Tech Outlook

November 2017

SEEING IS BELIEVING

Ixia's CloudLens solution eliminates network blind spots with increased cloud visibility.

What's going on inside your network *right now*?

Few organizations today can answer that question with much certainty. Networks are bigger, faster and more complex than ever before, making it difficult to keep tabs on the myriad factors that can impact network health, performance and security.

"Most network management professionals will readily admit that they lack visibility into large segments of their network operations," said Thomas Bock, Partner Alliance Manager, ProSys. "Cloud migrations, in particular, have contributed to network blind spots that make it difficult get an end-to-end view of network performance."

Top Priority

Eliminating these blind spots has become a top priority for IT professionals. In a recent Ixia survey of 220 IT executives, 61 percent said improving network visibility is the key to improving network performance, data protection and regulatory compliance.

More than half (54 percent) of respondents said that although they operate six or more network segments, they monitor only half of them. Of the 40 percent that reported handling more than 10,000 customer records, less than 10 percent actively monitor and protect their network.

By and large, those surveyed understand that their blind spots are making them vulnerable to many potential threats. Half said better network visi-

continued on page 2

TECH OUTLOOK

PRSRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

continued from page 1

bility solutions would help protect their organization against Distributed Denial of Service attacks, and 54 percent said they believed improved visibility would help them discover security breaches.

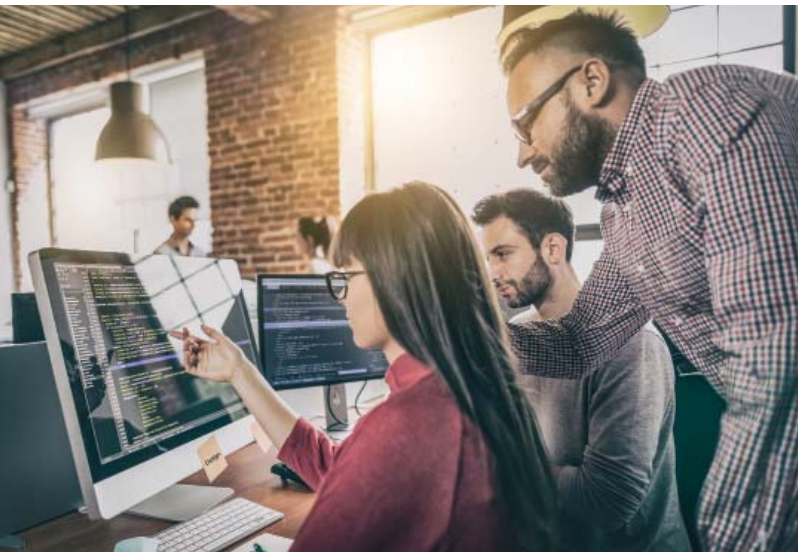
To gain network visibility, organizations typically employ a variety of monitoring tools that inspect and analyze packet data to identify patterns and anomalies. While it is fairly easy to intercept and inspect packets as they move between physical devices in the data center, things become much more complicated in the cloud.

"In an on-premises data center with physical access to the network infrastructure, you can physically insert network packet brokers and monitoring devices inline between network devices where they continuously copy and aggregate data," said Bock. "Obviously, you lose that capability in the cloud without hands-on access to the infrastructure, so your visibility is extremely limited."

Cloud Complications

One of the most appealing characteristics of cloud computing is that it relieves an organization of significant infrastructure burdens. The cloud provider hosts the infrastructure components traditionally present in an on-premises data center, including servers, storage, networking hardware and a virtualization layer. Because this infrastructure is essentially transparent to the client company, it is extremely difficult to intercept and analyze data packets moving between cloud components.

Further complicating cloud visibility is the fact that organizations are commonly using a multi-cloud strategy involving multiple cloud services offered from different providers at the same time. According to RightScale's 2017 State of the Cloud survey, cloud users today are running applications in an average of 1.8 public clouds and 2.3 private clouds.



In an effort to gain visibility into their cloud traffic, some organizations will backhaul cloud traffic to the physical data center for packet inspection and sorting. Others use a technique known as "hairpinning" to force network traffic to loop back through an inspection point. However, these techniques can dramatically reduce throughput and efficiency by creating congestion and latency.

Recognizing these limitations, cloud providers and infrastructure vendors have begun offering cloud-enabled versions of key monitoring tools. However, many of these tools have significant drawbacks — they report only on low-level metrics without packet-level visibility, they require cloud providers to be involved in data transfers and they don't scale well for multi-cloud environments.

At Your Service

Ixia's CloudLens platform has no such shortcomings. Offered via a Software-as-a-Service (SaaS) platform, CloudLens is fundamentally a collection of Amazon Web Services coordinated to provide on-demand access to network traffic across the entire infrastructure — whether it resides in a public or private cloud, data center or branch office.

Its serverless architecture enables it to function seamlessly in any public cloud deployment. It supports all leading public cloud platforms, including Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Bluemix and Alibaba Cloud, making it the ideal visibility solution for organizations running multi-cloud environments.

As a SaaS solution, it supports cloud-scale elasticity and self-serve installations for tenants, which eliminates the need for cloud provider involvement. CloudLens operates without network constraints and does not rely on hypervisor- or provider-specific features.

Unlike the cloud-enabled versions of data center solutions being developed by other vendors, Ixia's solution was purpose-built for managing cloud traffic. It has a microservices design that uses container technology to fully embed packet brokers in each cloud instance. This allows packet processing to take place in the cloud, eliminating the need to backhaul traffic to the data center. Processed data can then be sent to either on-premises or cloud-based security and monitoring tools.

Ixia has developed a broad ecosystem of technology partners to ensure CloudLens' interoperability with a range of monitoring tools. Key members of an organization can use a web-based management interface to feed filtered packet data from CloudLens into troubleshooting and analysis tools, application performance management tools, data loss prevention tools, and much more.

"CloudLens is the first solution that provides complete visibility across heterogeneous networks," said Bock. "It delivers on all the key challenges that organizations are facing as the result of network blind spots."

News Briefs

Compliance Technology Evolving

The use of technology to manage regulatory monitoring, reporting and compliance — so-called "RegTech" — has seen a sharp uptick since the 2008 global financial crisis ushered in a new wave of government and industry scrutiny. Initially focused on the automation of manual reporting processes to reduce errors and achieve compliance, RegTech is now evolving to actively identify and mitigate emerging threats.

A new survey by SWIFT and Dow Jones Risk & Compliance finds that 54 percent of global compliance professionals plan to increase RegTech spending in the next three to five years because it is improving their ability to tackle a variety of financial crimes. For example, behavioral analytics software can identify suspicious activity that could be a sign of misconduct. Analytics tools are also being used to predict disruptive events in financial markets.

"Technology can play a key role in providing new and enhanced capabilities that strike a balance between preventing criminal activity, meeting regulatory requirements and containing costs," said Paul Taylor, Director of Compliance Services, SWIFT. "The most sophisticated financial crime compliance solutions help mitigate risks and boost efficiency in several ways, from managing workloads to automating payments monitoring and reducing false positives, enabling compliance teams to focus on more strategic risk policy and financial crime prevention work."

Architecture Planning Needed, Report Finds

As companies rely more on cloud-based applications and foray into new areas such as the Internet of Things, comprehensive technology architecture planning is quickly becoming an essential need, according to a new report from a leading technology association.

Today, just 34 percent of companies say they build IT architecture strategies beyond a 12-month window, according to a CompTIA survey of 500 U.S. firms. Yet a majority acknowledge the need for improved planning across their entire IT architecture — hardware, software development, data and security.

There are obstacles to more comprehensive architectural planning. Forty percent of companies say they don't have the budget for new architecture investments. One-third say they lack expertise in emerging technologies and new trends.

However, most companies believe they are capable of planning a new technology architecture, and they recognize that such planning can lead to improved collaboration between IT and business teams, and a greater ability to evaluate current technologies against long-term objectives.

"By connecting the construction of IT architecture to overall corporate objectives, both groups will be better informed about the options available and the tradeoffs involved when selecting devices, applications or operational models," said Seth Robinson, senior director, technology analysis, CompTIA.

Tech Outlook

Editorial Correspondence:
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
Michelle.Clery@prosysis.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
info@prosysis.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
info@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
John.Little@prosysis.com

Indianapolis, IN
Phone: 317-688-1283
Bill.sanders@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
info@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
info@prosysis.com

Mexico City
Phone: +52 (55) 3601 3755
info@prosysis.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
info@prosysis.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
info@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
info@prosysis.com

Seattle, WA
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Smarter Security

Threat intelligence provides the actionable information organizations need to enhance their security strategies.

Most security tools are designed to detect and defend against specific types of cyberattacks. Firewalls allow only trusted traffic to flow through, while intrusion prevention systems examine data packets and drop those that appear to be malicious. Antimalware solutions look for viruses, Trojans and other malicious software and keep them from causing damage to systems.

These tools are very effective at combatting known threats. But as Gartner noted in a recent report, "leading indicators of risk to an organization are difficult to identify when the organization's adversaries, including their thoughts, capabilities and actions, are unknown." That's why advanced persistent threats (APTs) and zero-day exploits are so hard to detect using traditional security tools.

Typically, however, there are clues. Security threats don't exist in a vacuum. The challenge lies in uncovering those clues and using them to predict how and when a cyberattack might take place.

That's the role of threat intelligence. Gartner defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." In other words, threat intelligence tells organizations who is targeting them, what tactics are being used, and what systems or data are being targeted so they can take action.

"As an organization seeks to hone its information security team and harden its security posture, it is a natural step to consider the use of TI. Detecting incidents sooner, and potentially even preventing them, is the overall goal of TI. Mature information security teams often see TI as a way to bolster the environment and prepare for both known and unknown threats," wrote cybersecurity consultant Matt Bromiley in a recent SANS Institute whitepaper.

What Is Threat Intelligence?

The term "intelligence" is frequently used in a military context. It refers to the gathering and assessment of data about the enemy's size, movements and capabilities so that leaders can develop the best strategy. The FBI has defined intelligence as "information that has been analyzed and refined so that it is useful to policymakers in making decisions — specifically, decisions about potential threats to our national security."

The same definition could be used for threat intelligence by substituting "policymakers" with "IT security professionals" and "national" with "organizational." Threat intelligence isn't raw, unfiltered data but information that has been evaluated in the proper context. It is accurate, current and actionable, enabling security teams to respond to threats quickly and effectively.

Threat intelligence can be internal or external. Internal threat intelligence uses data gathered from security devices and systems within an organization. Security information and event management (SIEM), log management, security and

vulnerability management (SVM), risk management, and incident forensics are some of the tools used for internal threat intelligence.

External threat intelligence uses data from sources outside an organization. Many organizations subscribe to data feeds, including free services from the SANS Internet Storm Center, CERT and some IT vendors, and fee-based services that aggregate and correlate multiple data feeds and provide customer-specific alerts. Other sources of external threat intelligence include crowdsourced platforms and information from industry groups, government and law enforcement.

Gartner Research Vice President Anton Chuvakin divides threat intelligence tools into two broad types. Tactical threat intelligence includes system and network-level indicators that humans and machines use to detect and respond to attacks. Strategic threat intelligence includes higher-level reports on cybercriminals, their capabilities and activities that humans use for planning and decision-making.

Strong Demand but Hurdles Remain

According to a new report from Research and Markets, the threat intelligence market should see a compound annual growth rate of 17 percent through 2023. Demand for threat intelligence solutions is being driven by increasing numbers of cyberattacks, rapid uptake by small to midsize enterprises, and widespread adoption of crowdsourced platforms.

Adopters of threat intelligence claim to have greater visibility of attacks in context, and improved accuracy and speed in detecting and responding to threats. In addition, these organizations are using threat intelligence to develop general security policies and strategies.

However, threat intelligence remains underutilized. In a study by the Ponemon Institute and Webroot, 40 percent of organizations had a security breach within the preceding two years, and 80 percent of those victims believed threat intelligence could have stopped or reduced the impact of the attack. Yet 47 percent of survey respondents admitted that threat intelligence is not a core component of their security strategy.

Poor-quality data limits the value of threat intelligence, according to 85 percent of respondents — 56 percent believe intelligence data becomes stale within minutes or seconds. In addition, 49 percent use paid sources of data because free sources do not adequately support threat analysis and prioritization.

But data quality and the sources of data aren't the only problems. Only one in six respondents believe they have effective processes for using threat intelligence from external sources, and less than 30 percent believe they are capable of effectively handling internally generated data.

Nevertheless, threat intelligence is receiving a lot of attention as organizations seek to stem the tide of cyberattacks. By gathering and analyzing security data, and applying it to internal processes, organizations can supplement attack-specific tools with a strategic approach that will protect against the most elusive threats.

Incident Response Plays a Key Role in Effective Cybersecurity

Experts say that a security breach is virtually inevitable — that it's a matter of "when" not "if." How an organization responds to a security incident ultimately determines its impact.

Incident response refers to the process of addressing a cyberattack in order to minimize downtime, damage and costs. According to the SANS Institute, incident response begins with proper preparation and planning, so that key personnel know the procedures they should follow when a security breach occurs. The incident response team will likely include representatives from executive management, legal, human resources, public relations and customer service as well as IT.

The incident response plan should define what constitutes an "incident," which might include data exfiltration, unauthorized access, malware infection, denial of service attack and other security-related events. Incidents should be categorized based upon the type of data involved, the type of perpetrator responsible, the scope of the event, and any legal or regulatory compliance requirements involved.

Once a potential incident has been identified, the response team will likely need to conduct an investigation in order to understand what type of event they are dealing with. The initial investigation should be conducted as rapidly as possible and involve digital forensic experts at an early stage. Forensic experts can analyze systems in a way that preserves evidence.

Only then can the IT team work to contain and eradicate the problem and recover systems, applications and data. As a final step, the response team should assess the incident and how it was addressed, and look for ways to improve the process.

The average cost of a data breach is $3.62 million globally, according to a new report from the Ponemon Institute and IBM Security. However, a formal incident response plan can significantly reduce the financial impact of a security event.

"Quickly identifying what has happened, what the attacker has access to, and how to contain and remove their access is more important than ever," said Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services. "With that in mind, having a comprehensive incident response plan in place is critical, so when an organization experiences an incident, they can respond quickly and effectively."

Accounting Countdown

IT teams are under pressure as deadline nears for new financial reporting rules.

Most companies are significantly behind in their efforts to meet the impending Jan. 1, 2018, deadline for implementing the Financial Accounting Standards Board's new revenue recognition standard, according to recent Deloitte survey.

Officially known as Accounting Standard Codification (ASC) 606, the new standard is considered to be one of the most significant changes to U.S. accounting principles in years. Because it alters the way companies must book revenue, it essentially affects any organization that has contracts with customers.

The compliance process has strong implications for IT departments because it involves new ways of collecting, aggregating and reporting data. In most cases, implementing the new standard requires designing and implementing new software solutions and internal controls.

Nearly 70 percent of respondents to the Deloitte poll released in June said their organizations were still assessing how they will implement the new standard.

"Implementing the new standard is fast becoming a fire drill," said Deloitte consultant Eric Knachel. "From establishing a budget to ensuring proper data collection and testing system modifications, the implementation process requires substantial time and resources. Companies should not underestimate what a significant undertaking implementation will be."

Far-Reaching Impact

Revenue is a key metric for evaluating a company's financial performance and prospects. However, the previous U.S. and international standards were different, often resulting in different accounting for transactions that were economically similar. The new standard aims to remove those inconsistencies and ensure that financial statements provide more useful information.

However, the Deloitte survey indicates that most organizations don't seem to fully understand the reach of the standard. More than half (52 percent) of poll respondents said they do not think the change will have a material impact on their company's financial statements.

That may be a misreading of the standard, which was initially announced in May 2014. Unlike other accounting standards updates that affect only one or two line items in financial statements and can be taken care of by the accounting division, Deloitte says ASC 606 is a "transformational" rule requiring organization-wide changes that could take many months to implement.

"Companies should recognize that while the standard might not affect balance sheets or income statements in some cases, it can still have a significant impact on related disclosures," warned Knachel. "A significant risk around revenue disclosures is a potential loss of investor confidence and a decrease in shareholder value."

IT's Burden

Although compliance will require significant effort throughout an organization, it seems clear that IT departments will have to do some of the heaviest lifting. As finance departments analyze contracts to determine how they book

sales under the new rules, the changes likely will require IT to rewrite old accounting programs, install new applications, upgrade systems and revise internal controls.

These changes will have a cascading effect throughout IT, touching not only accounting systems but ERP, CRM, business intelligence, data warehousing, document management, enterprise application integration and more.

The reporting of financial results has always been a challenge for IT because financial data comes from multiple sources and is difficult to consolidate. Reporting breakdowns often occur when two or more highly autonomous operating units are using different analytical tools and different metrics to generate financial reports.

In some organizations, interpreting and consolidating these reports is typically a manual, spreadsheet-based process that is prone to error. Other organizations utilize business intelligence and data warehousing tools to create proprietary dashboards for merging reports. Either way, those processes must all be redesigned for the new requirements.

Many organizations likely will decide to implement new applications that have been designed for ASC 606 compliance. However, even that won't be a simple solution. New applications will almost certainly require some customization to fit existing systems and processes. If so, IT must work closely with internal and external auditors to ensure that the customizations don't bypass any audit-trail controls.

Managing the Change

IT will also have to take the lead in project management. The leading cause of tech implementation failure is poor project management. The IT department must ensure that any new or upgraded financial systems are selected and implemented within defined schedules, budgets and acceptable levels of risk.

Additionally, the project management team must ensure that there are no cross-application issues across departments. Without proper management, it is possible that different business units could wind up using different tools and different metrics — particularly given the easy access to a variety of cloud-based platforms. IT must enforce uniformity across reporting tools to ensure a "single source of the truth."

Given the size of the job, it seems shocking that 55 percent of the respondents to the Deloitte survey released in June indicated that their company has not started to assess internal controls from a revenue recognition standpoint. Furthermore, 56 percent said their company has yet to establish a budget for implementation.

"Revenue issues are the most common problem underlying accounting enforcement actions," said Knachel. "The clock is ticking, and it is critical that disclosures, internal control considerations and adequate resources be front and center as companies work to adopt the new standard."

Cisco Intersight

Managing the demands of digital transformation

Cisco Intersight™ is a cloud-based system management platform with embedded analytics and machine learning designed to address modern IT requirements. It features a dynamic user interface that can be customized by user role, and new functionality is delivered via portal updates without burdening customers with upgrades. The platform is designed to constantly learn to help make daily IT operations easier. It enables organizations to achieve a higher level of automation, simplicity, and operational efficiency. Contact your ProSys representative to learn more about Cisco Intersight's capabilities.

PROSYS

www.prosysis.com 888-337-2626