cpacket NETWORKS

Business Brief

Fixing the IT Security Staffing Crises

IT SecOps Productivity Depends on the Right Visibility Tools

3.5

million unfilled security positions by 2021

60%

of GISW members indicate their organizations lack number of cybersecurity professionals needed for today's threat environment

75%

of organizations will experience IT disruptions by 2020, primarily from a lack of qualified IT security professionals

108

days to detect a threat

Increase IT Staff by Enabling Their Efficiency

Organizations are continually challenged to find and hire qualified IT security or network security staff. An article in Forbes Magazine, August 2018, "The Cybersecurity Talent Gap is an Industry Crisis" discusses the problem. The lack of available security operations (SecOps) professionals means existing staff will continue to struggle to keep up with the threat volume. Compounding this is a lack of timely access to critical security information that further impacts SecOps efficiency and their ability to identify and respond to threats.

The 2017 Global Security Workforce (GISW) Study from (ISC)2 stated that because of a shortage of IT staff organizations can't address security issues by hiring. Additionally, their complex network design along with the number and location of security devices exacerbate the effectiveness of security systems. This complexity increases the difficulty to identify, assess, and analyze security problems. Consequently, SecOps has difficulty getting the information they need to determine threats, risk state, or an appropriate response.

The lack of available security professionals and expertise gaps are compounded by the number and variety of security systems. This combination of overly complex systems and not enough staff makes detecting and protecting against threats a challenge. Multiple security systems on each network segment end up creating duplication and increased alert volume. The result is some systems on a busy segment get oversubscribed and start losing information, impacting their effectiveness, while others on lightly used segments are underutilized. Since potentially harmful traffic traverses' multiple segments, duplication or lost information reduces SecOps effectiveness in identifying, prioritizing, and responding to threats in a timely manner. Detecting and blocking threats is further constrained when SecOps has to spend their limited time on continuous hardware and software updates and patches of a large estate of security systems.

Addressing Staff Gaps Requires Supporting Security Infrastructure

A new network architecture is needed to empower SecOps with visibility and access to all the relevant traffic. It should support the removal of traffic extraneous to ongoing security analysis, allowing staff to quickly gather actionable insight into threat or other activities and focus on critical issues.

A 2018 article in CIO Magazine 2016 quoted a Gartner survey stating 20% of organizations experienced visible IT security disruptions and predicted that number to increase to more than 75% by 2020. As noted earlier, this is due to the lack of available IT staff. The 2018"State of Cybersecurity" survey conducted by ISACA stated that the lack of expert staff also means it takes on average 108 days for organizations to detect threats with an added impact on the time it takes to respond.

Network Gaps Should Enhance Security Staff Capabilities

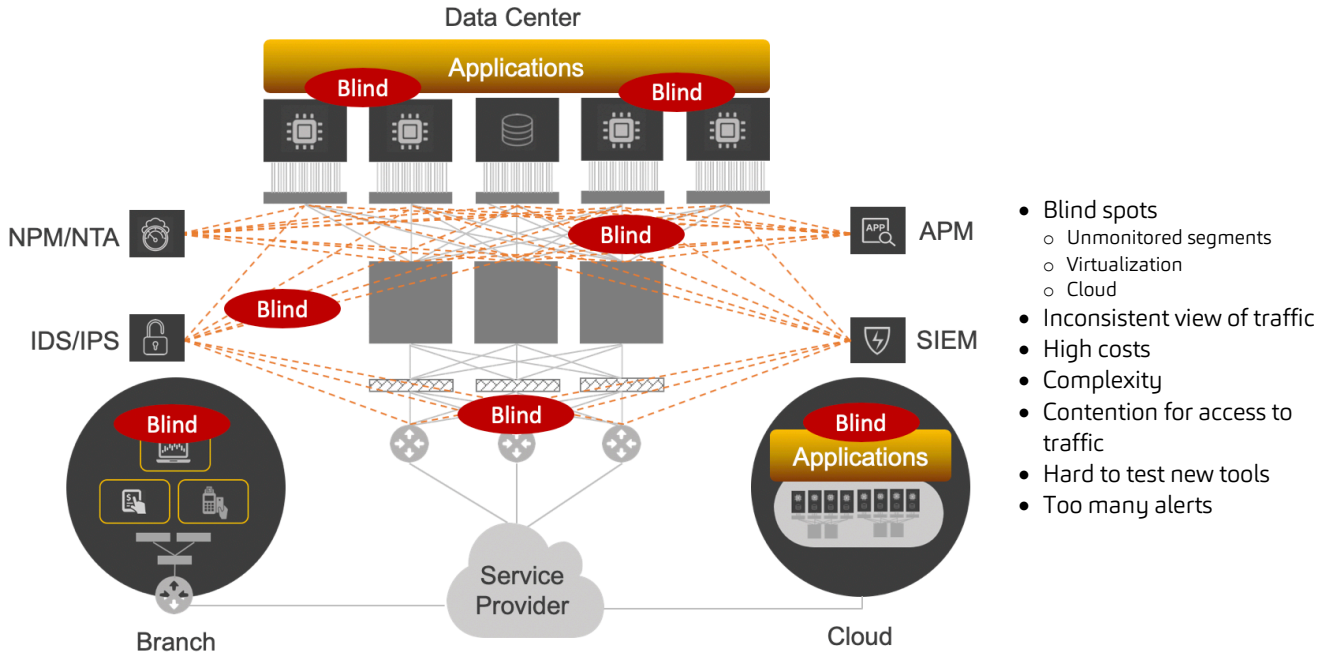
There isn't any technology that can replace security professionals. The complexity of information security and the ever-changing types of attacks require highly skilled and forward thinking SecOps professionals. Their expertise is central to security effectiveness and network reliability. However, without access to the right data, their analysis and response capabilities can be compromised. This can make even the best SecOps professional struggle to do their job. But with the right architecture designed

to reduce the complexity of existing setups, security tools and security staff can be more efficient and more effective.

Enabling Security Staff with Advanced Infrastructure

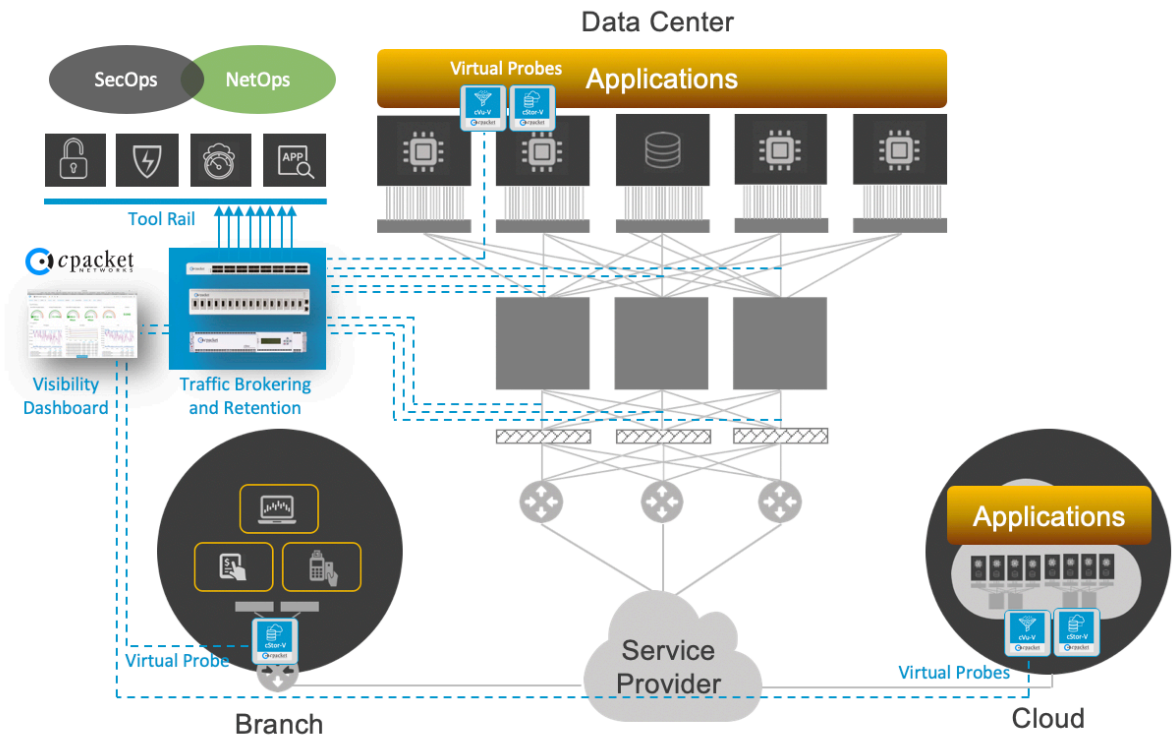
Numerous security tools deployed on multiple network segments increase costs and create contention for access to network data. The image below represents a standard network security tool deployment where tools are positioned throughout the network on the most critical network segments. This often leaves blind spots where threats can hide in less critical segments, virtual workloads, and in cloud deployments. This setup makes it hard for SecOps to review or correlate data across segments or between tools.

Enhancing security effectiveness derives from the ability to view and capture all available and relevant information. It must provide staff with the details for identifying and resolving threats quickly. To overcome visibility issues requires a well-architected network monitoring fabric. To ensure security systems do not miss an event, the monitoring fabric must remove blind spots, stop oversubscription, and not drop packets due to traffic bursts or lack of processing power. The architecture needs to provide functionality such as removing duplicate data and filtering of unnecessary data to reduce the traffic security tools need to process.



Partial Visibility – Complex and Costly with Blind Spots

A high-performance monitoring fabric avoids network issues that can overwhelm security systems while enabling complete visibility for more effective protection. Using cPacket cVu series Network Packet Brokers (NPB), all network traffic is collected from physical, virtual, and multi-cloud systems, processed and sent to a central tool rail. This approach allows high availability and redundancy of the security devices. Security efficiency is increased by removing traffic not needed by the security tools while first reporting on all the network traffic. This allows staff to quickly identify threats or anomalous behavior, find bad configurations, and identify errors. cPacket cStor series physical and virtual devices can further strengthen the security posture by capturing every relevant packet and store it for deeper analysis. With the availability of comprehensive threat information, staff can conduct detailed forensic analysis, security reviews, and audits to determine the nature of any ongoing or past attack and best-case response. All cPacket cVu and cStor products, physical or virtual, can be centrally managed and visualized through cClear dashboards.



100% Visibility – Delivering Reliable and Lossless Data to the Tools

Network and traffic levels will always grow but a well-architected monitoring infrastructure will support that growth while maintaining SecOps capabilities at the highest level.

An effective monitoring solution facilitates security staff ability to find threats by:

- Delivering the right data to the right tools
- Increasing the coverage of the security tools
- Reducing the time security professionals spend managing the security environment
- Increasing staff effectiveness by reducing the duplication of alerts for analysis
- Increasing the availability and performance of security tools
- Reducing costs and simplifying workflows
- Enabling adaptable security ecosystem based on real-time security and network information

Being able to monitor an entire network and its devices will reduce the number of existing tools for cost savings, free up resource time and investment funds, and more importantly, increase the efficiency of existing security staff.

To learn more, visit www.cpacket.com

About cPacket Networks

cPacket Networks delivers visibility you can trust through network monitoring and packet brokering solutions to solve today's biggest network challenges. Our cutting-edge technology enables network and security teams to proactively identify issues in real-time before negatively impacting end-users. Only cPacket inspects all the packets delivering the right data to the right tools at the right time and provides detailed network analytics dashboards. Whether you need greater network visibility for security tools or performance monitoring tools, our solutions are designed to overcome scalability issues and reduce troubleshooting time. The result: increased security, reduced complexity, with lower costs, and a faster ROI.

Based in Silicon Valley, CA, cPacket enables organizations around the world to keep their business running. Leading enterprises, service providers, healthcare organizations, and governments rely on cPacket solutions for improved agility, higher performance, and greater efficiency. Learn more at www.cpacket.com, the cPacket blog, or follow us on Twitter, LinkedIn, and Facebook.