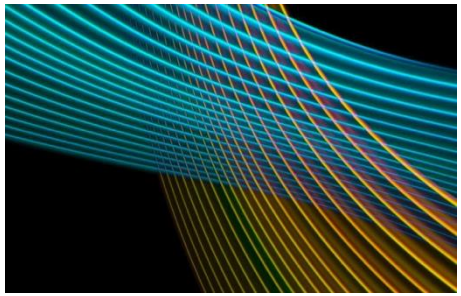
Zero Trust and Verify: Master Security and Availability with Hybrid Cloud Visibility

An Intellyx Analyst Guide for Gigamon

By Jason Bloomberg, Jason English and Eric Newcomer

Table of Contents

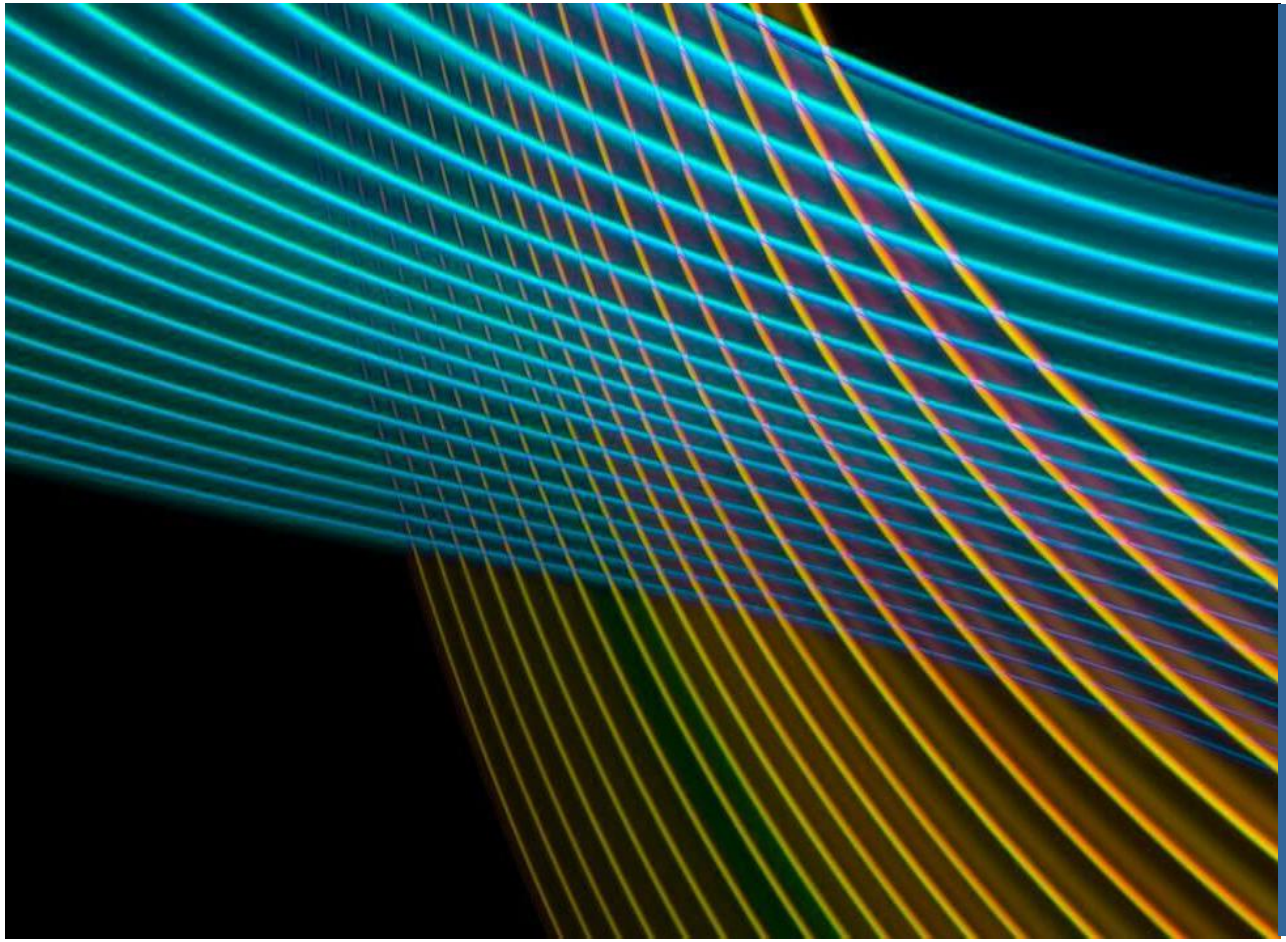


Introduction

Finding security and performance anomalies in a hybrid cloud application stack that combines data from cloud and on-prem services and servers is really hard. Metrics can be deceiving, and logs can lead you astray, depending on how you sample them—and there's always the network engineer's maxim of "packets don't lie."

Unfortunately, these disparate sources of data present a bigger problem for SecOps engineers and threat hunters: how to get visibility across a distributed zero-trust application environment and take action on the right signals.

This 4-part Intellyx Analyst Guide will help readers understand how interoperability and application-level network context can enable zero-trust security policies and forward-looking observability.



By Jason Bloomberg

Managing Partner & Analyst
Intellyx

Be Sure to Whack Your Cybersecurity Blind Spots

Part 1 of the Zero Trust and Verify Series

Managing risk is a top priority for every business executive — and given the prevalence of successful cyberattacks, cybersecurity risk is at the top of the list of challenges facing every organization.

Managing cybersecurity risk is like playing a never-ending game of Whack-a-Mole — except the number of moles seems to be infinite, while your hammers are expensive and in limited supply.

Worst of all, many of the moles are *smart*.

Pounding away at where you expect the critters to pop up isn't good enough. You must also recognize and target your blind spots.

After all, the blind spots are precisely where attackers — the moles — are looking to penetrate your network.

Identifying the Blind Spots

The starting point for any cybersecurity effort targets where you expect the attackers to strike — the holes in the Whack-a-Mole game board, so to speak.

These targets are *endpoints* — the computers, devices, and other equipment that can host endpoint detection and response (EDR) agents. By leveraging these agents, your EDR technology can whack the attackers whenever they attempt to breach an endpoint.

EDR, however, has plenty of obvious blind spots. The most obvious: any endpoint that can't run an agent, either because the technology doesn't support it or for some other reason, like a regulatory compliance restriction.

Other blind spots aren't as obvious. The agents themselves, for example, can also present many blind spots, since bad actors can compromise or disable the agents.

Software drivers also have blind spots. When users inadvertently install their own vulnerable drivers on their devices, EDR solutions are woefully unprepared to deal with the resulting vulnerabilities.

Enter *extended detection and response* (XDR). XDR goes beyond agents, collecting logs and other security telemetry from endpoints, cloud workloads, email, and other sources. It's basically an evolution of the EDR market. XDR then uses artificial intelligence (AI — machine learning in particular) to parse and correlate ingested data to automatically detect threats.

XDR works similarly to security information and event management (SIEM) platforms that also collect and correlate log data to generate alerts and identify potential security issues.

XDR can do everything EDR can do and more: It can extend EDR protection beyond endpoints to cloud workloads, servers, email, and containers.

And then there's *network threat detection and response* (NDR). NDR offers a centralized and automated system for analyzing and responding to security incidents, providing protection against both known and unknown threats that may traverse the network.

Implementing NDR enhances your visibility into network blind spots and ability to effectively identify any suspicious entities or activities within your network.

Are XDR or NDR the solutions to your Whack-a-Mole problem? Not so fast.

Whacking the Remaining Moles

Since most enterprises run SIEM, NDR, and XDR in combination, you might think that they have all their blind spots covered.

That's just what bad actors want you to think.

In reality, there are still several points of vulnerability in those obscure corners of your network where agents don't fit and nothing generates a useful log file.

Examples of these remaining blind spots include corporate printers and copiers as well as various legacy technologies. Many of these devices have been in place for years and communicate via insecure protocols on the network.

East-West traffic — traffic communicating laterally within a network also — qualifies as a blind spot, since many malware-based attacks require lateral movement within the corporate network.

Encrypted traffic, ironically, also presents a significant blind spot. Encryption, after all, hides the contents of messages. If those contents include malware or other malicious data, then the mole you need to whack is invisible.

Perhaps the greatest source of blind spots for many organizations is hybrid clouds that are some combination of cloud-based and on-premises technology. Few cybersecurity tools focus on hybrid cloud challenges.

As a result, there is a lack of comprehensive visibility across hybrid and multi-cloud environments — and the moles keep popping up.

Beating the Moles at their Own Game with Deep Observability

Agent-based and log-based cybersecurity tools are necessary, but they aren't sufficient. They simply leave too many blind spots for bad actors to compromise.

The missing piece: Solutions like the Gigamon Deep Observability Pipeline that provide packet-level intelligence on the network. Combining network-derived intelligence with agent and log-based tools gives organizations *deep observability*.

Organizations can use this deep observability to uncover threats that would otherwise fall into existing cybersecurity blind spots, even across hybrid and multi-cloud infrastructure, from the network to the applications.

Deep observability, in fact, is a foundational requirement for any Zero Trust architecture, because it exposes all the blind spots. Zero Trust assumes any information on the network is potentially malicious — a core part of the NIST SP 800-207 definition of Zero Trust.

Without deep observability, there's no way for cybersecurity infrastructure to rigorously separate benign traffic from malicious.

The Intellyx Take

Try as we might to whack all the moles, there will always be the possibility that one will slip through. Perfect cybersecurity is impossible.

As a result, organizations must also focus on *defense in depth* — combining EDR (agents), SIEM (logs and other telemetry), as well as packet-level visibility to achieve the deep observability necessary to ensure that the security team is able to detect and mitigate any threats that find their way past their cyber-hammers.

Defense in depth combines comprehensive security protections with the observability necessary to detect and mitigate any compromise. It derives implicit trust from an organization's cybersecurity controls.

XDR, NDR, and SIEM, either separately or together, aren't good enough. By combining them without high fidelity, network-level visibility, you've actually reduced your ability to correlate relevant data. Not only will you leave some moles unwhacked, but you might not even see the ones that slip through.

Combining network insights with log-based tools to detect previously unseen threats to provide deep observability solves this problem and is core to Gigamon's value proposition — what it calls its "better together" story.

With deep observability, you'll be able to spot those pesky critters as soon as they poke their head above the board.

By Eric Newcomer

CTO & Principal Analyst
Intellyx

Avoid Dead Reckoning: Why Zero Trust Requires Network Visibility

Part 2 of the Zero Trust and Verify Series

Introduction: Closing the Information Gap

Dead reckoning is how 18th-century sailing ship captains estimated their longitudinal position in the open ocean.

Dead reckoning relies on speed and time calculations from a known point, but it is subject to approximation errors and can be off by dozens or even hundreds of miles.

Similarly, the Zero Trust journey requires complete and accurate information about where you are starting from and exactly how you will get there. Approximation won't cut it.

The Gigamon Deep Observability Pipeline gives you the packet-level data you need to be sure you can trust your network. Without that level of detail, you are just approximating your position in the Zero Trust journey.

What Is Zero Trust?

Zero Trust is a concept, not a technology. Its basic tenet is not to trust anything in your environment that could lead to a breach or incident. Technology is essential to achieving Zero Trust, but technology by itself cannot tell you whether you have achieved it, let alone whether you can maintain it.

Achieving Zero Trust is a process relying on frameworks and methodology. No single solution is right for everyone. You must go through the steps and pay sufficient attention to Zero Trust to be confident that you have achieved the goal.

Frameworks such as those published by NIST, CISA, SABSA, and OWASP help by giving you lists of things to evaluate and the context within which to understand whether you have adequately identified and addressed your risks and vulnerabilities.

Zero Trust means evaluating and remediating risks at every layer of the stack, every network communication point, every application/integration point along the way, every access to the database, and back again.

The Challenge Is Bigger Because of the Internet

Cyber threats have expanded from targeting and harming computers, networks, and smartphones — to people, cars, railways, planes, power grids, and anything with a network connection.

Data is the building block of the digitized economy, and the opportunities for innovation and malice around it are incalculable.

Estimates have half the world's data in public clouds by now, and with generative AI, the need for data and processing will continue to grow unabated and with no end in sight. While the world focuses on the benefits of these technological advances, cybercriminals focus on exploiting the new attack surfaces.

It's an arms race — *the criminals are investing heavily in the latest technology and building tremendously powerful data centers, intent on infiltrating organizations for financial gain.*

The moment you let your guard down is the moment you leave yourself open to attack. And the network serves as the gateway for attacks.

Visibility into the Network Is Essential

Visibility into data in motion is a critical aspect of understanding the current state of the network.

When an endpoint or application workload is compromised, telemetry data generated at that level cannot always be trusted.

Network visibility at the packet level provides the reliable telemetry needed to detect any such compromise.

Zero Trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

But you must be able to observe all network traffic accessing those resources and filter out metadata about the connection from the data being transported. Monitoring tools should also be able to detect anomalies in the data being transported.

The Solution

The Gigamon Deep Observability Pipeline efficiently collects packet-level and network-derived intelligence from anywhere in the network and delivers it to any combination of security and network management tools, making them more effective at detecting threat activity.

Gigamon provides the actionable network-derived intelligence and insights you need to eliminate security and performance blind spots across hybrid cloud infrastructure and achieve new levels of efficiency.

The Gigamon Deep Observability Pipeline supports all popular environments, efficiently delivering network-derived intelligence to any combination of monitoring tools, such as:

- Network traffic analyzers: Palo Alto, Fortinet, Cisco, Nokia, Ericsson
- Application monitoring and SIEM tools: Armis, IBM, LogRhythm, LiveAction, Splunk
- Network intelligence and observability tools: Datadog, Elastic, Sumo Logic, Dynatrace, New Relic

Gigamon enriches raw packet data and sends the right data to the right tool, extending its value. Gigamon performs deep packet inspection to determine where the data is coming from and where it's going, and transforms it into the optimal format for each tool.

Different tools want to see different data. For example, some want to see the full network packet, some just the application metadata, while others combine network and application-level data.

The requirement for the Gigamon Deep Observability Pipeline is based on several factors:

- Multiple agents for multiple tools can be eliminated using the Gigamon Universal Cloud Tap
- Avoiding duplication of tools — some work with different stacks, and multiple tools compound resource and skills issues
- Existing tools don't talk to each other, making it difficult to have a common view of the network
- Gigamon can pull together all the information required to detect issues to tell you not only when an application is not performing well, but also tell you why

Gigamon also offers a range of GigaSMART® applications that can remove duplicate packets, set filtering criteria (for high-priority packets, for example), or just look at the header and not store an entire media stream.

Gigamon adds the required network-derived intelligence to application observability tools that lack visibility into what's happening at the network level.

The Intellyx Take

The transition from perimeter security in an implicit trust model to a complete Zero Trust environment can be a difficult and time-consuming journey. It involves ensuring the right monitoring tools are in place to get the data you need to detect and prevent incidents, outages, and breaches.

Network-level observability is foundational to Zero Trust. With so many more applications moving to the cloud — and accessed via the public internet — and so many more devices connected to the network, it's critical to any Zero Trust posture to understand what is going on at the network level.

The Gigamon Deep Observability Pipeline confronts this problem thoroughly and comprehensively — working with any network device and virtually any monitoring tool, and providing a consolidated view of all network traffic across any modern hybrid cloud infrastructure.

If the network isn't safe, you don't have Zero Trust. And if you don't have Zero Trust, there's a non-zero chance you will get hacked.

After all, knowing where you are is the first step toward getting where you want to go. The Gigamon Deep Observability Pipeline gives you the knowledge you need to start and complete your journey safely to Zero Trust.

By Jason English

Partner & Principal Analyst
Intellyx

Precryption: The Zero Trust Prescription for Decryption

Part 3 of the Zero Trust and Verify Series

Data ingestion and normalization

By now, we're all waking up to the reality that ransomware and other malicious cyberattacks aren't going away anytime soon. Threat actors are cashing in on a lucrative environment for exploits with few negative consequences.

Companies are moving critical business applications — once contained in on-premises walled gardens — into increasingly service-oriented and cloud-based hybrid IT environments. This is only natural as development teams want to be more agile in delivering software, scaling their environments, and expanding network topologies to meet changing business requirements and customer needs.

Unfortunately, this new norm of a distributed expanse of nodes and connections has opened up new network threat vectors, and the hacker world has devised new attacks and payloads that seem invisible to detection until they cause damage, even with Zero Trust security policies in place.

How can we realize the benefits of encryption, while getting ahead of the risk it can become in the hands of attackers?

Chasing Encryption in the Cloud

There are a few natural advantages of a modern cloud stack for cyber defense.

Major hyperscalers maintain perimeter security for North-South traffic coming into cloud instances and firewalls against incoming DDoS attacks — though AWS makes it clear in their shared responsibility model that *"while AWS manages security **of** the cloud, you are responsible for security **in** the cloud."*

Further, the elastic property of cloud infrastructure allows developers to call for microservices workloads that are launched into ephemeral clusters and containers that are released when no longer needed, often before attackers can detect them.

Still, having so many moving, changing systems and services loosely tied together within a hybrid IT application environment also exposes a complex and broad network threat surface with many potential handholds for attackers.

To obfuscate sensitive data from attacks, especially for East-West traffic that moves laterally within the organization's extended network, messages are routed through readily available open-source encryption libraries like OpenSSL, making it much harder for an outsider to break into a secured channel and decrypt that data into any useful or recognizable form.

Strong encryption was a game changer for cyber defense. At the same time, cyber attackers also have ready access to modern encryption tools to cloak their actions. By encrypting their own traffic and lateral movement through the network, they can often lurk undetected by threat hunters with security tools.

In fact, 31 percent of data breaches went undetected by security and observability tools, some of which may be attributed to this blind spot for encrypted traffic, according to a recent study by Gigamon.

Why Decryption Won't Mitigate Risk

Encryption has come a long way since good old PGP in our mail clients.

Perfect Forward Secrecy (PFS) is a feature within TLS 1.3 that makes it impossible to use out-of-band decryption. Even if the current session key is compromised, it cannot be used to reveal secrets within older sessions and past transactions.

Since each session creates a new key, hackers can't sniff the wire to collect keys — and even if they did somehow manage to decrypt one ephemeral key with supercomputing power, that key would be rendered useless for other sessions. PFS stymies the old man-in-the-middle (MITM) attack style that was popular a decade or more ago.

However, PFS also provides a private environment for bad actors to hide their movements within a network once they have stolen credentials. Longer-running attacks such as malware can be later reactivated, and remote commands effectively concealed from threat detection within that secure encrypted channel.

So, would decryption help?

Well, the odds of winning the lottery are better than a human or computer simply guessing a strong cipher, even if millions of tries are allowed.

This leaves operators trying to break into the encrypted channel of their own nodes and the network to collect and decrypt messages that look like keys and payloads that attackers might be using, which is an arduous task with mixed results for determining if encrypted traffic is benign or malicious.

Besides the relative difficulty and consumption of valuable compute resources of this form of monitoring, breaking and inspecting active messages would likely interfere with the performance and availability of local and network resources.

Traditional forms of threat hunting use inline proxies for decryption, which might be useful for North-South traffic coming into your data center or network from the internet, but they are unacceptably intrusive for East-West traffic.

Setting up a proxy that slows down customer traffic to avoid an unknown risk? That's not a compromise for which the business can settle.

Precryption Starts Earlier

There's a new approach that can stop encryption from helping attackers hide their own actions. What if you could know exactly what encrypted traffic is suspicious, ***before it is encrypted?***

Gigamon has done exactly this with a new breakthrough technology called ***Precryption™***.

Precryption provides a much simpler way to front-run any kind of encryption and eliminate blind spots by seeing concealed threat activity and anomalous data in the cloud, VMs, and containers, before it hits an encryption library and moves on to the network.

Gigamon Precryption technology operates through the new GigaVUE® Universal Cloud Tap (UCT), which utilizes plaintext to transform, analyze, and route encrypted cloud traffic for deep network observability and SecOps threat hunting, with message and packet visibility down to the Linux kernel level.

The rightful admin of a given Linux system or container image can use Gigamon Precryption technology to get a plaintext view of cloud traffic before it's encrypted, using eBPF networking privileges within the Linux system to understand communications between applications and the network tap.

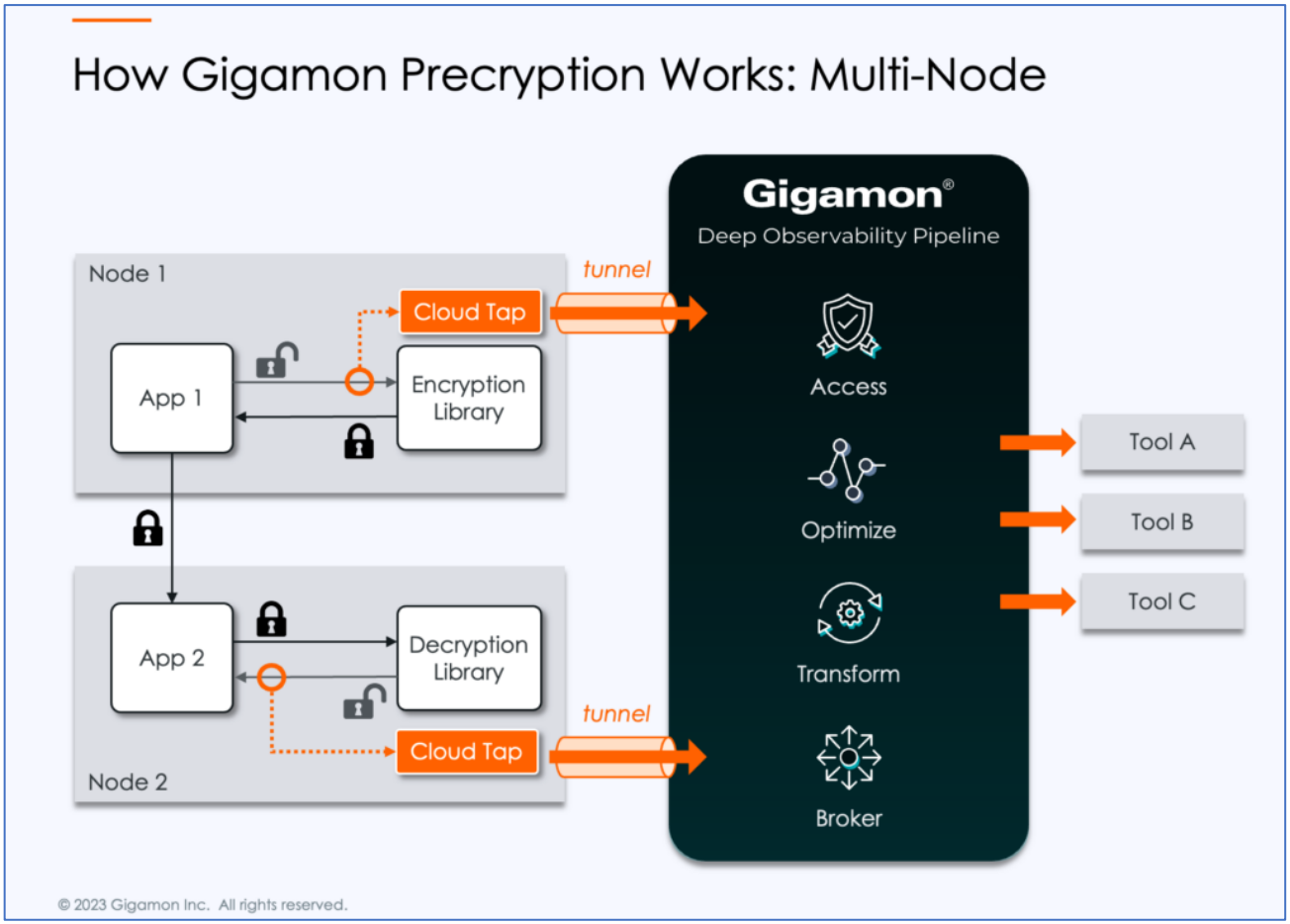


Figure 1. Gigamon Precryption used in a multi-node environment. *UCT, enabled with Precryption, gets a copy of a message before it hits the encryption library and goes on the network. The message can then be encapsulated in a tunnel and sent for processing for further analysis. Additionally, UCT with Precryption can grab and analyze a copy of the return message from the server end after decryption.*

In a multi-node scenario, Precryption technology can also be applied ***after*** decryption. Messages and responses coming back out of the network into the local system's decryption library channel can also be viewed and analyzed for threats without interference.

The Intellyx Take

Before Precryption came on the scene, there were many other ways to intercept and prevent dangerous messages. These options mostly centered on preventing outside intrusion and then getting into the middle of a transaction to find whatever suspicious activity made it through via decryption.

Standard decryption methods were never designed to meet the needs of distributed application environments, where network traffic involves application components and microservices sharing secrets with each other, rather than responding to external requests.

Visibility into encrypted traffic is a foundational building block of true Zero Trust practices. It would be safer to assume our perimeter security is already compromised and act accordingly. Once an intruder has gained access to some part of your network, they can use encryption to their advantage.

It's time to turn over a new leaf on encryption and decryption with Gigamon Precryption technology.

By Jason Bloomberg

Managing Partner & Analyst
Intellyx

How to Harness East-West Visibility for a Stronger Defensive Security Strategy

Part 4 of the Zero Trust and Verify Series

The days when a firewall-based perimeter was sufficient for a reliable security posture are long gone. Today, every endpoint, every user, every system is suspect. Compromises are taken for granted, and Zero Trust is becoming a way of life.

Given the need to reduce every organization's attack surface, encryption has become the go-to technology of choice for securing all kinds of network traffic. From web sites with secure HTTP to internal communications between corporate applications, encryption has become ubiquitous.

Encryption, however, is not sufficient – even for traffic within an organization, including what we call East-West or lateral traffic. Understanding the shortcomings of encryption, as well as how to mitigate them, is essential for strengthening your security posture in today's Zero Trust world.

East-West vs. North-South

The Wikipedia definition of East-West is traffic within a data center, while North-South traffic connects data centers. However, this definition does not reflect the subtleties of today's complex, hybrid cloud environments.

With virtual networks, the cloud, and now cloud-native computing, the definitions of East-West and North-South have climbed the ladder of abstraction.

Today, East-West refers to laterally moving traffic between endpoints within an abstracted network segment – perhaps a virtual private cloud, or in the cloud native context, between microservice endpoints in the same Kubernetes environment.

North-South traffic, in turn, often traverses APIs – either between organizations or among different clouds, domains, or network segments within an organization.

You need to secure all traffic regardless of the points on the compass, but East-West and North-South traffic present different challenges that bring importance to the distinction.

Perimeter-based security (firewalls, API gateways, and the like) have always secured North-South traffic. The challenge today is bringing Zero Trust to bear for East-West traffic.

Zero Trust may be simple in principle – *everything is untrusted until it is explicitly authorized to take a particular action—but the devil is in the details.*

Network microsegmentation can provide a measure of Zero Trust across distributed networks. This approach is a strategy for containing network issues and providing situationally targeted security monitoring for an improved security posture.

However, it is insufficiently flexible to handle East-West interactions in some situations, for example among ephemeral microservice endpoints. This leaves organizations with a lack of context as to what is occurring between each of the segments and where to focus their efforts when troubleshooting must occur.

What Zero Trust means in practice, therefore, can vary depending on the context of particular interactions. The result is increased complexity, and with it, expanded opportunities for bad actors to find and exploit points of compromise.

Encryption to the Rescue?

Given this complexity of East-West traffic at different levels of abstraction, it's not surprising that encryption alone doesn't address today's cybersecurity challenges.

Encryption is point-to-point by definition. It doesn't consider network complexity that underlies today's East-West traffic. In reality, communications may traverse many endpoints to get from point A to point B – many of which are hidden from view under layers of abstraction.

Those layers may obscure complexity, but they don't slow down attackers. In fact, every intermediate point on a message's journey gives adversaries an opportunity to mount a break and inspect (aka man-in-the-middle) attack.

Another primary encryption shortcoming is more subtle, but even riskier: the fact that encryption is a blunt tool that hides both bona fide corporate data as well as any malicious data bad actors wish to put in a message.

As Intellyx's Jason English explained in his previous article, hiding malicious data in encrypted communications on the network is a common MO, as East-West communications are essential for lateral movement and data exfiltration – fundamental elements of the MITRE ATT&CK Framework.

The Missing Piece of the Puzzle: Visibility into Encrypted Traffic

Encrypted communications from point A to point B might contain sensitive corporate data, while the next message contains malware looking for a juicy target. But since both messages are encrypted, how do you tell good from bad?

The simplest answer, of course, is to decrypt and analyze them, but once you decrypt them, they are vulnerable to further attack. This approach also slows messages down, introducing unacceptable latency.

Gigamon has cracked this problem by offering an alternative: Gigamon Precryption™ technology . Precryption technology provides a simpler way (by capturing plaintext traffic) to front-run any kind of encryption and eliminate blind spots by seeing concealed threat activity and anomalous data in the cloud, VMs, and containers, before it hits an encryption library and moves on to the network.

Precryption makes copies of messages that the Gigamon Deep Observability Pipeline moves to a protected environment for inspection. Such inspection can work at different levels of abstraction, all the way down to individual packets.

The Intellyx Take

In cloud native environments, microservice endpoints are ephemeral, and thus East-West traffic connects abstracted endpoints that may not even have fixed IP addresses.

In such environments, establishing visibility into encrypted traffic is especially challenging, and requires the Precryption technology that Gigamon provides. Anything less would give bad actors too many opportunities.

Cloud native, however, isn't the whole story. Virtual networks, virtual private clouds, and network microsegmentation all depend upon encrypted messages flowing east to west across some level of abstracted network.

Cloud native may be the latest generation of such abstraction, but virtually every organization has sufficient network complexity to take advantage of Gigamon Precryption technology to keep adversaries at bay.

About the Analysts

Jason Bloomberg is founder and managing partner of enterprise IT industry analysis firm Intellyx. He is a leading IT industry analyst, author, keynote speaker, and globally recognized expert on multiple disruptive trends in enterprise technology and digital transformation.

Mr. Bloomberg is the author or coauthor of five books, including *Low-Code for Dummies*, published in October 2019.

Jason "JE" English is Partner & Principal Analyst at Intellyx. Drawing on expertise in designing, marketing and selling enterprise software and services, he is focused on covering how agile collaboration between customers, partners and employees accelerates innovation.

With more than 25 years of experience in software dev/test, cloud and supply chain companies, JE led marketing efforts for the development, testing and virtualization software company ITKO from its bootstrap startup days, through a successful acquisition by CA in 2011. Follow him on Twitter at @bluefug.

Eric Newcomer is CTO and Principal Analyst at Intellyx, a technology analysis firm focused on enterprise digital transformation. Eric is a well-known technology writer and industry thought leader, and previously held CTO roles at WSO2 and IONA Technologies.

About Intellyx

Intellyx is the first and only industry analysis, advisory, and training firm focused on customer-driven, technology-empowered digital transformation for the enterprise. Covering every angle of enterprise IT from mainframes to cloud, process automation to artificial intelligence, our broad focus across technologies allows business executives and IT professionals to connect the dots on disruptive trends. Read and learn more at https://intellyx.com or follow them on Twitter at @intellyx.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.