStrike, Phantom, Demisto, and Palo Alto Networks to automate or simplify many time intensive tasks such as:

- Device Inventory
- Network Performance
- Incident Investigation
- Remediation

With Reveal(x), your organization gains the ability to identify threats other solutions miss, with strategic decryption that supports perfect forward secrecy, advanced machine learning, and confident response orchestration.

The Right Decryption Solution Is Critical to Effective SecOps

The survival of your enterprise may, at some point, depend on **encryption and decryption**. To be fully prepared to defend against advanced threats, you must:

- Consider current East/West traffic encryption and visibility gaps
- Investigate data-privacy standards in relation to decryption
- Evaluate new out-of-band technologies to address visibility gaps

ExtraHop Reveal(x) can eliminate blind spots, provide 50% faster threat detection, and 84% faster threat resolution.

Read our recent case study to see how ExtraHop's Reveal(x) provides the perfect decryption solution for a **heavily regulated healthcare environment.**

Contact us today for a **free demonstration**.