Integrated Security Total Cost of Ownership Supports CIO Automation Objectives

At the top of every IT organization’s objectives are drives to move faster, contribute to business growth, operate more cost effectively and most of all, do it all securely. Traditional IT deployment approaches are no longer cutting it. With disruptive technologies like Software-Defined Networking (SDN) and Open Networking promising faster and more efficient deployments, Chief Information Officers (CIOs) are reevaluating their security options.

In the Fall 2014 meeting of the Open Networking Users Group (ONUG), a forum of industry IT leaders discussing and debating emerging trends in IT, two key messages emerged:

1. Network operational expenditure has to fundamentally change.
2. Business unit managers are demanding self-service IT provisioning.

Why Opex Expenses Grow so Rapidly for Traditional Multi-Security Implementations

Traditional networks use the “hard-shell-and-soft-core concept” (Figure 1, Phase 1); build a hard shell perimeter of firewalls and IPS equipment around IT assets that are soft on security services. The theory was “if something makes it in, it should be safe,” and emerging threats were often blocked by employing additional security layers. Sometimes these new layers could be implemented from the same vendor hardware and sometimes not, creating separate manually updated management portals for multiple security products.

Firewall, IPS, network antivirus, web security, and sandboxing are great security solutions, but each requires separate management. Adding each individually drives up Opex costs, adds complexity, and is slow. Each new appliance adds additional time, patching, maintenance, management, and procedures.

Automated security deployment and management from a single integrated display has a huge impact on Opex. It is well known that 80% of a network engineer’s time is spent performing manual configurations and change management. Policy changes on firewalls, building and provisioning new network resources, and testing off-line changes to the network consume the majority of operational time spent. On average, one network engineer can only manage 120 devices using these manual processes. Compare that to the 20,000 servers one engineer can manage, and it is clear that network infrastructure and its associated services, of which security is a critical service, need to automate. The issue remains how to deploy security policy changes with the same speed and accuracy.

The path toward an automated security infrastructure starts with the consolidation and integration of multiple security appliances, such as firewalls, IPS, antivirus, Anti-Bot, web security, sandboxing, etc., into a single integrated security fabric extending across the enterprise. More importantly, being centrally managed has an enormous impact on Opex (Figure 1, Phase 2). We call this Next Generation Threat Prevention (NGTP) in computer networking, and Check Point has long been considered the gold standard in integrated multi-site, multi-appliance security management.

In an integrated network security approach (Figure 1, Phase 2) such as Next Generation Threat Prevention, a security fabric provides automated control of threat mitigation tasks, such as firewall, IPS, network antivirus, web security, data protection, sandboxing, etc. It was brought to our attention that Check Point offers its Check Point 12600 and 13800 as one of the first Next Generation Threat Prevention, or NGTP, offerings.
One of the key attributes associated with a NGTP is that a single management system is used for configuration and change management across all security appliances. In Check Point’s case, it uses a SmartDashboard security management console that provides Security Operations (SecOps) a comprehensive user interface for defining and managing all security policies—from firewall security, VPNs, network address translation, web security, desktop security, antivirus security, SmartDefense threat defense protections, QoS and VPN client security. All object definitions (users, hosts, networks, services, etc.) are shared among all elements for efficient policy creation and security management.

Within SecOps, integrating multiple different security appliance management systems together creates a single policy. SmartDashboard provides a consistent user interface across all security appliances, reducing the time to manage multiple different security appliances as each application looks and feels the same. We found it quicker and more efficient to create a security policy in SmartDashboard and apply that policy across multiple security appliances than any other approach we have seen.

### Integrated Network Security: Faster Deployments, Lower Capex

To demonstrate part of the economic advantage of using one security appliance versus multiple appliances, we conducted a Capex TCO analysis. This analysis is not empirical. We performed a conservative Capex TCO projected analysis to demonstrate the economic advantage of using one security appliance versus multiple appliances. The analysis follows these assumptions:

- Three-year straight-line TCO analysis; no depreciation or amortization is applied.
- Multiple security appliances include firewall, IPS, web filtering, sandboxing, network and antivirus from multiple vendors.
- The NGTP security appliance is based upon Check Point 12600 and 13800.
- Capital, Maintenance and License fees are broken out.
- We chose company sizes based on 2,000 and 5,000 employees.

We found the NGTP solution offers an overall TCO savings of 41% and 53% for 2,000- and 5,000-user environments over a three-year period.
Understanding Total Cost of Ownership (TCO) Parameters for Next Generation Threat Prevention

**FIGURE 2. NGTP vs. MULTIPLE SECURITY APPLIANCES – 3 YEARS**

2,000 Users

- **NGTP Cost:** $309
- **Multi-vendor Cost:** $523

5,000 Users

- **NGTP Cost:** $437
- **Multi-vendor Cost:** $940

**Multi-vendor Cost Legend**
- Sandboxing
- Web Security
- Network AV
- IPS
- Firewall

**FIGURE 3. COST BREAKDOWN – 3 YEARS**

2,000 Users

**NGTP**
- License Fee: 69%
- Maintenance Cost: 23%
- Capital Cost: 8%

**Multi-vendor**
- License Fee: 30%
- Maintenance Cost: 21%
- Capital Cost: 49%

5,000 Users

**NGTP**
- License Fee: 65%
- Maintenance Cost: 26%
- Capital Cost: 9%

**Multi-vendor**
- License Fee: 32%
- Maintenance Cost: 21%
- Capital Cost: 47%
The NGTP approach also has a rather substantially lower acquisition cost than the multi-product solution approach (Table 1). In the three-year, 5,000-user scenario, the NGTP TCO is $437,470 versus $940,031 for the multi-vendor approach.

In the 2,000- and 5,000-user scenario example, the NGTP’s capital outlay as a percentage of TCO is 23% and 26% versus 49% and 47% for the multi-vendor point product solution, respectively (Figure 3). Capital costs are typically depreciated over a period of years while maintenance cost and license fees are expenses paid or incurred annually, offering potentially favorable tax implications.

While we report a three-year analysis here, we also captured and analyzed one-year data. The one-year and three-year 2,000-user scenario TCO for NGTP is $139,184 and $309,302 versus $391,504 and $523,517 for the multi-vendor approach, respectively (Table 2). NGTP also scales better from a cost point of view as the cost per user actually decreases as the number of users increase. In year three, NGTP’s 2,000- and 5,000-cost per user is $154.65 and $87.49, respectively—dropping approximately 43% (Figure 4). Based upon this analysis, the NGTP approach offers a lower entry point that stays lower as the years and number of users increase.

### TABLE 1. 3-YEAR COST ANALYSIS OF 2000 USERS VS. 5000 USERS

<table>
<thead>
<tr>
<th>Security Model</th>
<th>2,000 Users – 3-Year Analysis</th>
<th>5,000 Users – 3-Year Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Cost</td>
<td>NGTP $70,700</td>
<td>NGTP $112,000</td>
</tr>
<tr>
<td></td>
<td>Multiple Vendors $257,795</td>
<td>Multiple Vendors $445,195</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>NGTP $25,452</td>
<td>NGTP $40,320</td>
</tr>
<tr>
<td></td>
<td>Multiple Vendors $110,862</td>
<td>Multiple Vendors $199,626</td>
</tr>
<tr>
<td>License Fee</td>
<td>NGTP $213,150</td>
<td>NGTP $285,150</td>
</tr>
<tr>
<td></td>
<td>Multiple Vendors $154,860</td>
<td>Multiple Vendors $295,210</td>
</tr>
<tr>
<td>Total Cost of Ownership</td>
<td>NGTP $309,302</td>
<td>NGTP $437,470</td>
</tr>
<tr>
<td></td>
<td>Multiple Vendors $523,517</td>
<td>Multiple Vendors $940,031</td>
</tr>
</tbody>
</table>

### TABLE 2. 1 YEAR VS. 3 YEAR VS. PER YEAR TCO TABLE

<table>
<thead>
<tr>
<th>Security Model</th>
<th>2,000 Users</th>
<th>5,000 Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Cost</td>
<td>NGTP $139,184</td>
<td>NGTP $209,440</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor $391,504</td>
<td>Multi-vendor $699,952</td>
</tr>
<tr>
<td>Maintenance Cost</td>
<td>NGTP $25,452</td>
<td>NGTP $40,320</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor $110,862</td>
<td>Multi-vendor $199,626</td>
</tr>
<tr>
<td>License Fee</td>
<td>NGTP $213,150</td>
<td>NGTP $285,150</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor $154,860</td>
<td>Multi-vendor $295,210</td>
</tr>
<tr>
<td>Total Cost of Ownership</td>
<td>NGTP $309,302</td>
<td>NGTP $437,470</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor $523,517</td>
<td>Multi-vendor $940,031</td>
</tr>
<tr>
<td>Per-year TCO</td>
<td>NGTP $103,101</td>
<td>NGTP $145,823</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor $174,506</td>
<td>Multi-vendor $313,344</td>
</tr>
</tbody>
</table>
**Recommendation and Closing**

Even from only a Capex equipment standpoint, NGTP is one half to one-third the cost of traditional multi-vendor security implementations according to our TCO calculation. A more in-depth TCO analysis that considers the impact of reduced headcount needed for operational configuration, management and maintenance would find a much larger difference. Empirical TCO studies that we have previously conducted find operational cost tends to be the dominant cost component, by as much as 70%.

NGTP offers a means to lower operational cost by employing an integrated security appliance management approach for policy creation, device configuration and change management, forensics analytics, auditability and much more. Check Point's SmartDashboard is a proven path to lower operational cost and faster IT delivery. Network deployments can only be as fast as its slowest part. Without an NGTP approach like Check Point's and its use of SmartDashboard, the speed and efficiency promise of SDN and Open Networking will never be fully realized (*Figure 1, Phase 3*).
About Nick Lippis

Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is the publisher of the Lippis Report, a resource for network and IT business decision makers to which over 35,000 executive IT business leaders subscribe. Its Lippis Report podcasts have been downloaded over 200,000 times; iTunes reports that listeners also download the Wall Street Journal’s Money Matters, Business Week’s Climbing the Ladder, The Economist and The Harvard Business Review’s IdeaCast. He is also the co-founder and conference chair of the Open Networking User Group, which sponsors a bi-annual meeting of over 400 IT business leaders of large enterprises. Mr. Lippis is currently working with clients to design their private and public virtualized data center cloud computing network architectures with open networking technologies to reap maximum business value and outcome.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, the state of Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cisco Systems, Hewlett Packet, IBM, Avaya and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply- and demand-side clients.

Mr. Lippis received the prestigious Boston University College of Engineering Alumni award for advancing the profession. He has been named one of the top 40 most powerful and influential people in the networking industry by Network World. TechTarget, an industry on-line publication, has named him a network design guru while Network Computing Magazine has called him a star IT guru.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press. He serves on the Dean of Boston University’s College of Engineering Board of Advisors as well as many start-up venture firms’ advisory boards. He delivered the commencement speech to Boston University College of Engineering graduates in 2007. Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters’ thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.