NetOptics
an ixia company

Fortifying Network Security with a Defense In Depth Strategy

White Paper

To battle today's sophisticated threats, organizations need the ability to deliver Defense In Depth—a layering of strategies and solutions that collectively protect against malicious attacks. Security-Centric SDN (Software Defined Networking), using multiple inline products, is the most effective approach to delivering that Defense In Depth protection. Point security solutions, although growing in effectiveness, are incapable of consistently, reliably thwarting intrusion and preventing the compromise of network security. That failure lays the network open to attack, with consequences spanning public endangerment, loss of personal and corporate assets, disruption of the social contract and deteriorating public confidence.

Regulators worldwide are mandating advanced protections and procedures to raise and tighten security levels. However, the network has grown to encompass social networking, remote access, and cloud computing. The resultant labyrinth of industry, national and local laws, added to the fact that many infractions result from third-party activities, makes compliance exceedingly complex. A defense strategy must take these and many more factors into account—performing effective monitoring and access control of the network without stifling the Internet's freedom of innovation and communication.

Deficits in Network Defense

As Niccolo Machiavelli said, "One who deceives will always find those who allow themselves to be deceived." The Internet is still learning how not to be deceived, and each incident is an expensive lesson. According to HP, the average cost now associated with a data breach in the United States is US $6.75 million. Laws created to regulate and control Internet relationships carry costly penalties of their own for infringement.

This unique situation is due to a number of factors, each one powerful in and of itself. The connected universe has become a wide-open field of opportunity for attackers to penetrate deep into organizational networks. However well-defended a system is, that is the degree to which it inspires ingenuity among the attackers. The problem cannot be bludgeoned out of existence; it must be treated as a chronic, mutating disease.

The speed of technological progress gives attackers an additional advantage, making a small, agile enemy capable of innovating faster than the organization under attack. "Asymmetric" conflicts such as guerilla attacks are paying off as never before, allowing attackers to quickly and cheaply expand their spheres of operation. The policies and procedures of a large organization, while making it accountable and substantial, also make it ponderous and bureaucratic. Implementing a new security strategy often takes too long to be effective when the need is urgent. Budget must be allocated; POCs completed, protocols followed. As well, even a newly purchased security solution can embody technology developed and acquired over time which may now be older than that of the attacker.

Today's "Internet of Things" creates a connected world where everyday objects like watches, smart TV, medical equipment, smart meters and industrial equipment become launch pads for intrusion. The consumerization of IT equipment and the standardization of interfaces, once considered an advantage, can now provide attackers reliable ingress. Confidential company data that was supposedly protected by state-of-the-art encryption, is now quickly shared via email, blogs and social media, putting the network at even greater risk.

When it comes to scale, protecting large networks is a greater challenge than protecting smaller ones. At the national-level, bulletproof network defense remains out of reach, just as it does with geographical borders. No number of TSA agents, magnetometers, scans, policing and other measures can hermetically seal a border and lock out those without permissions. In fact, such protection has proven to be rather easily evaded.

Because there is no "silver bullet" for preventing vulnerability, the best mechanisms for maintaining security lie with the network itself, utilizing the network's ability to combine, cascade and join multiple products agnostically to work in concert.

White Paper

The Choke Point of Security Measures

High levels of complexity and a rising number of nodes create a financial challenge for every organization; it seems there's never enough funding to provide cost-effective protection while simultaneously growing the business.

Looking again at the example of airports, it becomes apparent how an expanding security infrastructure can negatively affect revenue and productivity. It's been well publicized that the more procedures enforced by TSA, the longer the lines become. Adding more agents to handle them means making more space for them, equipping them with more inspection machines and so forth. Capital investment rises (as does customer dissatisfaction). Based on this comparison, when it comes to national-level network protection, any deployed measure is going to have an impact on scale and productivity. When building a security infrastructure, an organization's approach must:

- Meet current and future security challenges
- Meet current and future performance needs
- Address economies of scale
- Offer the 24/7 availability needed to respond instantly
- Bring to bear substantial resources to disable an attack
- Evolve as needed to promote security across a fast-changing network

Defense In Depth as a Network Protection Analog

Defense In Depth is a military concept whose principles are being applied to network security. Multiple levels of protection, layered into an IT system, can respond instantly and effectively if a security control fails or a vulnerability is breached.

A Defense In Depth architecture deploys multiple security solutions, including:

- Anti-virus software
- Authentication and password security
- Biometrics
- Firewalls
- Intrusion Detection Systems (IDSs)
- Logging and Auditing
- Packet filters
- Physical security
- Timed access control
- Security awareness training
- Virtual Private Networks (VPNs)
- "Sandboxing"

All of these resources work to fortify defense and reduce the impact of a breach. In our current environment of intense market competition, companies need high levels of agility to handle fast-arising threats. This need calls for a fresh perspective on infrastructure and operations that provides total visibility for a proactive response to these threats, or repair of the network before serious damages accrue. It's essential to harness application intelligence and visibility solutions to bolster network security and reinforce the ability to respond strategically to attack.

Building Security-Centric SDN

Security-Centric SDN marries an SDN controller with NPBs and a customer's chosen security solutions. NPBs, with their ability to "chain" solutions, integrate multiple systems, and distribute traffic, provide the ideal means for a dynamic defense. Such an architecture supports and enables Defense In Depth. It embodies dynamic attack monitoring; the use of NPBs for traffic distribution; and use of the network controller for assessing the network, provisioning SDN, and reacting to network activity. Under attack, Security-Centric SDN lets administrators quickly send orders that redirect data to forensics tools to expose and analyze an attack.

Out-of-Band—Out of Luck?

The out-of-band approach requires not just a separate network infrastructure but often a second networking vendor. An out-of-band device connects to the network in a way that lets it view all traffic passing through the equipment. Because it is not physically positioned between a sending and receiving device, it can actually increase risk. Also, it affects all user logins; therefore, failure of a server or controller can actually prevent users from logging in and create vulnerabilities when users log out. Out-of-band is also less scalable due to the necessity of reconfiguring network topology in order to deploy and maintain an out-of-band approach.

While inline devices can view and act on every packet to carry out intrusion detection and traffic monitoring, an out-of-band product depends on external systems for its functionality. The level of integration needed to convey host-state information hasn't yet been optimized, which limits integration. Since an out-of-band approach is also out of circuit, it offers no visibility into user traffic. A smart user would install an additional upstream IPS or other tool to even approximate inline security. In addition, an out-of-band solution may demand sensors, displays and reporting entities in order to approximate the security of inline monitoring.

Out-of-Band Risks

Out-of-band tools tend to be less effective and weaker than inline switch-based control. An inline device can conduct traffic shaping, catch attack command-and-control sequences, and detect inappropriate user access. So an additional out of band device actually can add latency and destabilize the network without adding compensatory value.

Out-of-band solutions provide only pre-connected security without the continuous post-connect security of inline solutions; therefore they are not effective against attacks such as spoofing and Man in the Middle (MITM). VLANs make it impossible to isolate users from one another; once a user resides in an authorized VLAN, that user's activities cannot be monitored by the security appliance. The user is free to attack in the authorized VLAN—or even the rest of the LAN. In-band appliances, on the other hand, can continuously block individual users from others on different access switches—even post-connect. This offers superior security overall and makes for easier resolution as well.

As the network becomes the primary resource for supporting its own health, an inline approach is emerging as the most effectual way to protect against intrusion. Previously, the choice between inline and out-of-band was roughly equal; but no longer. In fact, when contrasting online and out-of-band defenses, the comparison actually becomes quite lopsided.

The Advantages of Inline Monitoring-Based Security-Centric SDN

An inline strategy is the best way to carry out the mandates of Security-Centric SDN. Security-Centric SDN calls for an inline network architecture to because security today needs to be compatible, scalable and future-ready in order to anticipate threats and respond instantly to attacks.

Defense In Depth itself calls for inline security consisting of multiple systems working together and delivering instantaneous feedback for conducting forensics. These strategies combine, cascade and join multiple security solutions to work in concert transparently. Each component of this solution addresses respective risk factors and attack vectors.

The versatility of Network Packet Brokers (NPBs) is key to creating the fundamental Defense In Depth structure. Net Optics Security-Centric SDN calls on NPBs to integrate and focus disparate software and appliances. Each product addresses specific risk factors and attack vectors, layering and merging defensive tactics within the network to expand their power.

NPBs have the ability to integrate multiple products and systems seamlessly to unify this new security paradigm. Once united, these products can focus their combined strengths upon an attacking entity. This has proven to be the most effective way to provision the network with an advanced, available and agile defense.

Software Defined Networking is the enabling architecture of Security-Centric SDN, allowing for the easy addition of applications and streamlining of processes. SDN decouples routing and switching decisions from hardware and gives them to a software application called a controller, thereby reducing complexity, improving efficiency and providing a superior user experience. SDN centralizes and simplifies control of the network itself, increasing agility and enabling the automation and provisioning of monitoring applications and tools based on real-time traffic behavior.

SDN offers easy implementation and operation for end-to-end network monitoring, keeping data centers current with virtualization advances and secure cloud computing. With SDN, networks gain the agility to change behavior in response to threat level. In contrast, scenarios relying on static configurations remain the same under attack or in "peace time." In addition to enabling security, SDN helps reduce capital and operating expenditure, offering administrators an accurate view of network topology and usage, which can postpone upgrades and save on costs.

Inline Security: the Astute Approach

Inline security involves placing one or more appliances within the flow of network traffic—between the outer network environment and the proprietary network it protects, usually close to endpoint access—or even within the access layer switch itself. All client-side data must pass through this inline device, which serves as an enforcement point, as opposed to relying on another network system. Traffic to be screened passes through the device to be evaluated and, if certain criteria are not met, discarded. An inline solution can be a single box which acts as an internal firewall.

When it comes to achieving visibility and the ability to monitor, inline monitoring is increasingly the most practical, cost-effective approach to network security. Only the inline approach provides total, continuous visibility into all user activities and delivers user-based reports. Adding such advantages as persistent role-based monitoring and visibility as basic design features to an inline approach makes it even stronger. The best security is applied right at the point of entry to the network; ideally, this would be done using a secure switch with integrated pre-connect and post-connect security. However, for organizations not in the position to upgrade their access switches, an inline solution offers excellent, granular security.

Inline monitoring makes compliance straightforward, and avoids the VLAN steering that out-of-band solutions demand. (VLAN steering is a process that moves a user from one VLAN port to another. Besides being inconvenient, it adds to complexity because of the need to manage multiple VLANs in large environments.) Inline appliances provide fine-grained, identity-based access controls as a fundamental security feature.

Inline Reduces Expense and Complexity

An inline approach shelters infected or questionable users from one another, while an out-of-band solution struggles to quarantine noncompliant users within a VLAN—a cumbersome and possibly ineffective tactic. But evaluating cost really illuminates the comparative value of inline solutions. An inline solution works with the network as it is constituted, which means no heavy new investments or forklift upgrades; an out-of-band approach raises CAPEX for devices and controllers, puts pressure on operational costs and mandates upgrades of enforcement points. Thus, the inline approach offers a lower overall cost of deployment and management.

In most networks, an inline approach is simpler and more cost-effective, while an out-of-band approach calls for a lot more work and CAPEX just to stay in the same place. Each out-of-band device has its own management process and is burdened with the consequent issues that arise. Scaling also demands more costly capital investment.

The out-of-band user experience also tends to be more complex, with manual synchronization raising the need for administrators to become proficient on more devices. Login delays and confusion (i.e., out-of-band devices have difficulty supporting normal Microsoft boot and login sequences), plus the need to send SNMP traps to out-of-band controllers, obtain new IP addresses after VLAN changes and problems with devices such as IP phones with tandem POCs—all make the out-of-band approach a heavy commitment.

Robust Bypass Capabilities for Inline Availability and Continuity

Another major reason for an inline security approach; simply put is that it delivers an overall higher degree of certainty. Out-of-band is less certain when it comes to stopping the processing of identified malicious traffic. To ensure business continuity and network health then, inline is superior.

Net Optics now offers a powerful set of inline resources to extend the availability and security of the customer network. Both inline and out-of-band approaches use redundancy and failover for availability support, but inline provides the additional option of enforcing a default policy with basic access privileges.

Could an out-of-band solution approximate the advantages of iBypass? Out-of-band methods require that clients be given some access in order to evaluate compliance. The only way to check for compliance is to integrate the out-of-band product with the

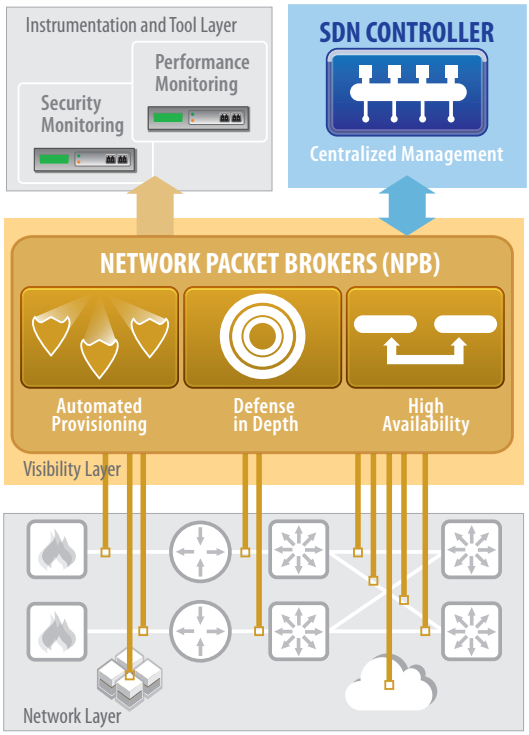
802.1X EAP processing (IEEE 802.1X is an IEEE Standard for Port-based Network Access Control. It provides authentication to devices attaching to a LAN or WLAN). Such integration would require an upgrade to the infrastructure as well as to the instruments at the endpoints, a very costly proposition.

Implementing Inline Security-Centric SDN in Your Organization

The Net Optics xStream™ Platform simplifies SDN integration, fortifies security and streamlines management. As an inline resource, this hardware and software platform offers scalability, high performance and seamless availability. The xStream Platform resides on a newly designed chassis with 24 ports or the equivalent of 64 10G ports—in one rack unit—for exceptional network productivity with an ultra-low latency 480G backplane for high visibility and performance. The xStream Platform merges three state-of-the-art products for quick link aggregation, network packet brokering and load balancing from a single platform. A flexible, scalable approach enables aggregation, regeneration, switching, and filtering of high traffic volumes with Deep Packet Inspection capabilities and extremely high port density. An expanded menu of commands ease configuration and control dramatically as well as delivering High Availability (HA) function to monitoring tools—a key benefit for networks under pressure for always-on performance.

The xStream Platform includes:

- **xStream 40**™ —a load balancing appliance for monitoring high-speed network traffic and easing migration to 40G. xStream 40 provides extensive NPB capabilities for 40G networks, including advanced filtering, aggregation, load- balancing, and time stamping. It offers a convenient way to perform 40G monitoring with existing tools and protects investment value while maintaining security and performance, boosting productivity and simplifying large-scale network management and network monitoring.
- **xBalancer**™—a purpose-built solution for distributing traffic to multiple monitoring tools, sharing the load caused by high traffic volumes, offering linear scalability and preserving the value of your tool investment.
- **Director xStream**™—a data monitoring switch that aggregates, regenerates, switches, filters, and load balances monitoring traffic. With the highest density of 10G ports in the monitoring industry, Director xStream empowers the NOC to share a pool of monitoring tools across a large number of network links.
- **iLink Agg xStream**™—a high-performance link aggregator that combines traffic from as many as 20 network links or Span ports and sends it to four monitoring tools.iLink Agg xStream speeds 10G traffic to 1G appliances, and 1G traffic to10G tools. iLink Agg xStream automatically performs all data-rate and media-type conversions, enabling 10G traffic to be sent to1G appliances, and 1G traffic to 10G tools.



Why a New Security Approach? Threats Are Growing in Frequency and Intensity.

Even a casual glance at the headlines reveals the growing severity of attacks and raises the question, is anyone safe? Surveys indicate that organizations, no matter how well-provisioned, have a lot of work ahead of them to protect at-risk information. Many have no overall information strategy in place at all, while others lack an integrated approach to information security.

October 3, 2013: Intruders steal the passwords of as many as 150 million users of Acrobat Reader and other Adobe apps.[1]

September 16, 2013: Cybersecurity professional hacks Nasdaq website: 'I needed 10 minutes'.[2]

August 27, 2013: New York Times is disrupted by hackers.[3]

March 27, 2013: Biggest DDoS attack in history slows Internet, breaks record at 300 Gbps.[4]

1. petapixel.com
2. nydailynews.com
3. nytimes.com
4. blogs.computerworld.com

White Paper

"Security is a Process, not a Product"

As organizations work to handle cloud challenges, consumerization, BYOD programs, mobility and virtualization, their greatest and most profound concern across all of these areas lies in thwarting cyber attacks. These have the potential to nullify all the progress and growth a company has worked to attain; steal their vital data and compromise their business goals. The current risk landscape demands an inline Security-Centric approach based on a Defense In Depth security model.

For further information about Net Optics' spectrum of security solutions, visit:

http://www.netoptics.com
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
United States
+1 (408) 737-7777
info@netoptics.com

Customer First!

Disclaimer: Information contained herein is the sole and exclusive property of Net Optics Inc. The information within this document or item is confidential; it shall not be disclosed to a third party or used except for the purpose of the recipient providing a service to Net Optics Inc. or for the benefit of Net Optics Inc. Your retention, possession or use of this information constitutes your acceptance of these terms. Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan attachments (if any).