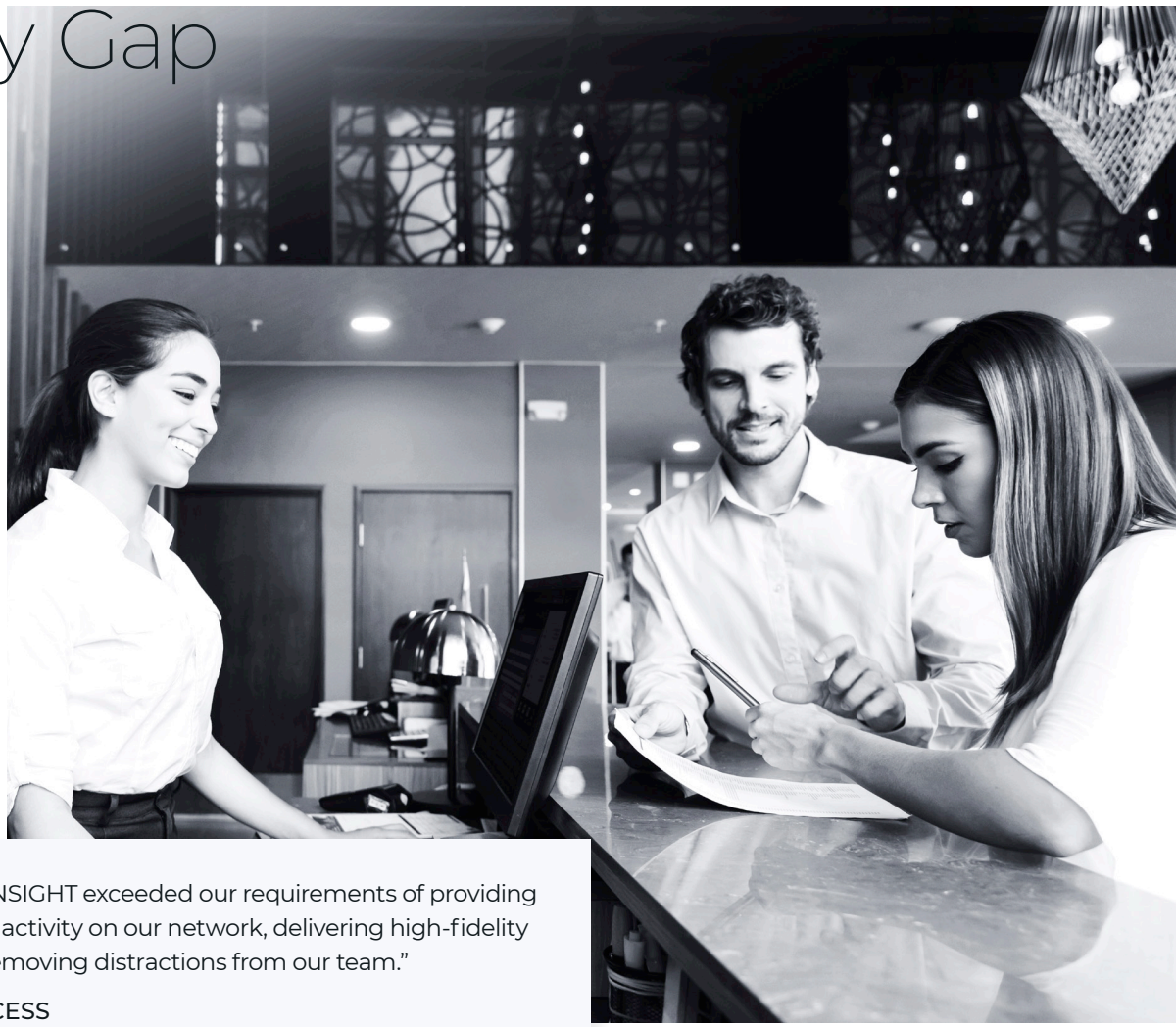
Wyndham: Closing the SOC Visibility Gap



> Gigamon ThreatINSIGHT exceeded our requirements of providing robust visibility to activity on our network, delivering high-fidelity detections, and removing distractions from our team."

MICHAEL FRANCESS
Senior Manager, Cyber Security Advanced Threat and Response
Wyndham Hotels & Resorts

CHALLENGES

+ Distributed properties and workers
+ Safeguard point-of-sale systems, corporate information, and personal identity information (PII) from cyber-attacks
+ Lack complete visibility across all devices on their core and cloud
+ Security tools require extensive training

SOLUTION

+ Gigamon ThreatINSIGHT™
+ GigaVUE-FM
+ Gigamon Cloud Suite in AWS

CUSTOMER BENEFITS

+ Foundational visibility: Combining with Wyndham's EDR to close the SOC visibility gap
+ Minimal distractions: Allows Wyndham's SOC/IR teams to focus on threat management, rather than tool maintenance
+ Powerful threat hunting with Applied Threat Research (ATR)

ABOUT WYNDHAM

Wyndham Hotels & Resorts, Inc is one of the largest hotel chains in the world based in United States, its portfolio consists of 20 hotel brands with over 9,000 locations. Wyndham Hotels & Resorts makes travel possible for all. From big cities and small towns to beachfront resorts and highway hotels, our 22 iconic brands bring a diverse perspective to the travel experience.

BUSINESS CHALLENGE

As one of the largest hotel chains in the world with distributed properties and workers, safeguarding Wyndham's point-of-sale systems, reservations, corporate information, and personal identity information (PII) from data breaches, ransomware, and other cyber-attacks is critical. While Wyndham's strong Endpoint Detection and Response (EDR) solution provides visibility into threat actor behaviors on protected endpoints, gaps remained on devices they couldn't deploy the EDR agent (unsupported devices or unmanaged IoT devices). To close the SOC visibility gap, Wyndham knew they needed to expand their visibility across all devices on their core and cloud network by adding a Network Detection and Response (NDR) solution. Wyndham also had another initiative to significantly reduce distractions to their SOC and IR teams, allowing them to focus on adversaries rather than dealing with security tools that require extensive baseline training, false positive tuning, or on-premises care and maintenance.

RESOLUTION

With a strong frontline (e.g., NGFW, AV, SASE, etc.) security-stack, EDR and SIEM in place, Wyndham turned to Gigamon ThreatINSIGHT Guided-SaaS NDR and GigaVUE Cloud Suite for AWS to provide full L2-L7 network visibility to every device on their core and cloud networks. While examining multiple leading NDR vendors, Wyndham chose ThreatINSIGHT based on the offering's ability to deliver:

+ Cloud-native Architecture
+ Comprehensive Network Visibility
+ Extend security and compliance to AWS deployments
+ Wide-ranging Detection Techniques
+ Advanced Threat Hunting Capabilities
+ Robust Triage and Investigation Tools
+ Guided-SaaS with Expert Support
  - Fast, Simple Deployment
  - Zero Maintenance
  - Ongoing Product Enablement
  - Threat and Response Guidance

BENEFIT

By closing the SOC visibility gap, Wyndham has created a robust deep observability foundation to protect their distributed network of properties and workers.

+ **Foundational visibility:** Combining with Wyndham's EDR to close the SOC visibility gap
+ **Minimal distractions:** Aiding Wyndham's SOC/IR teams to focus on threat management, rather than tool maintenance
+ **Advanced detections:** Identifying threats by blending threat intelligence, behavior analysis, and machine learning
+ **Powerful threat hunting:** Enabling Wyndham's hunters with observations and retained historical network metadata
+ **Guided triage and investigations:** Assisting Wyndham's SOC analysts with published guided-next steps
+ **Unique Guided-SaaS solution:** Providing Wyndham with experienced advice when it matters most

USE CASES

Management & Maintenance

+ **Technical Capabilities:** ThreatINSIGHT provides a cloud-native architecture and SaaS deployment model provide quick and easy deployments.
+ **Customer Benefit:** Wyndham visibility to network activity of any device on their network within minutes. With near-zero ongoing care and feeding, Wyndham SOC/IR teams can focus on adversaries, not tool management.

Visibility

+ **Technical Capabilities:** GigaVUE Cloud Suite for AWS and ThreatINSIGHT provides East-West, North-South and container traffic as well as L2-L7 near-pcap level visibility in the form of recorded rich network metadata
+ **Customer Benefit:** Wyndham's SOC and IR teams can triage, hunt, and investigate active threats and have the context to understand the adversary's behaviors.

Adversary Detection

+ **Technical Capabilities:** ThreatINSIGHT delivers a combination of proprietary threat intelligence, behavioral analysis, and both supervised and unsupervised machine learning techniques to identify and classify attacker behavior.
+ **Customer Benefit:** The wide range of detection techniques provides higher fidelity findings and reduces Wyndham's Mean-Time-To-Detect (MTTD).

Baseline Training and Tuning

+ **Technical Capabilities:** The ThreatINSIGHT detection techniques run in the cloud where Gigamon's ATR team performs continuous QA and detection tuning on all detection techniques to ensure high quality findings.
+ **Customer Benefit:** Wyndham doesn't have distractions posed by other NDRs that require extensive baseline training for a month or ongoing routine false-positive tune-ups.

Threat Hunting

+ **Technical Capabilities:** ThreatINSIGHT delivers ATR-derived 'Observations' (hunting starting points), advanced query capabilities, and enriched metadata that includes detailed information about the entity and event context
+ **Customer Benefit:** Wyndham now has a single platform with all the network context to hunt for the presence of adversaries.

Triage and Investigation

+ **Technical Capabilities:** ThreatINSIGHT offers 'Guided Next-Steps' provides threat specific advice on how to both triage a threat and best practices to perform an investigation.
+ **Customer Benefit:** Wyndham now has a single platform and tools to query and examine retained network metadata to quickly validate findings and begin the response process.

Deployment & Support

+ **Technical Capabilities:** The ThreatINSIGHT Guided-SaaS delivery model includes field-tested Gigamon security analysts or incident responders (TSMs) to assist with deployment, enablement, health checks, and incident advisory guidance.
+ **Customer Benefit:** Facing a potential incident, Wyndham's SOC/IR team can receive threat actor technics, tactics and procedures and best practice guidance on how best to investigate and respond from Gigamon TSMs.

GIGAMON DEEP OBSERVABILITY

While being a Gigamon GigaVUE next generation network packet broker customer is not a requirement to achieve the value ThreatINSIGHT provides, it ensures you are providing the right network traffic to your NDR. For Wyndham, their confidence in Gigamon's network visibility expertise bolstered their assessment that ThreatINSIGHT was the best NDR for them. Wyndham knew they could easily manage the traffic being observed by ThreatINSIGHT, decrypt any encrypted traffic for inspection, and de-duplicate any traffic to ensure optimized ThreatINSIGHT performance.

ABOUT GIGAMON

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables 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 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

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