WHITEPAPER

How to Gain Control of Complex Applications in the Time of Digital Transformation

Application intelligence provides both the visibility and the context needed to manage and secure the microservices-based digital applications at the core of your DX strategy.

Preamble

Among the goals of digital transformation (DX) are streamlining business processes, cutting costs, improving productivity and introducing new business models that redefine industries — or build new ones. These are ambitious goals, and they're ultimately realized through new digital applications built on intricate microservices-based architectures.

For examples of successful DX applications look no further than ride sharing apps like Uber and Lyft, or home sharing apps like Airbnb. In the financial world, consider robo-advisors, peer-to-peer lending services, crowdfunding campaigns and cryptocurrencies — these are all DX innovations. Applications built around connected Internet of Things (IoT) devices can also fit into the DX category, as can industry-specific solutions, such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and medical systems protocols.

While these modern, multi-tiered DX applications bring agility and innovative capabilities, their complexity makes monitoring and securing them difficult, if not impossible, with current network visibility tools. This puts the success of these applications in particular — and digital transformation projects in general — at risk.

NIKE

Athletic shoe and clothing giant Nike says that DX now permeates its business from top to bottom. "It is truly an end-to-end initiative at Nike," said CFO Andy Campion. "It starts with consumer data and analysis around consumer data. And I'd say, that is manifesting itself right now already and most importantly, in terms of digital demand sensing."

According to Retail Info Systems, "Nike's SNKRS app has become the world's number one footwear shopping app, according to Nike. In 2016 Nike acquired Virgin Mega, a 12-person tech start-up focused on building gamified mobile shopping experiences for millennials."[1]

KEY TAKEAWAYS FROM THIS WHITEPAPER

- Digital transformation, made possible by digital applications, is central to business success
- Modern digital applications are incredibly complicated so new approaches are required to monitor and secure them
- Application intelligence based on deep packet inspection and other techniques provides a consistent and reliable way to do so

Introducing Application Intelligence

Fortunately, there is a source of information to solve these challenges: the incredibly rich application data flowing across the network. How then can IT leaders access network-based application data and put it to use for managing DX applications? The answer lies in a new set of capabilities collectively known as application intelligence.

Next, we'll explore these topics in more detail. Read to the end to find information about Gigamon Application Intelligence.

The Complexity of Today's Digital Applications

The two- or three-tiered applications that held sway for so long are rapidly being replaced with microservices-based architectures running on-premises, in the cloud and on partner clouds, delivered through web and mobile interfaces, simultaneously.

Amazon, for example, moved "from a two-tier monolith to a fully-distributed, decentralized, services platform serving many different applications" where "between 100–150 services are accessed to build a page."[2]

Many of today's microservices, moreover, use third-party software and open-source libraries over which you have little control. And each microservice may run in a much more distributed fashion than in the past. For example, what used to be an on-premises Oracle data tier may now be a mix of MongoDB in VMware, Elastic Search in VMware and JSON objects in a private cloud, while still making calls to the on-premises Oracle database.

All in all, today's digital applications provide tremendous flexibility and agility because new functionality can be developed, tested and deployed much faster than before. That enables organizations to pivot quickly to address new needs.

No Free Lunch: Complexity Has Consequences

So what happens when these component microservices don't work well or even fail? What happens when hackers exploit vulnerable attack vectors or expose personally identifiable data?

The Monitoring Challenge

First off, in the age of microservices-based architectures, application monitoring is far more difficult. Rather than monitoring a single monolithic application, you now must monitor hundreds or thousands of component services — all interacting in intricate patterns.

Among the consequences of this are:

- Logic that's distributed across many microservices and embedded in the data flow between them, and the fact that the same microservice may be serving more than one application, makes it difficult or impossible to monitor applications
- You cannot instrument third-party software over which you have no control
- Small changes in microservices you don't know about — especially in third-party software — can have large effects on overall application function

The result? It's much more difficult to locate where bottlenecks are occurring, know if suspicious data is flowing out and understand what the user is experiencing. Picture thousands of customers complaining that their mobile banking app freezes or crashes, with your IT team being unable to isolate where the problem is occurring, to get the idea.

The Security Challenge

While the security challenge includes many of the monitoring challenges described above, there are additional factors to consider.

- First, because DX application data can flow across many servers running on many different infrastructures, the surface area for potential attacks is exponentially larger.
- Digital applications, moreover, are much closer to the edge because application components need to communicate with third-party systems, which increases exposure to outside threats.
- Compliance issues come into play as well, and not just for heavily regulated industries like healthcare and financial services. If you don't know that an obscure database run by a third-party microservice is leaking customer Social Security numbers, you're putting your entire business at risk for heavy fines or worse.

The bottom line, according to Gigamon CTO Shehzad Merchant, is that "no one developer truly understands all communication patterns between the different microservices. Each microservice also has its own surface area of attack by hackers, and many of these microservices are developed by third parties who may not know how to secure them."

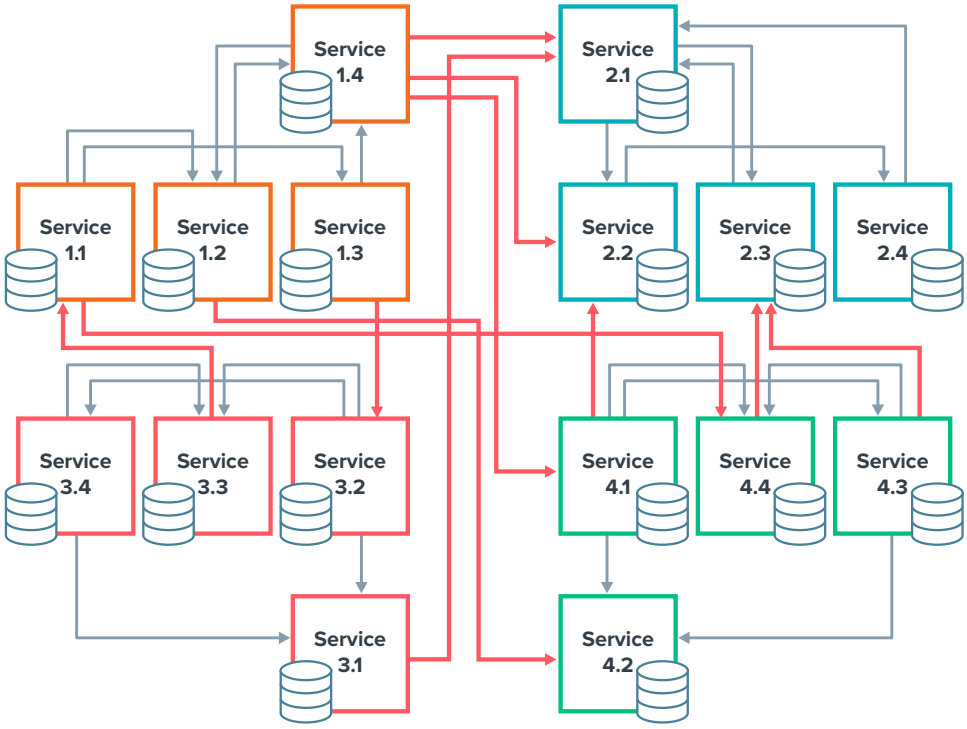

Figure 1: The intricate interactions between microservices makes monitoring and securing DX application difficult, if not impossible, using traditional capture methods.

ATTACKS AT THE EDGE

For an example of a multi-tiered application with a larger attack surface and closer to the edge, look to Tesla. In 2018, RedLock, a cloud monitoring and defense firm, discovered that some of Tesla's Amazon Web Services (AWS) cloud infrastructure was running cryptocurrency mining malware, after being hit with a sophisticated cryptojacking operation — because of an open server that wasn't password protected.[3]

The Limitations of Today's Network and Security Tools

Why can't today's network and security tools do the job? The answer lies in the fact that they're not getting the traffic they need to perform their given functions. Why not? To gather data, network and security tools rely on agents placed next to application components. With so many components in so many locations — including third-party and cloud-based components — it's just not feasible to place agents next to them all.

If, for example, the security monitoring tool gets data from only 30 percent of the application's components, that leaves 70 percent unexamined. Or if the application performance monitoring (APM) tool cannot isolate a malfunctioning payment protocol, then the tool cannot be used to troubleshoot why payments keep failing for customers.

Solution: Go to the Network and Capture Application Flows on the Wire

To address these problems — complex microservices-based applications that are difficult to monitor and secure — we turn to the network and its handling of traffic between microservices.

According to Sudip Chakrabarti writing in *Medium*:

> "Therefore, a packet-level inspection of that traffic, combined with the application telemetry data collected for each service, should offer an unparalleled X-ray image of a distributed application in execution unlike any other we have seen before."[4]

Application Intelligence: Putting Network Data to Work

To be useful, however, you need to capture all application traffic on the network, including all traffic between the many component microservices. Once you do that, you can identify applications and their microservices, extract information and metadata, and then distribute that information to monitoring and security tools.

Collectively, this is called application intelligence. It removes noise and brings clarity to each tool to see and analyze precisely the applications that are relevant for it, thus increasing that tool's effectiveness and efficiency, and decreasing security vulnerability.

Application intelligence will have three main parts to accomplish this.

1. Application-Aware Visibility

Application-aware visibility identifies applications and their component microservices across multiple tiers. This helps IT teams locate and remove bottlenecks in complex applications running across hybrid networks.

2. Application Data Extraction

Complex DX applications can drive up network traffic, which can overwhelm monitoring tools. Application extraction extracts application traffic from the network and forwards only the relevant information to the appropriate tools. For example, a Data Loss Prevention (DLP) tool does not need to analyze streaming media traffic.

3. Application Metadata

Application metadata fed to analytics tools provides the context behind an incident — whether performance or security-related. It enables the deep application insight needed to understand why an application is running slow, how it's performing and what the customer is experiencing. For example, application metadata might reveal a slow load time for a mobile app or the fact that an embedded video froze during playback.

Application Intelligence Cannot Be an Afterthought

Application intelligence isn't a feature that is simply built into a DX-ready infrastructure; it's the fabric of the DX-ready infrastructure. To be truly successful in your DX journey, make investing in application intelligence your first step.

"Network traffic is a fantastic source of telemetry in that you can tie it back to the application, or microservice. It's a uniquely effective way to map out communication patterns and profile them, and through that you can fingerprint application activity."

- Shehzad Merchant, Chief Technology Officer at Gigamon

VISIBILITY INTO NON-END-USER DEVICES

The so-called things experience can be as important as the customer experience because IoT devices are often integral to modern IT landscapes. These devices are greatly diverse, and their closed architectures make monitoring difficult. Having visibility into each device's network activity is critical to monitoring and even more so for security.

Gigamon Application Intelligence

Gigamon Application Intelligence is able to identify more than 3,000 applications and more than 5,000 application metadata elements. It captures all application and microservice traffic running across the network. With that data, IT teams can visualize each app, extract an app's or app component's traffic for precise analysis, and use application metadata to ensure strong customer experience and security.

To learn how Gigamon can help, visit www.gigamon.com/app-intel.

[1]Grill-Goodman, Jamie. "How Nike's Digital Transformation is Personalizing Retail." Retail Info Systems. September 26, 2018. Accessed April 30, 2019. risnews.com/how-nikes-digital-transformation-personalizing-retail.
[2]Hoff, Todd. "Amazon Architecture." High Scalability. September 8, 2007. Accessed April 30, 2019. highscalability.com/amazon-architecture.
[3]Newman, Lily Hay. "Hackers Enlisted Tesla's Cloud to Mine Cryptocurrency." Wired. February 20, 2018. Accessed April 23, 2019. wired.com/story/cryptojacking-tesla-amazon-cloud.
[4]Chakrabarti, Sudip. "In the Land of Microservices, the Network Is the King(maker)." Medium. March 3, 2016. Accessed April 30, 2019.

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