Zscaler and Gigamon ThreatINSIGHT

Enabling Cloud-based Network Detection and Response for Mobile, Branch and Headquarters.

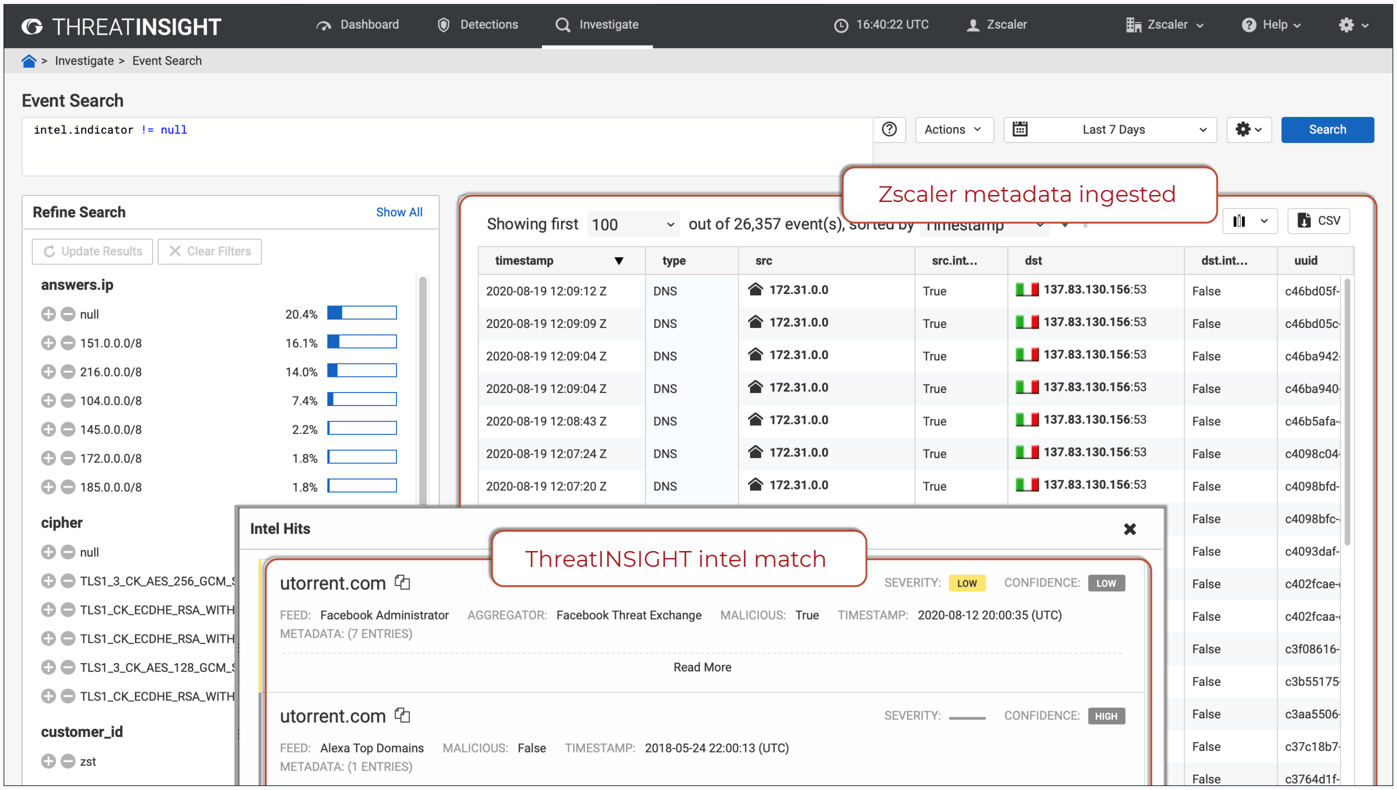
The rapid migration to work from home ushered in by these unprecedented times has resulted in expanded attack surfaces and resources stretched thin. Mobile workers and branch sites are now on the frontlines for attacks. In response, security operations teams need cloud-based SaaS solutions to reduce or eliminate operational tool maintenance while expanding visibility and achieving faster threat detection and response through cloud analytics. Zscaler and Gigamon ThreatINSIGHT™ have partnered to offer security operations teams unparalleled visibility across their organization and rapid network detection and response.

KEY JOINT SOLUTION FEATURES

- One-click integration for ThreatINSIGHT and Zscaler Internet Access customers
- All TCP/IP (including HTTP, DNS and SSL) activity observed by Zscaler is automatically delivered as metadata to ThreatINSIGHT
- Integration enables automated threat detection and investigation with corrective response capabilities an attack, lateral spread, targets and sequence of events — even if those events weren't known at the time of occurrence
- ThreatINSIGHT and Zscaler are delivered as pure cloud-based, SaaS solutions with minimal on-premises footprint

KEY JOINT SOLUTION BENEFITS

- Eliminate blind spots with comprehensive visibility across your attack surface (teleworkers, remote sits, headquarters)
- High-speed, high-fidelity detection of emerging threats
- Rapid investigations to make informed mitigation response actions that stop threats
- Eliminate operational maintenance, enabling response teams to focus on threats and not management of tools



Zscaler metadata ingested

ThreatINSIGHT intel match

Event Search

```
intel.indicator != null
```

Refine Search

answers.ip

null	20.4%
151.0.0.0/8	16.1%
216.0.0.0/8	14.0%
104.0.0.0/8	7.4%
145.0.0.0/8	2.2%
172.0.0.0/8	1.8%
185.0.0.0/8	1.8%

cipher

- null
- TLS1_3_CK_AES_256_GCM_S
- TLS1_CK_ECDHE_RSA_WITH
- TLS1_CK_ECDHE_RSA_WITH
- TLS1_3_CK_AES_128_GCM_S
- TLS1_CK_ECDHE_RSA_WITH

customer_id

- zst

Showing first 100 out of 26,357 event(s), sorted by Timestamp

timestamp ▼	type	src	src.int...	dst	dst.int...	uuid
2020-08-19 12:09:12 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c46bd05f-
2020-08-19 12:09:09 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c46bd05c-
2020-08-19 12:09:04 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c46ba942-
2020-08-19 12:09:04 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c46ba940-
2020-08-19 12:08:43 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c46b5afa-
2020-08-19 12:07:24 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c4098c04-
2020-08-19 12:07:20 Z	DNS	172.31.0.0	True	137.83.130.156:53	False	c4098bfd-
					False	c4098bfc-
					False	c4093daf-
					False	c402fcae-
					False	c402fcaa-
					False	c3f08616-
					False	c3b55175-
					False	c3aa5506-
					False	c37c18b7-
					False	c3764d1f-

Intel Hits

utorrent.com
SEVERITY: LOW CONFIDENCE: LOW
FEED: Facebook Administrator AGGREGATOR: Facebook Threat Exchange MALICIOUS: True TIMESTAMP: 2020-08-12 20:00:35 (UTC)
METADATA: (7 ENTRIES)

utorrent.com
SEVERITY: — CONFIDENCE: HIGH
FEED: Alexa Top Domains MALICIOUS: False TIMESTAMP: 2018-05-24 22:00:13 (UTC)
METADATA: (1 ENTRIES)

Zscaler NSS logs provide visibility into mobile, branch office and headquarter users, enabling ThreatINSIGHT to identify hidden and emerging threats

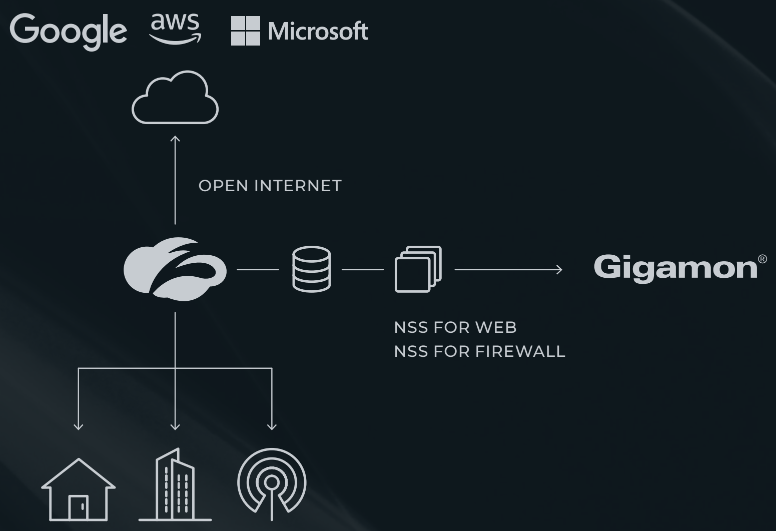
The Challenge

While most organizations rapidly shifted to a work-from-home (WFH) workforce without major issues, the enabling of greater access to more web-based applications, the expansion of unsecured endpoints accessing those applications and expanded cloud infrastructure has resulted in a New Tomorrow with greater attack surfaces and a wider net of vulnerabilities. And that's all to the benefit of threat actors.

Now more than ever, security operations teams need technologies that work together to provide network visibility across this expanded attack surface and fast, high-fidelity detection techniques that leverage cloud-based machine learning and behavioral analytics to identify hidden and emerging threats. And incident responders need the ability to easily hunt, search and investigate network activity to understand the extent of any incident so they can make informed mitigation plans and response actions that eliminate the risk to the organization.

The Solution

Zscaler and Gigamon ThreatINSIGHT, both cloud-based SaaS solutions, have partnered to provide security teams unparalleled visibility across mobile users, branch offices and headquarters. The integration enables Zscaler Internet Access (ZIA) customers to easily deliver ZIA network activity metadata directly to ThreatINSIGHT sensors for ingestion and immediate analysis for the detection and response to hidden and emerging threats.



ELIMINATE BLIND SPOTS

Whether mobile, branch office or headquarter users, Zscaler and ThreatINSIGHT will have visibility into their network activity. Combined technologies offer:

- Always-on security regardless of where your users and devices are
- ThreatINSIGHT provides deep visibility to North-South and East-West traffic and cloud infrastructure workloads, including SSL encrypted traffic
- Zscaler provides visibility to mobile, branch and headquarter users' internet activity

CLOUD-BASED HIGH-FIDELITY DETECTION AND RESPONSE

Cloud-ready platforms that empower security analysts and incident responders. Key benefits include:

- Leading threat intelligence, machine learning and behavioral analysis delivering high-fidelity, accelerated threat detection across entire MITRE ATT&CK framework
- Fast omnisearch, threat hunting and full investigation and incident management workflows to make informed, complete response decisions

ZERO-MAINTENANCE SECURITY

With cloud-first designs from both Zscaler and ThreatINSIGHT, customer enjoy zero-maintenance security. Key benefits include:

- Plug-n-play deployments and integrations: Initiate and complete Zscaler integration within minutes in the ThreatINSIGHT portal
- Security staff can remain focused on threats, not tool management or maintenance
- Cloud-based analytics and storage mean solutions scale to any size customer

Conclusion

Security teams seeking solutions for managing distributed environments benefit from integrated cloud-based SaaS solutions by Zscaler and Gigamon ThreatINSIGHT by achieving comprehensive visibility, gaining fast, high-fidelity detection techniques, and benefiting from rapid response capabilities to reduce risks.

For more information on Gigamon ThreatINSIGHT and Zscaler, please visit:

GIGAMON.COM/THREATINSIGHT | ZSCALER.COM/PRODUCTS/ZSCALER-INTERNET-ACCESS

WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations around the world.

Take ThreatINSIGHT for a test drive, visit gigamon.com/demo.

Gigamon®

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