WHITE PAPER

Edge Computing:

Four Smart Strategies for Safeguarding Security and User Experience

It is a brave new world for enterprise networks. Smart devices are getting smarter, and edge computing is emerging as a viable way to reduce latency and improve performance. But as network architectures grow increasingly amorphous, what kind of impact will this have on security and performance?

New Technologies, New Threats

Is edge computing driving better user experiences, or expanding your network's attack surface? Are Internet of Things (IoT) devices enterprise enablers, or potential vulnerabilities?

Those are just a couple of the questions network architects ask themselves every day. SD-WAN, IoT, and 5G are pushing the limits of the cloud. As businesses demand faster response times and higher performance, edge computing has emerged as an ideal solution. Everywhere you look, devices, appliances, and branch locations are processing more and more data locally.

But as we trust IoT with more business-critical transactions, are we increasing our vulnerability in the process?

KEYSIGHT TECHNOLOGIES

Network perimeters are vanishing, and so are the traditional defenses that once secured them. But your security and performance monitoring tools are still only as good as the data you feed them. Too much noise or too little data can seriously impact their ability to correlate events, identify breaches, and safeguard your end-users' experience.

Unfortunately, capturing that data is more difficult than ever — and edge computing is only making it harder. After all, when data no longer flows through your central data center, blind spots are bound to occur.

Now that's the bad news. **But it doesn't need to be that way.** By capturing dynamic network intelligence from your network's edge, you can arm your security and performance tools with actionable insights — protecting your assets, applications, credibility, and bottom line all at once.

Here are four key considerations to help you start:

1. Eliminate Blind Spots by Capturing Packet Data

When it comes to security, time to detect and time to remediate are critical to containment. In fact, according to a recent study from Ponemon and IBM, **companies that can detect and contain a data breach within 30 days save, on average, more than $1 million.**[1]

You need to get in front of attackers. That means eliminating vulnerable blind spots by capturing traffic from your network edge — traffic that your centralized security tools might not be able to see. But not just any data will do. Log files are easy to capture, but they never tell you the whole story. By contrast, packet data is the gold standard, and most tools require it to properly detect and diagnose security threats.

What We Recommend: Boost Security by Deploying a Fleet of Network Packet Brokers

Edge computing makes it harder to capture packet data, but it is by no means impossible. Since your centralized security and performance monitoring tools are no longer receiving data directly, you need to bring the data to them. By installing network packet brokers (NPBs) across the edge of your network, you can gather critical packet data and send it back to your centralized tools for analysis.

1 Ponemon, 2019

Pro Tip

Not all NPBs are created equal. Some are prone to dropping packets, while others have difficulty when multiple filters or features are used at the same time. In contrast, with decades of experience building test gear for all the major network equipment makers, Keysight's highly optimized hardware and software architectures allow features to be applied while traffic continues to flow at wire speed with no dropped packets. Check out Keysight's full suite of NPBs to discover what sets us apart — and how we perform under pressure.

2. Manage Cost and Scale

Traditional network tools are expensive appliances designed to reside in centralized locations such as corporate data centers. However, since edge computing relies on localized data processing, that approach will not work. You need to collect packet data across the entirety of your network's edge. That means deploying NPBs at all your large branch offices.

Unfortunately, most tools are simply too large and costly for that. Sacrificing coverage is the last thing you want. You need a solution that is inexpensive enough to purchase at scale and small enough to deploy at remote locations.

What We Recommend: Make Sure Your NPBs Are Compact and Cost Effective

You cannot secure what you cannot see. That's why it is so critical that your edge NPBs are designed and built for that application. Specialized tools like these should be affordable enough to scale, yet integrate seamlessly with your centralized data center infrastructure — enabling you to remotely access metadata as well as packet data from branch sites and remote locations.

Pro Tip

Edge-optimized NPBs are few and far between, but they are worth seeking out. Configuring and modifying a fleet of devices via command line interface (CLI) is not only time consuming — it is an easy way to make mistakes. In fact, a single error in a regex configuration at a major CDN recently caused a mass website outage, bringing down a significant portion of the internet for a half hour.

This is one of the reasons why devices like Keysight's Vision Edge series (Vision E100, Vision E40, Vision E10S, and Vision E1S) can be deployed and administered with an easy-to-use GUI that saves valuable time and minimizes errors.

3. Do Not Settle for Bare-Bones Features and Functionality

A cost-effective solution does not have to mean compromising on features. In fact, settling for the bare minimum can cost you even more.

Take load balancing, for example. Your security and performance monitoring tools may rely on packet data, but an uninterrupted stream of information can be like drinking from a fire hose. While most tools feature some load balancing, too much data can easily overwhelm them — causing latency issues, missed events, and false positives.

What We Recommend: Remote Administration and Smart Data Processing Are Non-Negotiable

The right features make all the difference. Things such as centralized management consoles can seem insignificant at first. But think about it: do you really want to deploy a significant number of devices that do not support efficient provisioning or remote administration? After all, individually configuring and controlling each device takes a considerable amount of time and effort.

At the same time, you need the ability to capture, filter, and deduplicate out-of-band monitoring data at the source. That way, you can save your tools' bandwidth for more expensive and elastic needs, such as machine learning and artificial intelligence.

Pro Tip

Keysight's edge-optimized NPBs (Vision E100, Vision E40, Vision E10S, and Vision E1S) make it easy to get maximum performance with minimal effort. All come standard with our industry-leading Visibility Intelligence (including NetStack feature set). They also include an intuitive drag-and-drop interface that enables faster, more accurate configuration and administration — even at scale.

4. Take Control of User Experience with Active Monitoring

Edge computing is supposed to reduce latency and improve user experience. But what happens when things go wrong? Passive monitoring tools that utilize packet data are great for troubleshooting, root-cause analysis, and course correcting; but they can be inconsistent and will only alert you to an existing problem. If you want to get ahead of problems and safeguard user experiences at the edge, you need a proactive approach.

In contrast to normal performance monitoring, active monitoring (also known as "synthetic monitoring") tools simulate traffic by sending synthetic packet data to various endpoints across your network. You get the best of both worlds: you can monitor user experience in real time while proactively probing for issues that would otherwise only reveal themselves under live traffic loads.

What We Recommend: Install Active Monitoring Endpoints at Every Branch Location

In today's enterprise, a quality user experience is non-negotiable. Connectivity is the heartbeat of business. Employees and customers alike depend on peak performance. With such unforgiving expectations, an active/synthetic monitoring strategy is imperative. By deploying hardware- and software-based endpoints at all your branch sites and remote locations, you can make sure no performance problem goes undetected.

Pro Tip

When delivering services to small branch offices (like retail stores or bank offices), monitoring last-mile connectivity, network service level agreements (SLAs), and quality of service (QoS) is both incredibly important and incredibly difficult. A simple way of addressing this challenge is with a solution like IxProbe. A scalable inline monitoring system, IxProbe enables SLA verification and insight into the ability of the network to meet QoS expectations by combining active/synthetic monitoring with inspection of real traffic to help provide a true understanding of your network's health and performance.

For larger branch deployments, consider Vision Edge 1S. Featuring an integrated endpoint for Keysight's Hawkeye active monitoring platform, it combines active/synthetic monitoring capabilities with a cost effective NPB — giving you an integrated solution that improves security and network performance all at once.

Network Intelligence Helps You Future-Proof Your Network's Edge

We are in the midst of a sea change for enterprise networks. Like it or not, the cloud is not enough anymore. And despite potential security and performance concerns, edge computing and IoT are not going anywhere.

So what does this mean for you? It means it is time to future-proof your network. A rapidly expanding edge means managing a significantly larger attack surface and a host of potential performance problems — but that that does not necessarily mean you are fighting a losing battle.

Security and user experience are far too important to leave to chance. Provided you take the right steps in capturing network intelligence, you can protect your network for years to come. From your data center to the farthest reaches of your network's edge, you can rest easy knowing your data is safe, secure, and under control.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES