WHITE PAPER

Exposing Hidden Security Threats and Network Attacks

Nearly one-third of IT teams are using 11 or more active tools to monitor and troubleshoot their networks.

Introduction

Over the years, information technology (IT) departments have been implementing solutions that answer two questions:

- How do I make as many services available to stakeholders as possible?
- How do I protect and secure everything?

While some IT departments approach these as a dual mandate, others treat them as competing goals with tradeoffs. Sometimes security takes priority and other times new services are so powerful or transformative they are deployed immediately and secured with best efforts.

Cloud, virtualization, and mobility have brought a wave of vendors offering point solutions with benefits such as scalability and efficiency. At the same time, the number of security vendors offering advanced types of protection have exploded. While new trends in IT have increased availability and access to services, it has also shattered the traditional network boundary—data and assets no longer sit in a single location behind a firewall. As a result, many enterprises have erred on the side of *there is no such thing as too much security*, especially with the increased frequency and sophistication of attacks. A recent study of network management practices found nearly one-third of respondents are using 11 or more active tools.[1]

1 Enterprise Management Associates, "Network Management Megatrends 2018," April 2018, available to subscribers.

KEYSIGHT TECHNOLOGIES

With company data everywhere and a slew of security products and network monitoring tools already deployed, enterprises are now asking if there is a way to get more out of these investments. A way not only to get access to data no matter where it is, but also to provide security tools with needs-based access to all, some, or none of the data, in the format it can use. Keysight addresses these concerns with a deployment model that combines network intelligence and security solutions into a cohesive security architecture capable of efficiently exposing hidden threats and attacks aimed at the network.

The Digital Warfare Attackers Are Waging

Protecting data and IT assets is more challenging partly because attackers employ more sophisticated methods to get around enterprise security. Some of these attacks hide within encrypted communications and observers predicts this technique will be increasingly used in malicious attacks. Here are some common weapons in a hacker's arsenal and how they use them.

Malware - Malicious software that comes in many different forms. Many malware instances morph or are regenerated daily so they can avoid signature-based detection systems.

Phishing - an attack where seemingly valid emails are sent to unsuspecting users in an attempt to trick the user into clicking on an embedded link in the email. Phishing emails typically appear to be from valid senders, such as an employer or the user's bank. When the recipient follows a link, they are then prompted to enter sensitive information or malware is pushed down to their system.

Botnet - an orchestrated army of infected hosts that unknowingly participate in malicious campaigns under the control of a botnet herder or controller. The botnet controllers communicate with these infected hosts using "Command and Control (C2)" connections, which can be sent over many different common protocols such as IRC, HTTP, DNS, and others. They are typically encrypted to avoid detection. Botnet controllers send commands to infected hosts directing them to leak sensitive data, download additional malware, or attack other targets in a DDoS attack.

Exploit - Hackers often conduct large-scale reconnaissance, looking for hosts with exposed vulnerabilities. Many services have to be advertised to the Internet in order to conduct business such as HTTP/HTTPS, SSH, VoIP, RDP, VPN, and others. Vulnerabilities are discovered over time in the software packages which advertise these services and hackers are constantly scanning for sites which run vulnerable services.

Hijacked IP Ranges - are stolen from their legitimate owners, typically by corrupting the routing tables of Internet backbone routers. Once hijacked, they are used for malicious purposes such as phishing and malware distribution.

Distributed Denial of Service (DDoS) - an orchestrated attack from hundreds or thousands of sources that flood a target with so much needless traffic that it cannot process legitimate traffic. DDoS attacks aim to disrupt and overload a system to bring it down or to impair network security from properly protecting the network. Some DDoS attacks are used as a smoke screen for data theft.

Advanced Persistent Threat (APT) - a network attack where the goal is to get into a network and stay there, undetected, for a long time. The purpose is to steal data rather than do damage. It usually starts with an attacker gaining access and then establishing a back door so he can come and go easily. Once inside, the attacker attempts to gain access to other systems and networks and opens more back doors. Malware is spread inside the network to collect data and then it is exfiltrated through the numerous back doors.

IT Trends

Trends in IT such as cloud and virtualization, combined with workforce mobility and globalization, mean businesses must protect themselves from all angles. Data centers are now distributed and increasing mobility is forcing companies to extend their network edge—often into places where they cannot easily gain visibility to the traffic they need to monitor. This causes blind spots, which rapidly become havens for security attacks.

- **The Mobile Employee** - Modern employees are no longer tethered to the office. They use an array of mobile devices for both personal and professional purposes, blurring the line between home and work. As a result, employees are downloading their own applications to their devices, beyond what was part of the corporate standard issue. In mobile environments, data traffic frequently bypasses traditional security defenses and flows directly from mobile devices to the cloud. A global survey of security professionals found that 64% are doubtful their organizations can prevent a mobile cyberattack.[2]
- **The Cloud** - As businesses migrate workloads from their private data center to public clouds, applications and data no longer have a permanent home. While the cloud offers unprecedented flexibility, it also expands the perimeter. Data, sensitive or not, are being sent to the cloud, worked on in the cloud, and stored in the cloud. In fact, according to the Cisco Global Cloud Index, cloud data center traffic will represent 94% of total data center traffic by 2021.[3] And enterprises are not just

2 Dimensional Research, "The Growing Threat of Mobile Device Security Breaches," April 2017, accessed at: https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf.

3 Cisco Global Cloud Index: Forecast and Methodology, 2016-2021 White Paper, February 1, 2018, accessed online.

using one cloud or one application in the cloud. According to Forbes, a recent study on cloud usage predicts that 83% of enterprise workloads will be in the cloud by 2020 and 41% will be running on public cloud platforms.[4]

- **The Internet of Things** - IoT is transforming off-line or manual functions into devices that are now connected to the network and share information. This happens often with little to no security oversight. Whether it is IoT devices like security cameras or production automation, IT security has more network connections to manage and more data in transit to monitor. The IoT world will explode to a projected 200 billion connected devices by 2020, according to Intel[5], potentially posing security risks to our homes, energy grids, wearable devices, connected cars, and digitally monitored implantable medical devices.

The Challenges Of Securing Enterprise Networks

Businesses are using a complex array of multi-vendor appliances and threat analysis tools to protect, secure, and analyze network traffic. Choosing between them, integrating them successfully, and monitoring them effectively has become a significant network visibility challenge. With traffic volumes and threats increasing, the number of security tools that need access to a reliable stream of data is also growing.

- **Inline Security** - The key to successful inline security monitoring is to enable active, real-time traffic inspection and detection without impacting network and application availability. This methodology is designed for proactive threat prevention. If one of your security tools becomes congested or fails, you need to keep traffic moving, continue monitoring, and prevent a network or application outage. Some organizations deploy their inline security appliances behind the firewall in a serial configuration. With this design, if an appliance becomes congested or fails, traffic stops. Redundant network paths can help avoid this, but they require twice the number of tools. Ensuring both paths can handle the full volume of traffic is expensive and leaves tools on the inactive path under-utilized during normal operations. Examples of typical inline security tools include the following:
  - Intrusion prevention systems (IPS)
  - Firewalls and next-generation firewalls (NGFWs)
  - Data loss prevention (DLP) systems
  - Unified threat management (UTM) systems
  - SSL decryption appliances
  - Web application firewalls (WAF)

- **Out-of-Band Security** - The key to successful out-of-band security monitoring is to enable passive traffic inspection, detection, and recording for routine analysis. This methodology is useful for delivering key information to your security tools for detailed threat analysis. Either a standard network tap, a virtual tap, or a network switch port is converted to a SPAN to gain access to network data from different

4 Louis Columbus, "83% of Enterprise Workloads Will Be in the Cloud by 2020," Forbes, Jan. 7, 2018. Data from LogicMonitor Cloud Vision 2020: The Future of the Cloud Study, accessible online.
5 Intel "A Guide to the Internet of Things," accessed online Aug 20, 2018.

points in the network. Some organizations directly connect out-of-band security appliances to a tap or SPAN port, but this greatly reduces scalability when there are more network segments that need monitoring than ports on a tool. Examples of typical out-of-band security tools include the following:

- Security Information and Event Management (SIEM) systems
- Intrusion Detection Systems (IDS)
- Behavior analysis systems
- Forensic tools
- Data recording
- Malware analysis tools
- Log management systems
- Packet capture tools

Prepare Enterprise Networks For Stronger Protection

Organizations today are moving away from connecting security tools directly to tap or SPAN ports. Instead, they are building a security architecture on top of a network visibility platform that aggregates all of the network traffic across their organization--including virtual and cloud-based segments--and then delivers filtered traffic to their security solutions and appliances. This architecture uses physical, virtual and cloud taps to see traffic on each network segment and network packet brokers (NPBs) with the ability to filter and groom traffic. Bypass switches are added to protect network availability in the event of a device outage. This is a better solution because the visibility platform can enable both failsafe deployment and provides a stable foundation for any number of network and security tools.

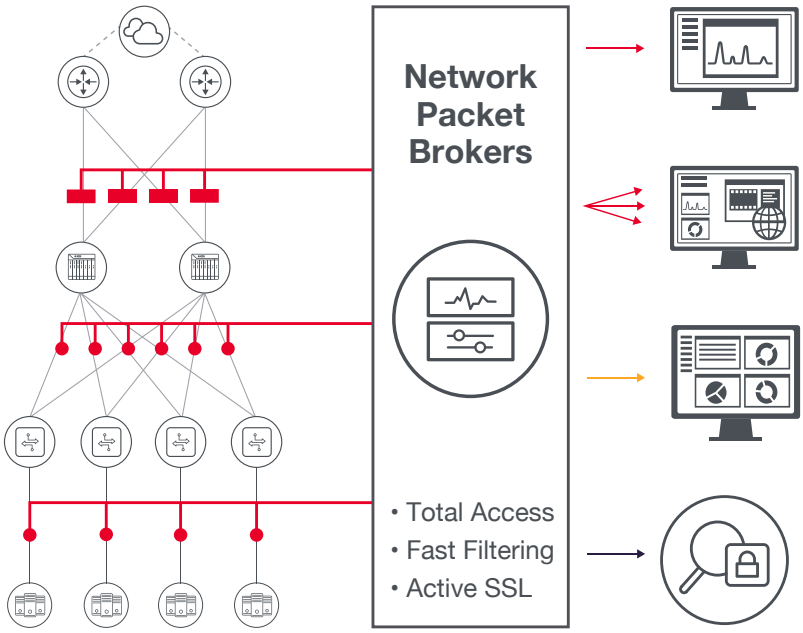
Modern network architecture provides multiple paths through the network to increase network reliability. Using virtualization and cloud resources to run workloads creates a high amount of east-west traffic that may never touch a touch a physical link. Both of these realities create a challenge for effective monitoring. Security tools need all data from a session to perform an accurate analysis. A network visibility platform addresses this need by aggregating traffic from multiple physical and virtual links, essentially stitching it together, to provide a more complete view for security tools, which improves inspection, detection, and protection.

A key advantage of a visibility platform is the ability to gather traffic from dissimilar network segments, aggregate and filter it, and then deliver it at the speed each security solution prefers. This type of security architecture combines 100% data access, resilience, and intelligence to reduce the load for the enterprise security team by ensuring the right data gets to the right tools, every time, even at high speeds.

The Keysight Visibility Platform

Keysight delivers complete, end-to-end visibility for both inline and out-of-band security tools. Some security tools need to see all data, while others only a subset. But they all need safeguards to ensure alternate paths exist in case of single tool outages. With a security architecture based on a total visibilty platform, you increase the effectiveness of analytics and security tools and optimize their data access.

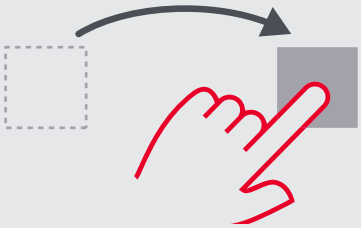
An Keysight network visibility platform strengthens security, but does not allow security monitoring to slow or disrupt network response times. The strength of Keysight's platform comes from the ability to apply context awareness to raw packet data and distribute only relevant traffic to your network security and monitoring tools. Keysight's visibility platform is also a breeze to configure and manage.



A security architecture based on Keysight's total visibility platform has four layers, each adding a critical element to create a powerful visibility engine for your security appliances and network monitoring appliances and network monitoring tools.

Why graphical configuration is superior to command line

As you configure connections and define filters in any visibility platform, management and control can quickly become complex, especially when there are many traffic sources and many tools. You want to distribute only relevant data to your tools—not the traffic it does not need. For example, you may want to send a certain monitoring tool only VLAN 100, 200, 201, and 300 traffic in addition to HTTP traffic, HTTPS traffic, and email traffic. In an environment with many data sources and many monitoring tools, setting up traffic filters for these parameters using a Command Line Interface (CLI) will become complex very quickly. It is also prone to mistakes and errors you may not uncover until you perform analysis. By then, it is too late. With a network visibility platform based on Keysight components, you configure and manage data sources and tools using an intuitive and powerful drag-and-drop interface. You have complete, granular control of your data and the patented compiler automatically creates and updates simple filters, overlapping filters, and dynamic filters behind the scenes. This ensures every type of packet you want delivered to a security tool gets there. With the straight-forward graphical user interface, you visually see the connections and the data no matter if you have one data source going to multiple tools or multiple data sources going to one tool—regardless of how you filter traffic.

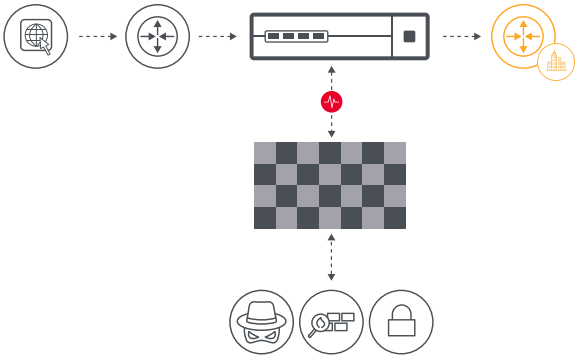


Data Access Anywhere - To get security tools the data they need, data access is critical. This can be done with physical and virtual taps or by converting a switch port to a SPAN port on a network switch. While using SPAN ports can be effective, they do have limitations. SPAN ports can only mirror traffic that passes through a network switch. If the network switch gets busy, the switch will drop packets on SPAN ports in favor of processing live traffic on switch ports. On the other hand, taps are a passive splitting mechanism placed between two network devices. A tap does not introduce delay and is unaffected by bandwidth saturation. It duplicates all traffic on the link (including MAC and media errors) and forwards it to the network packet broker's processing engines.

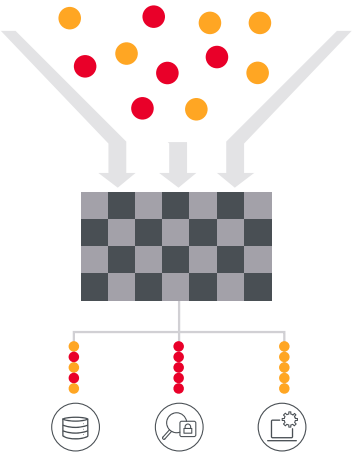
Security Resilience - To achieve security resilience for inline (or in-band) security tools, deployment requires maximizing availability and minimizing the impact from a failure. This is done with an external bypass switch that constantly monitors ports and paths and can automatically route around security tools at super fast speeds during traffic congestion, security tool failures, or maintenance events. To monitor every tool and path, Keysight bypass switches uses regular and negative heartbeats. Regular

heartbeats are injected into the normal data stream to see if a path or device is alive. Devices receive and return each heartbeat packet to let the bypass know they are online and ready to receive data. If two or more heartbeats in a row are not returned, the device is assumed to be offline. Negative heartbeats refer to the condition where heartbeats are sent to offline devices in order to know when they resume functioning. When a so-called negative heartbeat is returned to the bypass, it can automatically resume sending traffic to the device.

Keysight bypass switches also have the ability to fail open to ensure continued network availability or fail closed and block access to the network. When high availability is a requirement, Keysight's security architecture supports serial or parallel high availability and uses synchronous configuration and load balancing to ensure fully redundant security with near instant failover.

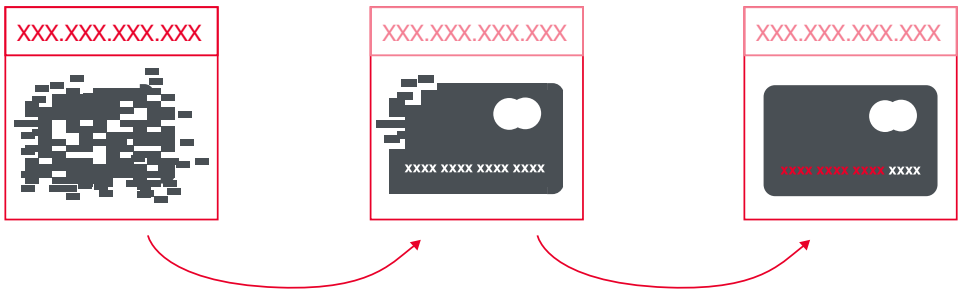


Context-Aware Data Processing - To get the right data to the right security tools, packet brokers use intelligent data processing to recognize rich metadata and deliver enhanced NetFlow information. This goes deeper than source and destination ports and IP addresses. Context-awareness requires a deep understanding of network traffic based on applications, devices, sessions, conversations, and geolocation and knowing which security tools need the data. And when multiple network segments are tapped, the Keysight NPBs automatically keep track of duplicate packets and ensure security tools only get one copy. Keysight allows you to create granular rules on the traffic forwarded to your security and monitoring tools. Over 220 application signatures are already built-in—just point, click, and configure with no cookbooks or scripting necessary.



Security Intelligence Processing - Your security tools are already working hard enough. With security intelligence processing, you can offload certain process-intensive tasks from your security tools to focus on suspicious traffic analysis. It starts with seeing all of the data, clear or encrypted. Keysight packet brokers are equipped with active SSL decryption capabilities to allow data to be identified and intelligently distributed to security tools. It saves security tools from

processor intensive decryption and helps avoid blind spots as some security tools do not have decryption capabilities. Security intelligence also means supporting data compliance. Keysight NPBs have the capability to strip off header data containing sensitive information or mask personally identifiable information such as credit cards or social security numbers before passing the data to network monitoring and security analysis tools. This is vital for compliance and to avoid penalties and fines. In addition, Keysight lets you integrate a threat intelligence feed so you can remove known bad traffic from ever entering your network. Removing traffic from IP addresses known to distribute malware, viruses, and other attacks can reduce the workload on your security tools by up to 35%[6] and reduce SIEM alerts by up to 80%[7].



6 Keysight internal analysis, 2016.
7 Keysight case study: "Hyper Box Tackles Attack Traffic with Keysight ThreatARMOR," June 14, 2016.

Summary

Network security monitoring requires processing and examining data that is exploding within a perimeter that is expanding. Hackers and the tools they use to infiltrate enterprise networks and exfiltrate company secrets are more sophisticated than ever. As a result, many organizations are using more security and network monitoring tools to spot threats and protect their business. This requires a deployment and integration model for inline and out-of-band security tools to integrate them properly and get the most out of their capabilities.

Keysight's security architecture, based on a network visibility platform, is the foundation for stronger inline and out-of-band monitoring and ensures resilient traffic delivery to all of your security, compliance, and analysis tools. With context awareness, Keysight helps you manage your network more efficiently by delivering only relevant, de-duplicated packets to your security and and monitoring tools.

Find out more about the Keysight security architecture at https://www.keysight.com/solutions/network-security.

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