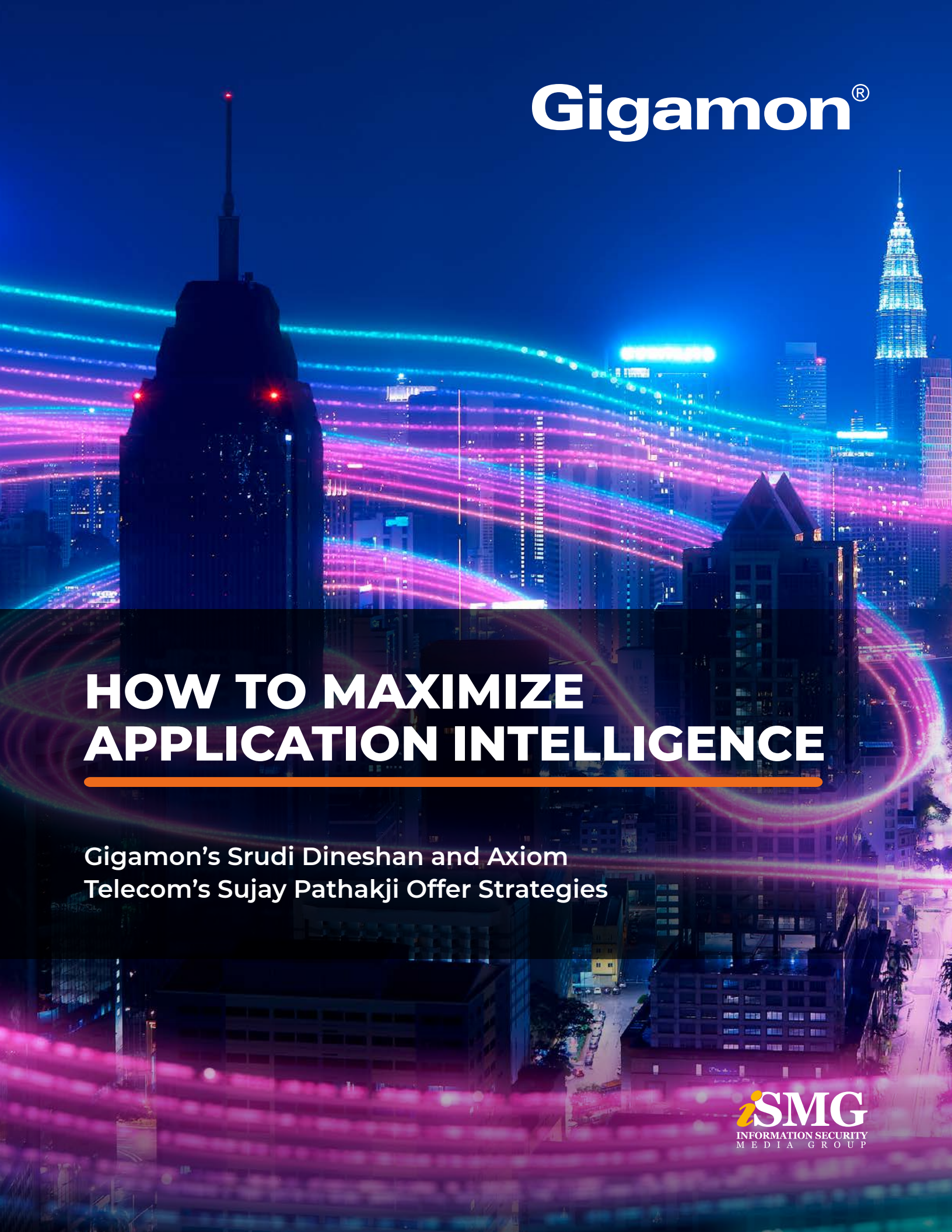
Gigamon®
HOW TO MAXIMIZE APPLICATION INTELLIGENCE
Gigamon's Srudi Dineshan and Axiom Telecom's Sujay Pathakji Offer Strategies
iSMG
INFORMATION SECURITY
MEDIA GROUP

SUJAY PATHAKJI

Dineshan is a senior product marketing manager at Gigamon.

Pathakji is a seasoned IT professional with strong emphasis on understanding business vision, requirements, effective communication and team building to deliver robust Agile IT solutions and services.

SRUDI DINESHAN

At a time when applications are more business-critical than ever - and visibility is more challenging to achieve - we need to discuss new strategies and tools for maximizing application intelligence. **Sujay Pathakji** of Axiom Telecom and **Srudi Dineshan** of Gigamon share insights.

In this video interview with Information Security Media Group, Dineshan and Pathakji discuss how to:

- Improve visibility into network and application data;
- Deliver the right application traffic to the right analytics tools;
- Reduce bottlenecks and meet security and compliance requirements.

APPLICATION INTELLIGENCE CHALLENGES AND RISKS

TOM FIELD: When it comes to maximizing application intelligence, where do you see organizations, including your own, struggling the most today?

SUJAY PATHAKJI: Applications need to give proactive information or decision-making insight to the business, and with certain legacy

“Applications need to give proactive information or decision-making insight to the business, and with certain legacy applications, it is challenging to pull that kind of data together to help the business make decisions on the spot.”

– Sujay Pathakji

applications, it is challenging to pull that kind of data together to help the business make decisions on the spot.

SRUDI DINESHAN: Organizations are struggling more with having visibility into what’s going on in their network and discovering the blind spots that can eventually lead to attacks or vulnerabilities.

FIELD: What’s at risk if these challenges remain unaddressed?

PATHAKJI: The biggest challenge is to support the business in the right way, at the right time, as per the requirement, without interrupting the business at a critical time.

DINESHAN: There are a lot of risks involved. If you’re missing something on your network, that becomes a huge challenge, which often goes unidentified without the right solution in place.

EVOLVING AND MAXIMIZING APPLICATION INTELLIGENCE

FIELD: Sujay, how have you seen the approach to application intelligence evolve over the past three years?

PATHAKJI: I’ve seen quite a few changes happening in past three years, especially post-pandemic, because the way businesses work has changed to a great extent. With the manpower split between working in the office and working from home and coming from different network segments to connect to the same infrastructure, it is challenging to control, coordinate and deliver the right result to the business. You need to segment the network coming in from the internal office and the network coming from the suppliers and collaborate and deliver fast results. There’s a lot of focus on security equipment, processes and policies to sharpen the time to the market.

FIELD: What are some specific examples of how you’re maximizing application intelligence today?

PATHAKJI: We have implemented a couple of SIEM solutions to identify and log the events coming onto the network, especially from unidentified networks or the home networks where a majority of the decision-makers are working due to the pandemic. And we have implemented a Smart MDM solution to lock the geographical interface to make sure there is no risk to the application.

COMMON CHALLENGES

FIELD: Srudi, how common are the challenges in the solutions that Sujay just detailed?

PATHAKJI: The challenges that Sujay mentioned are extremely common. It is crucial to maximize application intelligence and visibility, and we need both broad and deep visibility. Broad visibility means visibility into all infrastructure and across all data in motion, so you don't have blind spots, which are a huge security risk and hinder troubleshooting. Deep visibility is about gaining more information from the network and extracting intelligence from your network traffic.

Ten to 15 years ago, it was all about sending packets to the tools that need to process network data. But now – and five to 10 years from now – it's going to be all about extracting intelligence from network traffic. That's where application intelligence comes in because application intelligence allows customers to get actionable insights from the traffic itself and from the application the users are running. Application intelligence helps you identify things such as cryptocurrency mining, extract duplicate traffic and detect expired certificates, all of which is very critical. Application intelligence goes broad by being able to identify over 3,500 different applications and 5,000 attributes, and it goes deep by enabling you to decrypt encrypted traffic with deep packet inspection.

IMPROVING DATA VISIBILITY

FIELD: Srudi, how do you recommend organizations improve visibility into network and application data?

DINESHAN: Typically, IT teams take manual steps to mitigate these issues, but manual workarounds bring their own challenges. Whenever some change occurs, such as growth in an application's usage or the introduction of new applications, NetOps teams must update their physical network segmentation. And while regular expression-based application identification can work and application traffic patterns and behavior can change over time, IT must constantly test and update their home-drawn regedit signatures each time, which is a pain.

I recommend improving visibility into network and application data by deploying a solution that can go both broad and deep, to automatically

provide complete visibility and context needed to discover, manage and secure even complex and multi-tier applications. And this is exactly what Gigamon application intelligence provides. It employs flow pattern matching, bidirectional flow correlation, heuristics and statistical analysis to accurately identify thousands of standard and even custom applications. And it directs that information, along with application-aware metadata, to selected tools to improve their effectiveness, which is super critical.

MATCHING TRAFFIC AND TOOLS

FIELD: How do you deliver the right application traffic to the right analytics tool?

DINESHAN: Historically, all applications were treated as data equally, and data from each application was sent to every tool. There were two issues with that. Number one is that the tools were being overwhelmed by irrelevant data because most of the time, duplicate packets were being sent to these tools. Duplicate packets in the network don't add any value. Cutting back traffic does not mean weaker security or less visibility. In fact, it means better visibility because you're streamlining and optimizing your traffic and eliminating blind spots across your network.

The second issue is that not all applications are important to all the tools. Each application is unique in its importance to each tool. For example, a forensic solution needs to see all traffic, whereas a web application firewall need to see only the web traffic. Secure email gateways care about emails, attachments, embedded URLs, etc. So it is important to extract and precisely match an application's traffic and information with the right tool. This also provides the ability to isolate the application and its components and protocols, which makes it easier to facilitate that app's tool matching so you can easily enforce policies on categories of applications. Then administrators can define a set of tools that analyze all corporate traffic, another for all database traffic and a third set for shadow IP and P2P traffic.

Gigamon application intelligence enables IT to select the traffic by application or family of applications and send it to the appropriate

"Gigamon application intelligence enables IT to select the traffic by application or family of applications and send it to the appropriate tools. This ultra-granular control lessens the burden on tools and allows them to focus on the mission-critical applications."
– Srudi Dineshan

tools. This ultra-granular control lessens the burden on tools and allows them to focus on the mission-critical applications.

MEETING SECURITY AND COMPLIANCE REQUIREMENTS

FIELD: Going forward, what are your recommendations for how security and technology leaders can reduce bottlenecks and meet security and compliance requirements?

PATHAKJI: Security should be considered at each stage of the application, and that is where the Agile technology called DevSecOps plays a major role. When you embed security right from the conception of a software until its end delivery, you address the application intelligence issue at a better level than the legacy softwares, because the security is embedded right from day one. The applications, by default, have intelligence built in to segregate and deliver quality analytical traffic to the tools so you can make very knowledgeable decisions to stop security threats.

DINESHAN: One of the top things on a security or technology leader's mind is how to reduce the bottlenecks and meet the security and compliance requirements while trying to prevent advanced threats and attacks to your network. So it is critical to derive these application behaviors and details pertaining to flows, reduce false positives on your network, identify nefarious data extraction and automatically identify a wide range of applications and their underlying components and accelerate threat detection through proactive, real-time monitoring versus reactive forensics.

I recommend deploying a complete visibility fabric that goes both broad and deep. Without a visibility fabric in the middle, the tools are forced to get all relevant and irrelevant data, and this increases false positive across your network and makes it difficult to detect nefarious data extraction and attacks. Some tools don't need to see specific traffic, such as Spotify or Netflix traffic, that is considered safe but that has huge files. We filter out that type of traffic, send cleaner data to further optimize your tools and reduce bottlenecks. Also, the right visibility fabric helps you with compliance and privacy. It can mask out PII information in a healthcare record but send everything else over to the tool, which is super critical. And because compliance and privacy policies change, your fabric should be completely agile and easy to adapt.

Gigamon®

NETWORK VISIBILITY FROM CORE TO CLOUD

Gigamon helps the world's leading organizations run fast, stay secure and innovate. With visibility into network traffic across the entire hybrid cloud infrastructure, organizations eliminate security blind spots and helping improve SOC effectiveness. Close the SOC visibility gap with Guided-SaaS NDR and access expert advisory guidance when it matters most.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io