Secure Pipes: Changing the Expectation of Your Internet Service Providers

FROST & SULLIVAN

An Executive Brief Sponsored by Level 3

Frank Dickson
Industry Principal – Information & Network Security

January 2015

The Internet was a 20th century blessing, and one which continues to provide transformational benefits in the 21st century. The Internet is no less significant in transforming the world economy than the sextant or steam engine. However, the benefit of the Internet has brought with it a dark side; a side that is regularly illuminated by high profile data breaches, whose names include Home Depot, Target and RSA.

The reality of today's Internet is that cyber threats are becoming increasingly more sophisticated. Advanced Persistent Threats (APT), botnets, zero-day attacks, and countless malware variants have caused significant monetary damage on a global scale. Essentially, APTs are the result of lessons learned from cyber nation-state attacks such as GhostNet and Stuxnet.

As the sophistication of the threats increase, the battle lines in the war against cyber miscreants have also changed. What was once an almost impenetrable perimeter "wall" around enterprise networks has become a defensive membrane, one which stops many attacks but regrettably allows some attacks to pass through.

The increasing sophistication of attacks has driven an evolution in the tools used to combat these exploits, and has motivated network security vendors to create new tools. An unforeseen problem has developed though. As the complexity of the threats being combatted increased, the complexity of the existing tools used to combat the threats also increased.

This problem of complexity is only exacerbated by the fact that the universe that security professionals need to secure is growing as more organizations, public and private, move their IT resources to the cloud, and employees increasingly access resources with their personal mobile devices—a trend often referred to as BYOD (bring your own device).

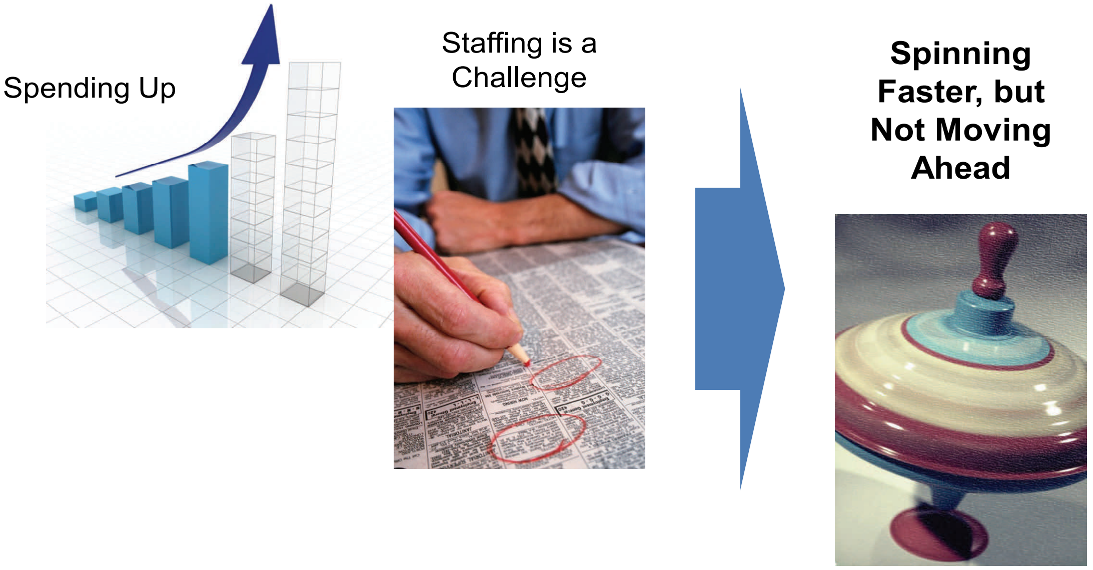
Managing the increasing complexity of network and information security is being attempted by security teams that are already overtaxed. In a recent survey conducted by Frost & Sullivan, on behalf of the (ISC)^2, of over 12,000 information security professionals, 56% reported that their organizations have too few information security workers.[1]

Security professional staffing issues cannot simply be addressed by "throwing money at the problem." Cyber security requires distinguished credentials, which are in high demand; and, as cyber security is a constantly changing field, training of existing and new employees is essential. Additionally, retaining security professionals presents an extra challenge as other organizations place a high demand on your security specialists. Consequently, providing a rewarding work environment, including a desirable career path for your security professionals, is a must.

The practical reality for many organizations is that they are spending more money on security, and are expending more and more energy addressing staffing challenges; but these same organizations are simply "spinning faster" but not making any true progress. Something has to change. At the risk of employing an overused term, a paradigm shift is in order. The manner in which security is approached needs to fundamentally change.

[1] This survey finding and others are contained in *The 2013 (ISC)2 Global Information Security Workforce Study*, available at https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf.

Today's Cyber Security Conundrum



Spending Up

Staffing is a Challenge

Spinning Faster, but Not Moving Ahead

CONCEPT OF A SECURE PIPE

In the early days of the Internet, Internet service providers focused on providing access—both more access (locations) and better access (speed). Both consumers and organizations seemed content with assuming responsibility for the security of the access; after all, more is better, right? Cyber security after-the-fact, sometimes referred to as "bolt-on" security, seemed to suffice.

Organizations are increasingly starting to ask more from their Internet service providers. Why accept traffic that is contaminated, only to examine and attempt mitigation of the threats once this traffic has arrived at your locations? Analogously, when we purchase items such as automobiles, we expect safety features to be integrated into the products that we purchase. Imagine purchasing an automobile, and then trying to add air bags, antilock brakes, brake lights, and other safety features after the fact.

Sandboxing and "big data" analytics are innovations resulting from fundamentally rethinking the approach to security—being proactive rather than reactive. In a like manner, organizations are increasingly looking to Internet service providers to examine and filter network traffic before that traffic ever reaches their premises, rethinking the way that cyber security is delivered by integrating security into the "pipe."

After all, no one wants a dirty pipe, least of all a security professional. Many security functions can effectively and efficiently be conducted in the network, minimizing misdirected time and effort investigating false positives or incidents that have low impact, and saving security professional resources for operations requiring a professional interaction. This is the concept of "secure pipes."

In practice, secure pipes are more than clean pipes. A clean pipe provides filtered traffic, readily identifying and purging known bad traffic from the traffic flow before reaching the organization's network. Clean pipes are good;

but a secure pipe is much more: think next-generation clean pipes or clean pipes 2.0. Secure pipes are the result of clean pipes (filtered) plus analytics for detection and prediction (expose and predict). Fundamentally, Internet service providers leverage their network assets and in-house security teams to improve the quality of the pipe in three stages.

Filter

In filtering, an Internet service provider integrates its vast intelligence collected from the proverbial "catbird's seat" of a large global network. At this stage, the network stops "known bad" by detecting and purging malicious files contained in inbound traffic using signatures, and filtering outbound traffic destined to known bad, suspicious, and undesirable URLs.

Traffic filtering not only prevents malware but also has a secondary benefit of mitigating the impact of existing breaches by interrupting botnet command and control traffic. For example, Cryptolocker, a ransomware Trojan targeting Microsoft Windows computers, requires that the infecting malware call-out to its command and control server to get the private keys that it needs to encrypt the files of a victim's computer, preventing legitimate user access to files. If the malware is unable to reach that server, the malware is rendered impotent.

Given the extreme rate of change of malware, filtering is most effectively done in the network, utilizing intelligence that is updated virtually instantaneously, rather than hourly or even daily in many on premises-based solutions. Additionally, productivity benefits are created by filtering within the carrier provider network. Little reason exists to expend security professional resources on traffic that is known to be bad, saving their time for where the deductive reasoning of a trained professional can be better applied. No one wants to see "known bad" traffic.

Expose

In the filter stage, the goal was to stop the known bad. In the expose stage, covert and unknown malicious content is illuminated though the application of advanced analytics, identifying and investigating the questionable. Exposing unknown malicious activity in the network employs three key methodologies:

- Anomaly Detection – Monitor network traffic, establish a baseline of what is normal, and detect anomalous traffic that is indicative of malicious activity
- Behavioral Analysis – Analyze traffic for known behaviors that indicate improper activity
- Flow Data Comparison – Monitor traffic flows for activity that is not congruent with legitimate known good patterns

Expose is the stage in which the advantages of applying security in the network come to light. The ability to expose unknown malicious traffic is directly correlated to how much can be seen, or the scope of visibility. Even the largest enterprises have only tens of thousands of endpoints. Having the visibility of millions, tens of millions or hundreds of millions of endpoints provides visibility benefits that cannot be replicated by a single enterprise. Additionally, there is an effectiveness benefit as security is applied at light speeds. Breaches and data exfiltration time is measured in minutes and sometimes seconds. Applying security at line rates within the carrier network provides an additional layer of security, extending defense in-depth and refining the network perimeter.

Predict

The goal of prediction is to stop an attack before it starts, blocking before the first punch is thrown. For example, distributed denial of service attacks are preceded by "pinging and prodding" of Web sites and networks, as cyber miscreants perform pre-attack reconnaissance. The resulting digital breadcrumbs provide the foresight to anticipate attacks, and then ensure proper protection, minimizing business interruptions. Proactive security such as this can best be accomplished by Internet service providers, as it requires the visibility of an entire network.

WHAT IS EXPECTED FROM A SECURE PIPE?

Several core security technologies are integrated into a secure pipe. These technologies include:

- **Network firewall and intrusion detection and prevention systems (IDPS) services** – Best -in-class network firewall and IDPS software is continually refreshed without the need of capital outlays for equipment purchases, maintenance, or training staff.
- **Distributed-Denial-of-Service (DDoS) Protection and Mitigation** – Network based DDoS protection allows security to scale with customer needs, eliminating the need to worry about unanticipated issues.
- **Email and Web filtering** – Policy options and administrative controls enable customizable policy settings and granular administration controls similar to those associated with dedicated gateway appliances.
- **Advanced Analytics** – Applying "Big Data" principles with state of the art analytics and precise execution improves network security. Flow-based security monitoring provides data such as bandwidth, application performance, and network utilization to augment traditional security data. The key is integrating the analytics into the pipe to provide "serious security horsepower" that is applied on behalf of the customer. The burden of implementation and operation are adeptly handled by the Internet service provider.

BENEFITS OF SECURE PIPES

The concept of secure pipes changes the way in which organizations should think and approach security. Much of the historical model of security was based on hardware and software that needed to be managed and maintained, often with an electronic leash (known as a pager, and now a smartphone) for security professionals. Secure pipes changes the model by providing 24x7 protection by default, as the carrier is always "on," always alert. Remember, business continuity is a fundamental component of a carrier's DNA.

Secure pipes changes the way security is managed. Network technicians and security professionals can now share the responsibilities of security. Network technicians can manage the IT infrastructure. Security professionals can focus on activities that require specialized expertise. Coordination and cooperation create a holistic approach to integrated network security. Perimeter defenses placed at the edge (LAN-WAN demarcation) of an integrated network security architecture can be sized to be smaller (less traffic to process), and have policies that are complementary and more surgical than the policies used in the "pipe."

Additionally, secure pipes reduces the required security responsibility of in-house security staff and network administrators. Security professionals are less likely to need to be experts in all aspects of security, allowing them to optimize or re-prioritize their attention on the many important and urgent tasks and initiatives pulling at their time and talent.

Secure Pipes is a New Innovation; The Market Need is Not New

In many ways, secure pipes is an enhanced methodology to address the market need first addressed by Unified Threat Management (UTM) appliances, which combine security technologies onto a single platform as a means to reduce complexity and improve security integrity for the business. These technologies are predominately focused on protecting the private networks of businesses from the inherent risks of conducting business operations and communicating over the Internet. As Internet service provider networks represent the bridge or gateway between business networks and the Internet, the migration of UTM from the edge of the business network into the communications network is a natural. This migration retains the core value proposition of UTM, and adds optimization of the network access connections, outsourced management of the security hardware and software infrastructure, and the potential cost savings of a cloud-delivered service (e.g., the cost of essential flex infrastructure is spread over a subscriber base rather than a single business).

Secure pipes validates and goes beyond the value of a traditional UTM solution by providing DDoS, WAF, and analytics. Secure pipes combines security technologies, the cloud, ubiquitous visibility, and robust connectivity into a single service that is easily subscribed to by the customer. However, UTM provides an illustrative example of validated market demand.

BENEFITS BEYOND SECURING THE PIPE

Secure pipes is also about optimizing the performance experience of connected users, and reducing network costs as the flow of network traffic changes. By placing security in the network carrier's pipes, performance issues affecting end users can be prevented before they arise. Additionally, tangible examples of this performance assurance include:

- **Blocking of DDoS Attacks at the Carrier's Edge** – In a nod to reducing core network usage in mitigating DDoS attacks, and a change of course from its earlier blocking approach of attack traffic, secure pipes can move blocking upstream, nearer to DDoS attack traffic origination. The core network provides the route optimization benefit (i.e., avoids congestion points) via real-time traffic analysis and routing algorithms. Significant expense savings can be had by not carrying unwanted traffic, or by not unnecessarily moving traffic greater distances than needed. Additionally, scrubbing traffic at the edge reduces latency for legitimate traffic. Lowering cost while improving performance is compelling for organizations—a win/win.
- **Unified Threat Management (UTM) in the Pipe** – By integrating security services such as stateful firewall, VPN, intrusion detection and prevention, anti-malware, Web content filtering, and data loss prevention into the pipe, each of the customer's locations virtually sits on the doorstep to the Internet. Internet-destined traffic from branch offices and remote locations is not re-directed to a headquarters gateway for security treatment, or to a small number of regional, multi-tenant security platforms. The performance hit due to network hair-pin turns is essentially eliminated.

- **Protecting the Internet of Things (IoT)** – The deployment and use of traditional endpoint security software on smartphones and tablets trails PCs by a wide margin, despite attractive multi-device packaging by vendors of endpoint security software. As the IoT moves forward, the risk of compromise will surely rise. Yet, the prospect that the innumerable variations of device types in IoT will be inherently secure (e.g., via embedded security), or will buck the trend of mobile devices, and have after-market security software extensively deployed, is unlikely. A new approach to protect these devices from the risks of being Internet-connected, and likely connected 24x7, is needed. With effective instrumentation, management, and monitoring, secure pipes could be the type of low-cost and reliable means to protect literally thousands, if not millions or billions, of IoT devices at or near their point of Internet connectivity.

THE LAST WORD

The time has come to change the way that security is conducted. The era of "bolt-on" security solutions needs to come to an end, or at least be recalibrated. Built-in security should become the expectation. Customers are not looking to buy "products" such as broadband access or Web filtering. Customers are looking for a solution—i.e., clean and secure connectivity.

"Secure pipes" changes the conversation from a reactive security approach to one that is proactive. It addresses prevention in a more optimized manner, and includes what is needed, recognizing and appropriately responding to attacks and incursions that are designed to evade traditional defenses.

With secure pipes, the potential to have layers of complementary protection is possible: at the distributed edge or edges, and at a centralized gateway. Protection policies can be escalated to thwart attackers in a stepwise fashion. At the outer edge, general policies that yield high results in purging bad traffic with limited processing requirements and fast throughput are employed. As the traffic moves closer to the protected asset (e.g., a Web site), the policies become more sophisticated and require more processing resources, to trip-up attackers of more modest skills. At this stage, the throughput demands are less, as the volume of traffic to process is less than at the outer edge. Before reaching the protected asset, a final set of highly sophisticated and compute-heavy policies are used to thwart expert attackers. With this multi-layer approach, the development and deployment of policies is optimized for both security efficacy and resource optimization, to produce a balanced approach.

Overall, secure pipes improves an organization's cyber security posture. Organizations cannot do all security all the time by themselves. Secure pipes allows security professionals to begin from a quality security starting point, leveraging the network to provide a new and unique asset to improve cyber security.

Frank Dickson

Industry Principal – Information & Network Security
Frost & Sullivan
frank.dickson@frost.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Detroit
Dubai
Frankfurt
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mumbai
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Sarasota
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC