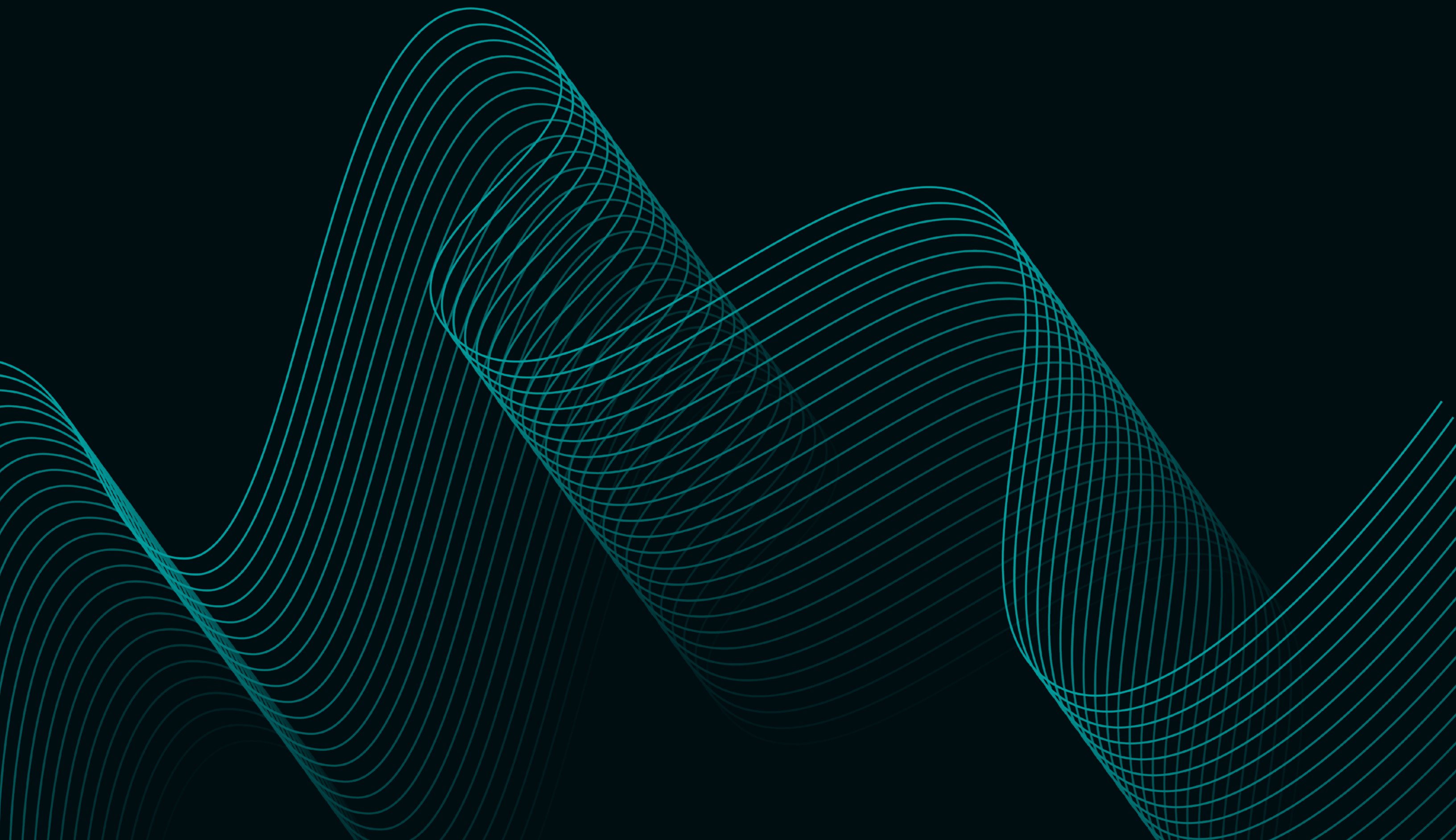
Gigamon®

# Building an Effective Ransomware Solution Through Deep Observability

The Gigamon Deep Observability Pipeline, SSL/TLS Decryption, and Application Metadata Intelligence provide deep observability to combat today’s ransomware threats



## The Challenge

Ransomware attacks are becoming more sophisticated as cyber criminals have shifted their tactics to make campaigns more effective and increase their chances of successfully collecting ransom payments.

280
Days

37%
Global orgs

130
Different strains

Moving on from the opportunistic, mass-distribution ransomware that was so prevalent in the past, cyber criminals are now spending more time in a target's network, researching the target, and escalating privileges to compromise more sensitive data. Once the data is in their hands, they threaten to publish it if the ransom isn't paid. This "double extortion" technique has proven to be much more effective (and lucrative) for the criminals and disruptive to their targets.

## Highlights

**New ransomware targets and motivations emerge:** As of 2019, cyber criminals have shifted their focus to large enterprises and critical infrastructure. While financial motivation is still paramount, a secondary motive is prolonged business disruption.

**Endpoint tools are falling short:** Endpoint detection and response tools don't have visibility into the data-in-motion in your network. Cyber criminals are becoming more adept at disabling endpoint agents and modifying SIEM logs while unprotected IoT, OT and ICS devices present a visibility gap that can be exploited.

**Cyber criminals rely on encrypted communications:** Ransomware actors are hiding their command-and-control communications inside encrypted traffic.

## The Solution

Fortunately, the solution is simple: ensure deep observability into network traffic. The shift in tactics and extended attacker dwell times mean effective security teams need:

1. Comprehensive visibility into North-South, East-West traffic
2. The ability to inspect encrypted traffic
3. Gain application visibility to empower your NDR, SIEM, and other security monitoring tools

Gigamon can collect and inspect all data-in-motion, detect early-stage ransomware threats, and identify potential network security risks quickly.

## How it works

**Deep Observability**
The Gigamon Deep Observability Pipeline gives your organization the ability to access and aggregate data from any network source—managed or not, on-premises or in the cloud—transform and analyze it for visibility into lateral threat activities across your network.

### Inspection

Ransomware attackers are relying on encrypted traffic to hide their malicious communications. The Gigamon SSL/TLS Decryption capability allows operations teams to inspect encrypted traffic and centralize decryption to not over-burden your existing security tools.

### Application Intelligence

Gigamon Application Metadata Intelligence empowers your security information and event management (SIEM) and network performance monitoring tools with critical metadata attributes across thousands of business, consumer and IT applications and services. It provides the deep application visibility needed to rapidly pinpoint performance bottlenecks, quality issues and potential network security risks.

Gigamon helps organizations eliminate cloud and security blind spots while simplifying IT complexity by streamlining data to your NDR, SIEM, and other security tools. This ensures organizations can deliver exceptional customer experiences, maintain their security while preventing the disruption of a ransomware attack.

## For More Information

Get more information about the Gigamon Deep Observability Pipeline

Learn more about SSL/TLS decryption capabilities in Gigamon solutions

Get more information about Gigamon Application Metadata Intelligence

Gigamon®

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