Eliminate the Biggest Blind Spot with Precryption™

Gigamon Precryption technology delivers plaintext visibility of lateral traffic to the full security stack, including virtual, cloud, and containers. No decryption required.

#1

Concern among IT Security Leaders: ***Blind spots being exploited that you did not know were there***[2]

91%

of threats **use encrypted channels**[3]

81%

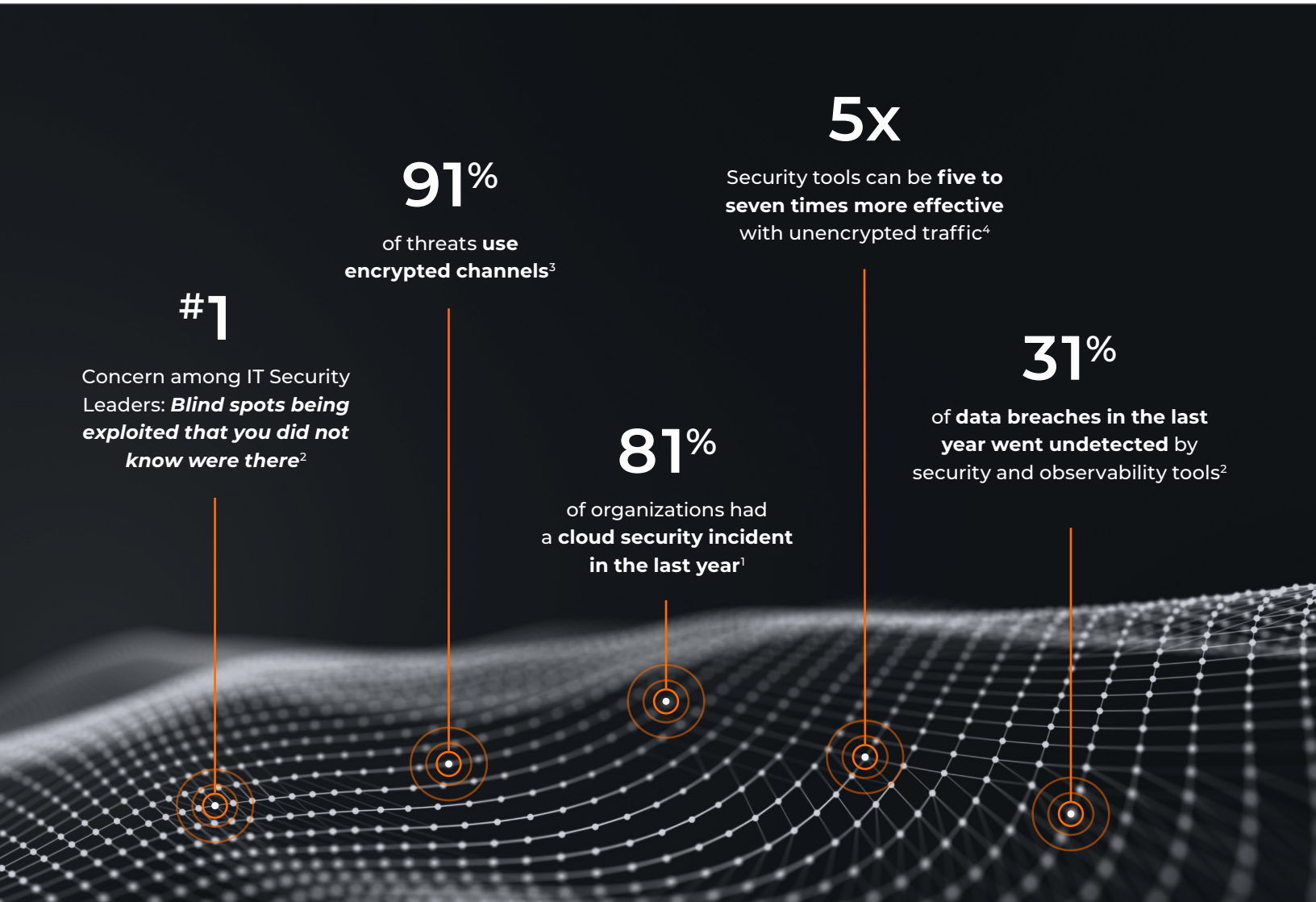
of organizations had a **cloud security incident in the last year**[1]

5x

Security tools can be **five to seven times more effective** with unencrypted traffic[4]

31%

of **data breaches in the last year went undetected** by security and observability tools[2]



Gigamon Precryption™ technology redefines security for virtual, cloud, and containerized applications, delivering plaintext visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption.

Information Security Challenges

1. Increasing Cloud Adoption
2. Dev Teams Running Fast
3. Concealed Threat Activity

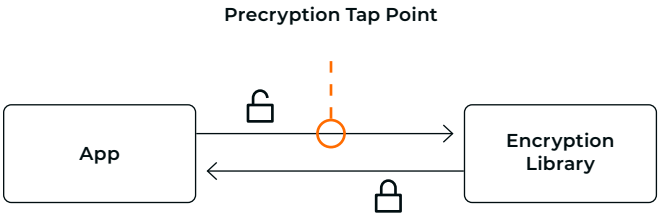
The use of encrypted communications is nearly ubiquitous today across modern hybrid cloud infrastructure, shielding sensitive data from traditional interception techniques. Threat actors have responded with new, more sophisticated approaches to infiltration, compromising key systems to gain access to sensitive data. These infiltrators are now using the same encrypted communication channels to conceal their own activity, especially lateral movement, sensitive data access, and exfiltration. Gaining plaintext visibility into encrypted traffic moving laterally among virtual workloads is nearly impossible using existing solutions on the market, making it extremely difficult to detect concealed threat activity. This is why encrypted lateral communications remain the biggest security blind spot.

Precryption Technology Sees Concealed Threat Activity

Precryption technology is an innovative solution directly addressing the biggest blind spot in today's hybrid cloud infrastructure—lateral movement from threat actors, obfuscated through modern forms of encryption, including TLS 1.3. Precryption offers plaintext visibility into encrypted virtual communications in an efficient, friction-free form factor, without having to run expensive decryptions or getting bogged down with key collection and management.

How Does Precryption Technology Work?

Precryption technology leverages native Linux functionality to tap, or copy, communications between the application and the encryption library, such as OpenSSL.



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy, no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

Precryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms.

As an added bonus, UCT with Precryption technology runs independent of the application, and doesn't have to be baked into the application development lifecycle.

Key Use Cases

Thwarting cybercrime: Lateral movement in the cloud is a blind spot especially evident in cybercrime attacks. Once past perimeter security, encrypted packets go unmonitored, enabling a threat actor to employ all manner of tricks and techniques to evade detection.

TLS 1.3 compliance: Some organizations today have delayed necessary adoption of TLS 1.3 specifically because the lack of visibility into encrypted traffic. Others have resorted to managing separate decryption solutions.

Zero Trust: A key foundation to any effective Zero Trust architecture is the ability to see the packets, to inspect every interaction between resources on the network and apply policy.

Network-derived intelligence: Security tools, like SIEMs, are often reliant on metadata transformation and enrichment to better detect threats.

Why Gigamon Precryption?

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure, providing East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

Key Features

- **Plaintext visibility into communications with modern encryption** (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy)
- **Plaintext visibility into communications with legacy encryption** (TLS 1.2 and earlier)
- **Nonintrusive traffic access** without agents running inside container workloads
- **Elimination of expensive resource consumption** associated with traditional traffic decryption
- **Elimination of key management** required by traditional traffic decryption
- **Zero performance impact** based on cipher type, strength, or version
- **Support across hybrid and multi-cloud environments,** including on-prem, virtual, and container platforms
- **Keep private communications private** across the network with plaintext threat activity delivered to security tools
- **Integration with Gigamon Deep Observability Pipeline** for the full suite of optimization, transformation, and brokering capabilities

Key Benefits

- **Eliminate blind spots** for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls
- **Monitor application communications** with an independent approach that enhances development team velocity
- **Extend security tools' visibility** to all communications, regardless of encryption type
- **Achieve maximum traffic tapping efficiency** across virtual environments
- **Leverage a 5–7x performance boost** for security tools by consuming unencrypted data
- **Support a Zero Trust architecture** founded on deep observability
- **Maintain privacy** and compliance adherence associated with decrypted traffic management

Challenges: A Closer Look

Three significant challenges face IT organizations in securing the systems and data with which they have been entrusted to protect: increasing virtual and cloud adoption, dev teams requirement to move quickly, and concealed threat activity.

1. Increasing Virtual and Cloud Adoption

81 percent of organizations had a cloud security incident in the last year[1]

This movement towards virtualized systems—whether on-prem, private, or public cloud, VMs or containers—continues to increase and shows few signs of slowing down. These modern architectures are designed to be operationally efficient and have largely outpaced the evolution of perimeter-based security architectures. Lateral movement is extremely difficult to detect. Some organizations take a calculated risk by allowing encrypted communications to flow across their hybrid cloud infrastructure; others try to augment the virtual architecture by deploying additional firewalls, giving up desirable efficiency for security. And when a majority of enterprises have multiple virtual platforms, the challenges and risks multiply.

2. Dev Teams Running Fast

83 percent of organizations have adopted collective accountability between IT and Security teams[2]

Software development teams are principally incentivized to develop applications, contributing towards revenue growth or saving the organization time and money. As they are continually rushed to meet deadlines, DevOps teams focus on the core function. They may care about security to some degree but are not typically experts on intrusion prevention and are simply unaware of vulnerabilities that may be introduced. Moreover, they may be resistant to deploying security agents in their software and systems, as agents can impede testing and add work and time to the software development lifecycle.

Security organizations approach this problem in different ways. Some go through rigorous exercises for compliance and force agents into all code, others embed security people into the dev teams, and others have no choice but to allow developers to run fast without rigorous security oversight. The vast majority, however, place at least some level of security accountability onto the dev teams.

3. Concealed Threat Activity

91 percent of threats use encrypted channels[3]

Encrypted communications are great for preventing some threats, but they also enable others. It's common practice for threat actors, upon gaining access to any system, to delete, disable, and/or modify the logs as their first order of business. Then come the callouts to a command-and-control server, privilege escalations, lateral movement, secretive copying of data, and ultimately the exfiltration of data—all using encrypted communications.

Security tools can be 5–7x less effective for encrypted traffic[4]

Common encryption methods can be divided into two categories:

- **Modern encryption,** which uses Perfect Forward Secrecy (PFS) to prevent any break-and-inspect decryption on intercepted communications, because any intercepted encryption keys are ephemeral and are worthless for out-of-band decryption. Modern encryption includes TLS 1.3, mTLS, and some deployments of TLS 1.2 that have PFS optionally enabled. Gigamon estimates that roughly 30–40 percent of network traffic today uses modern encryption, and this will continue to grow.

- **Legacy encryption,** which does not use PFS and can be decrypted with an intercepted key. This includes some deployments of TLS 1.2 and older versions of TLS and SSL (Secure Sockets Layer).

Security tools exist that can monitor networks with encrypted communications. For legacy encryption, they typically try to decrypt this traffic themselves. This is a computationally expensive proposition and a significant impact on performance, requiring a lot more “boxes” to address the processing requirements Moreover, the underlying key libraries must be continually updated, and key management is also time consuming and complex. But even with all of this, it still only addresses legacy encryption, while ignoring modern encryption.

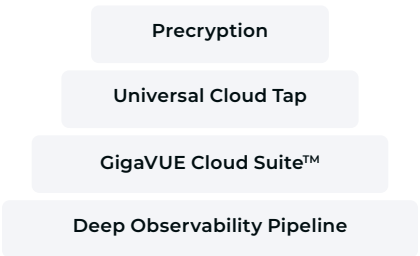
For modern encryption, these tools must take a different approach, since communications cannot be decrypted “in the middle”. Therefore, they feed packet headers, packet size, packet frequency, and other signatures into machine learning algorithms to assess the risk of any given communication. While this is better than nothing, results have been mixed at best, prompting some organizations to either monitor only legacy encryption, place their trust in perimeter security, or ban modern encryption from their applications, none of which are ideal security postures.

In a recent survey of over 1,000 IT and security leaders, it was admitted that 31 percent of data breaches went undetected by their security and observability tools.

Better solutions are needed.

Precryption Solution: A Closer Look

The GigaVUE Universal Cloud Tap (UCT), now with Precryption technology, eliminates encrypted virtual and container communications blind spots, enabling IT and security leaders to regain control.



GigaVUE UCT is a modern virtual tap that leverages native Linux eBPF technology, designed to be the most efficient method to mirror communications in a virtual environment. UCT acquires the unencrypted data, and efficiently delivers it to the Gigamon Deep Observability Pipeline, where further optimization, transformation, filtering, and brokering occurs, ultimately delivering the right data to the right tools, whether physical or virtual.

Gigamon Precryption technology is built on GigaVUE UCT and integrates seamlessly with Linux and encryption libraries such as OpenSSL, acquiring virtual and container communications prior to encryption across the network, or for some applications, after it’s been decrypted across the network.

- ✓ Network communications are untouched, preserved, and remain encrypted across the network.
- ✓ There are no expensive decryption computations. As such, Precryption technology works with modern and legacy encryption and is not impacted by cipher type, strength, or version.
- ✓ There are no application keys exposed, no hassles of application key management, and no unnatural virtual routes required.
- ✓ Precryption technology runs independently of the application being monitored, thus eliminating any impact on the application’s resources and lifecycle management and won’t cause faults within the application.

How Gigamon Precryption Technology Works: Single Node (Figure 1)

1. When any app needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.

2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it's encrypted on the network.

3. The encrypted message is sent to the receiving app, with unmodified encryption. No proxy, no re-encryption, no retransmissions.

4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to GigaVUE V Series in the deep observability pipeline. Gigamon further optimizes, transforms, and delivers the data to tools, without need for further decryption.

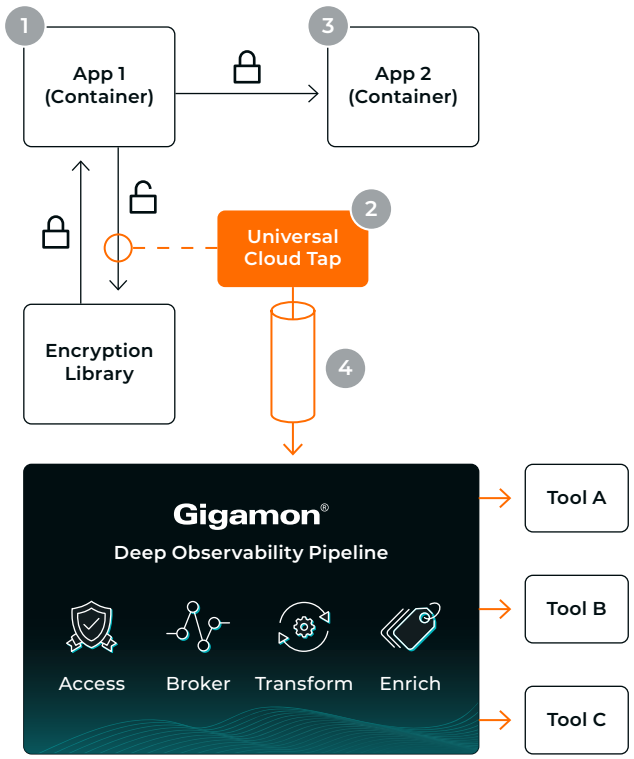


Figure 1

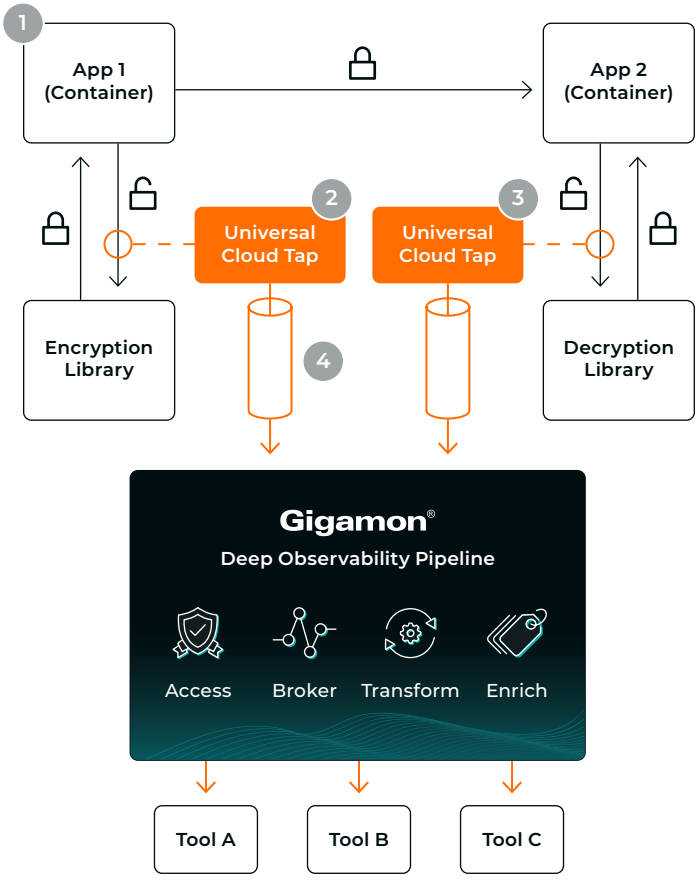


Figure 2

How Gigamon Precryption Technology Works: Multi-Node (Figure 2)

1. When any app needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.

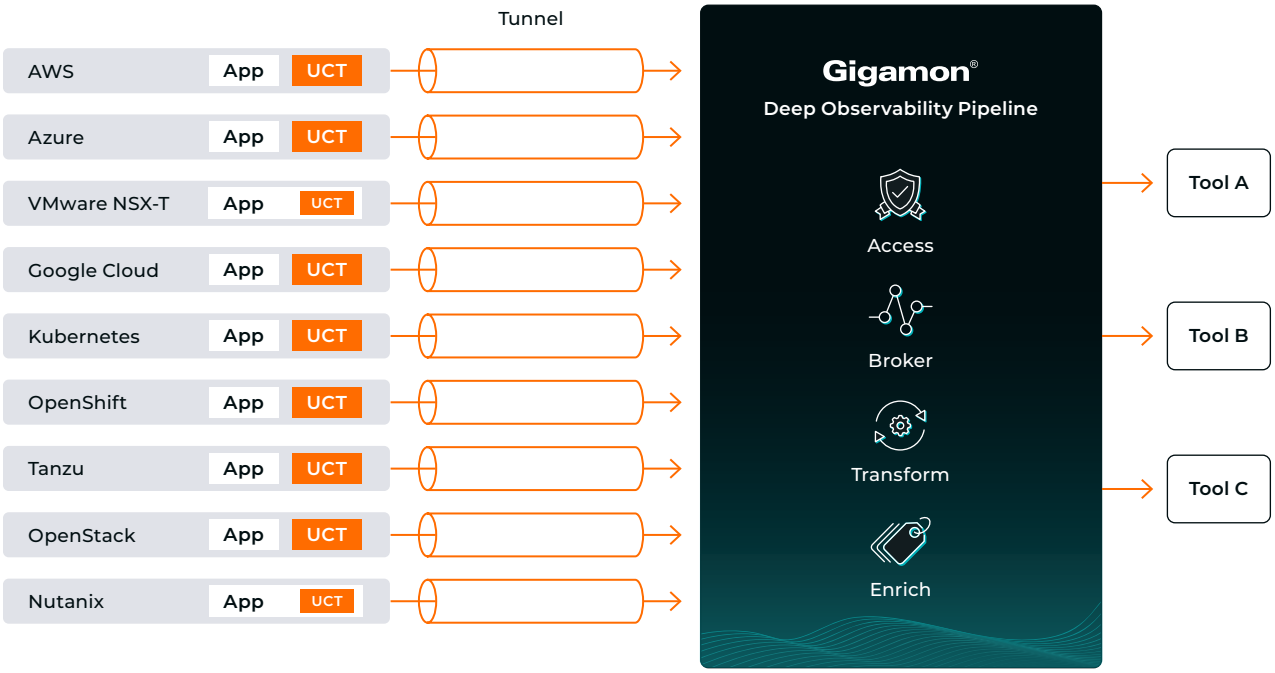
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption, gets a copy of this message before it's encrypted on the network.

3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end, after the decryption.

4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without the need for further decryption.

Works for Multi-Cloud and Large Scale Environments

- ✓ GigaVUE UCT with Precryption technology works across multiple virtual and cloud platforms, including VMware, AWS, Microsoft Azure, OpenStack, Google Cloud, Nutanix, and more, feeding into a common data pipeline, with a single global management interface.
- ✓ Automatic deployment in Kubernetes supported for ease of scalability
- ✓ One shared license pool across all cloud environments; unlimited instances



GigaVUE UCT Runs Independently of the Application

The term “agent” can have different meanings depending on the context. Consider the following table to understand the advantages of UCT versus typical agents.

Typical Agents	GigaVUE UCT
X Runs inside application space/pod	✓ Independent user space in an independent pod
X Impacts application resource usage	✓ Independent node resources
X Requires coordinated version upgrades	✓ Independent upgrades
X Requires testing along with app	✓ Independent lifecycle management
X Can introduce app latency	✓ Independent capture
X Can introduce instability or fail closed	✓ Independent fault domain

Add Network-Derived Intelligence to Improve Security Posture While Developers Run Fast

Once the unencrypted data is extracted, the Gigamon Deep Observability Pipeline can be further leveraged to transform the raw communication data into flow-level metadata records to reduce false positives, help identify nefarious activity like port spoofing, and accelerate threat detection through proactive, real-time monitoring versus reactive forensics. This network-derived intelligence is not subject to log modification, works for IoT and other agentless devices, and feeds into observability tools used by both SecOps and DevOps teams.

For highly sensitive environments, UCT can also optionally re-encrypt mirrored communications destined for the deep observability pipeline, as well as mask sensitive data like credit cards or personally identifiable information (PII) before forwarding to the tools.

Use Case

Detect Cybercrimes Using Precryption Technology

A cybercrime attack, also known as a ransomware attack, typically starts with a threat actor gaining access to an employee's laptop off network, through phishing or some other credential harvesting technique. One would hope that endpoint security would detect or prevent this, but unfortunately, that doesn't always happen.

Once inside the network, a threat actor has many resources available to them, including sophisticated techniques to delete logs, elevate their privileges, and seek out other, more interesting network resources, such as hosts, applications, workloads, etc. with more sensitive data. Given enough time and attack vectors, they will be able to infiltrate these other network resources. This technique is known as lateral movement.

Eventually, the threat actor will make their way into more interesting applications, where data is exposed and communications are spied upon. The threat actor will slowly siphon data off to a drop location within the network, that they control. This siphoning is done in a careful manner so as to not impact performance or trigger alarms. When the actor has enough data and is ready, they implement a final fast-and-large data exfiltration event, to export the stolen data externally, and then extort the organization for money.

In this narrative, there were four major types of activities performed by the threat actor:

1. Initial phish or credential harvesting to bypass endpoint security
2. Lateral movement within the network
3. Slow siphoning of sensitive data to a drop location
4. Fast data exfiltration event

Here is a look at how plaintext visibility using Gigamon Precryption technology helps tools detect this activity:

	What a Security Tool Might See without Precryption	What a Security Tool Can See with Precryption
Initial Phish	Regular employee activity	Regular employee activity
Lateral Movement	Benign noise	Known attack was deployed and successfully infiltrated the server
Data Siphoning	Benign noise	VIP data is being accessed and transmitted on unauthorized channels
Data Exfiltration	Large data transfer	Detailed accounting of what was stolen

For a more detailed walkthrough of the cybercrime scenario, download the infographic.

Conclusion

Gaining visibility into encrypted traffic and metadata dramatically improves hybrid cloud security, monitoring, and troubleshooting. The Gigamon Deep Observability Pipeline directly addresses modern security challenges for monitoring virtual and container traffic, both on-prem and in public cloud. GigaVUE UCT addresses the growing adoption of cloud through robust platform support and a single management interface. Gigamon network-derived intelligence feeds quality metadata to security tools for DevOps, CloudOps, and SecOps teams alike. And Gigamon Precryption technology now addresses the particularly thorny problem of how to monitor concealed activity in the cloud using modern encryption and does so in an elegant and lightweight fashion designed to improve security posture and keep the bad guys out.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

1. Shelley Boose. 81% of Companies Have Had a Cloud Security Incident in the Last Year. Venafi, September 28, 2022. https://venafi.com/blog/81-companies-have-had-had-cloud-security-incident-last-year-venafi-research.
2. 2023 Hybrid Cloud Security Survey: Perception vs. Reality. Gigamon, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon-survey-hybrid-cloud-security-2023.pdf.
3. Internet Security Report – Q2 2021. Watchguard, 2021. https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021.
4. Deepen Desai. Encrypted Attacks Rise 314%: New ThreatLabz State of Encrypted Attacks Report. Zscaler, October 28, 2021. https://www.zscaler.com/blogs/security-research/encrypted-attacks-rise-314.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

09.23_01