Adaptive Network Security
Sales Training – Indirect Channel Partners

Randy Tucker (moderator) Marketing Manager
Dominique Singer (main presenter) – Sales Director, Security Solutions CISSP CISM CRISC GSEC Gold
Beth Kohler (product specialist) – Senior Director, Product Management
Agenda

• Marketplace – Forces Driving Customer Needs
• CenturyLink Vision for Security & Portfolio
• CenturyLink Adaptive Network Security – What It Is and Does, Use Cases
• How to Sell Adaptive Network Security – Simple Bundles & Pricing
Market Drivers, CenturyLink’s Vision and Approach to Security
Marketplace Forces Driving Customer Needs
Businesses Challenged by Accelerating Change

<table>
<thead>
<tr>
<th>Today - Digital Transformation:</th>
<th>Our Customers Tell Us They Need:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networks are becoming more complex and the traditional network perimeter is evolving, increasing complexity and risk</td>
<td>Consistent protection across their network with centralized uniform policy management and local security gateways</td>
</tr>
<tr>
<td>Security costs are growing exponentially and there is a scarcity of in house security expertise</td>
<td>Uniform security posture and self service capabilities for ease of management, better control and a lower total cost of ownership</td>
</tr>
<tr>
<td>Rising cybersecurity threats to business functions, compliance and regulatory requirements</td>
<td>Visibility into the threat landscape, proactive notification and ongoing governance, and provider responsiveness</td>
</tr>
</tbody>
</table>

These complex challenges intersect with CenturyLink investments, expertise, and capabilities
CenturyLink Security Vision

To cost effectively and efficiently secure people, data, and things with an adaptive security ecosystem as they transition from premises-based to cloud-based solutions.
CenturyLink Leadership in Cyber Threat Intelligence, Analysis & Defense

We monitor ~1.3 billion Security events per day

We respond to and mitigate ~120 DDoS attacks a day

We identify over 267 and remove 35 new C2s a month

We monitor over 114 billion NetFlow sessions per day

We track over 5,000 C2s per day

We collect ~357 million DNS queries per day
CenturyLink Security Services

NETWORK SECURITY SERVICES
- Adaptive Network Security Services
- DDoS Mitigation Solutions

PROFESSIONAL SECURITY & CONSULTING SERVICES
- Strategy, Risk & Compliance Services
- Network & Application Security Consulting
- Security, Vulnerability, and Penetration Assessments

PREMISES SECURITY SERVICES
- Managed Firewall
- Managed IDS/IPS

ANALYTICS AND THREAT MANAGEMENT SERVICES
- Security Log Monitoring & Management Service
- Adaptive Threat Intelligence Service
- Incident Management & Response Service
The Defense: Layered Complexity

InfoSec in Practice

- Email
- DLP
- Web
- Operations
- Alerts: SIEM
- Log sources
- Anti-Virus
- App Control
- Firewall
- Encryption
- Malware Control
- File Integrity
- Host IPS
- Firewall / IPS Manager
- WAFs
- Syslog
- Databases
- Servers
- Endpoint Security Manager
- Risk, Threat, Vulnerability Management
- Policy, Process and Implementation
Deploying a Multi-Layered Security Approach

PREVENTIVE MULTI-LAYERED SECURITY

- Managed Firewall
- Application Awareness and Control
- Intrusion Detection and Prevention
- Web Content / URL Filtering
- Anti-malware (Sandboxing)
- Data Loss Protection
- Two-Factor Authentication

LOGGING, ANALYTICS AND INTELLIGENCE

- SIEM Integration
- Security Analytics / Threat Intelligence
- Security Alerts with Controls

Application Awareness and Control identifies, reports, and enforces applications on the network.

Anti-malware scans, blocks, and reports on malicious code found in network traffic.

Sandboxing places unknown anomalous payloads in a protected environment for observation. If the payload acts malicious, a signature is created and pushed to Gateways to detect and mitigate future threats.

Web Content Filtering service controls how Internet resources are used based on URL, Content, or IP address.
- Inspect and block downloaded website content for malicious code before it reaches users.
- Integrate with Active Directory server for granular policy definition and reporting.

Data Leak Protection monitors, prevents, and reports on attempts to send sensitive data.

Threat Intelligence correlates traffic against known malicious communication utilizing FortiGUARD and supported by CenturyLink proprietary analysis and threat data.

CenturyLink® Professional Security Services

CenturyLink Global Security Operations Centers

CenturyLink® Threat Research Labs

© 2018 CenturyLink. All Rights Reserved.
CenturyLink Adaptive Network Security
Designed for Digital Transformation

Traditional Internet Access Through VPN

Centralized Model With Adaptive Network Security

Traditional Premises Security Model
CenturyLink Adaptive Network Security
Designed for Digital Transformation

Value Differentiators and Features:
- Co-located in high Peering locations
- Carrier Agnostic Solution (BYOB)
- Carrier-Grade Global deployment
- Logging and reporting to portal
- 24/7 Global Security Operations

SIMPLIFY MANAGEMENT
A centralised platform, with around-the-clock protection from CenturyLink’s highly trained security engineers

IMPROVE SECURITY
Next-generation cloud firewall that leverages CenturyLink’s unique network to bring security closer to threat

REDUCE COST
Lets you move from a Capex-heavy security model to a more efficient Opex-based charging model.

INCREASE EFFICIENCIES
Adopt carrier agnostic, network based protection with flexible commercial models and access options
Global Platform for Digital Change Security

North America (11)
- Boston
- Chicago
- Dallas
- Las Vegas
- Los Angeles
- Miami
- Phoenix
- San Diego
- San Jose
- Seattle
- Washington DC

South America
- Bogota
- Buenos Aires
- Sao Paulo

EMEA (16)
- Amsterdam
- Barcelona
- Brussels
- Copenhagen
- Dusseldorf
- Frankfurt
- Johannesburg
- London
- Manchester
- Marseilles
- Milan
- Oslo
- Paris
- Sofia
- Stockholm
- Warsaw

APAC (3)
- Hong Kong
- Singapore
- Sydney
Adaptive Network Security – Target Buyer, Use Cases and Case Studies
Security Solutions: Target Buyer

Elevator pitch: CenturyLink Adaptive Network Security is a network-based suite of protections against an increasingly complicated threat landscape. It forms the basis of a secure network solution that brings multiple sites into one holistic platform, leverages Bring Your Own Bandwidth (BYOB), and is available regionally, nationally, and globally.

<table>
<thead>
<tr>
<th>Business challenges:</th>
<th>Business challenges:</th>
<th>Business challenges:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Recruiting and retaining skilled in-house Security expertise</td>
<td>- Increased public awareness of cybersecurity risk, and associated damage to reputation in the event of a major public breach</td>
<td>- Simplified security architecture to manage and fewer technologies to learn/train</td>
</tr>
<tr>
<td>- Growing threat to organisations from the ever changing threat landscape</td>
<td>- Reducing operational complexity and associated costs</td>
<td></td>
</tr>
<tr>
<td>- Addressing the skills gap</td>
<td>- Wider adoption of Cloud based applications and how to secure them</td>
<td></td>
</tr>
</tbody>
</table>

INFLUENCER: IT Manager

Chief Information Security Officer (CISO)

Chief Information Officer (CIO)
Adaptive Network Security Use Cases

The Adaptive Network Security Bundles include 3 Standard, scalable Use Cases.

The Use Cases are “Building Blocks,” and can be combined to deliver services in-region, nationwide, and globally.

Standard Use Cases:

1) TO Internet FROM MPLS
2) TO MPLS FROM Internet
3) Secure Internet FOR Remote offices
Use Case #1 – Securely To Internet from MPLS/IPVPN

- Customer Sites can be directly connected or use remote access to fLVLT VPN
- Only supported with fLVLT MPLS/IPVPN product
- Replaces legacy SIA functionality

Scenario: Customer wants all inbound/outbound Internet traffic to go through their fLVLT VPN (Internet Drain)
Use Case #2 – Remote Site to MPLS/IPVPN from Internet

Remote Site to MPLS

Scenario: Customer wants to connect to their fLVLT MPLS/IPVPN network from a location that has a BYOB Internet Connection

- Remote sites connect to Customer MPLS/IPVPN without purchasing MPLS/IPVPN!
  - Secured with IPSec and any broadband connection
- Provides backup method into MPLS/IPVPN if primary MPLS/IPVPN access fails
- All Inbound and outbound communications protected by Adaptive Network Security
- Only supported with fLVLT VPN product definition
Use Case #3 – Securely TO Internet FROM Internet

- Bi-Directional traffic inspection and Security Policy Enforcement
- Remote Sites connect to Adaptive Network Security over the Internet using IPSec
- Ideal for Customer migrating from CPE security solution to Cloud
- Can be sold with any Internet connection (CenturyLink or third party)

Scenario: Customer wants a cloud firewall approach to secure locations with Internet connectivity.

- To avoid a bottleneck issue (and low or no bandwidth issues at a site), Adaptive Network Security bandwidth should cover the aggregate bandwidth for ALL sites combined.
Financial Services Company: Case Study
Improving Risk Management

Customer:
Financial Services Company

Situation
The customer had disparate network assets that were expensive to maintain and secure. They suffered through several publicized cyber attacks, and review of their infrastructure revealed susceptibility to significant data and revenue losses.

CenturyLink Solution
• Deployed a single MPLS/VPN network with internet connectivity to remote locations to efficiently and cost-effectively connect ~90 sites
• Standardized security policy management and local security gateways
• Deployed DDoS Mitigation to protect critical sites and internet circuits
• Improved ease of management with central security policy control and visibility
Customer: Media Organization

Situation
The organization suffered from a conglomeration of networks, firewalls and security solutions due to ongoing merger and acquisitions. They required network consolidation and a uniform security posture for ease of management, lower costs, better control and increased visibility.

Solution
• Consolidated into a single MPLS network
• Provided cloud-based protection with centralized policy management and local security gateways
• Enhanced security posture with no impact to operations, no capital expense and no additional in-house staff
• Delivered visibility into the threat landscape
Adaptive Network Security Bundles Overview and Selling Points
Sales Enablement “Lever” for Partners and Channel Managers which includes:

- Pre-defined Feature Packages
- Three primary Use Cases
- Pre-defined Technical Scope
- Pre-defined Sizes

* Partners are not restricted to pre-defined sizes. Adaptive Network Security supports up to 3Gbps per Gateway, per Customer
Bundles of Standard Features + Size

- **Essential**: Adaptive Network Security Firewall with IDS/IPS
- **Enhanced**: Essential + Web Content Filtering
- **Comprehensive**: Enhanced + DLP, Application Control, Anti-Malware Sandboxing

**Size** is Aggregate Bandwidth required at each Gateway; Design “Building Blocks”

- **15M = Small** (e.g., 3 sites requiring 5M Internet Access)
- **150M = Medium** (e.g., 10 sites requiring 15M Internet Access)
- **300M = Large** (e.g., 10 sites requiring 30M Internet Access)
Why Sell Adaptive Network Security?

• **MRC commission based product!**

• **Logical fit with network services**
  - Foundation for a secure network solution
  - Highly-scalable platform for local, national, global networks
  - Networks with multiple Internet providers (bring your own bandwidth) are supported!

• **New Dedicated Security Sales support**
  - You don’t have to be a security expert. Let us be the experts. Initiate the initial conversation with customers, CenturyLink will provide expertise and ‘right size’ the solution based on customer needs.
  - Exclusively Channel-focused Sales and Architecture team
Why Choose CenturyLink?

- **Broad Global Coverage**
  - Proximity to customer improves latency
  - Localized gateways allow regional support

- **Ease Of Deployment**
  - No client software is required
  - Efficiently layer new technologies in a network-based environment (cloud)

- **Flexible Connectivity Options**
  - Supports GRE, IPsec, IP VPN
  - Hybrid on-premises and cloud-based deployments

- **Breadth of Next-Generation Technology Options**
  - Comprehensive suite of optional services
  - Based on best-in-class next generation firewall technology

- **Increased Efficiencies**
  - Cloud-based protection with flexible commercial models

- **Comprehensive Visibility and Control**
  - Centralized policy management with visibility through a consolidated portal
  - Supported by CenturyLink® Threat Research labs and the SOC
Resources and Sales Enablement Collateral
Resources and Sales Enablement Collateral

Please see the Partner Portal or Access Alliance under Products > A-Z List > Security Services - Detect & Respond Services

- Adaptive Network Security Bundles Sell Sheet
- A recording of the Adaptive Network Security “Ask the Experts” Webinar (available soon)
- Mammoet Case Study
Q & A Session

More Info: IndirectSecuritySales@Centurylink.com
High Level Process Flow – Shop, Buy, Get, Use, Pay, Renew

- Customer receives invoice from CenturyLink
- Customer calls CenturyLink directly, Indirect Partner is not contacted
- Indirect Partner provides quote to customer. Proposal – customer receives proposal from CenturyLink Channel Manager Team
- CenturyLink Service Delivery (provisioning/implementation) and Service Assurance (Operations) will reach out to customer. Indirect Partner is usually not involved.
- Indirect Partner and/or Channel Manager engage CTL Indirect Security Sales
- Customer receives invoice from CenturyLink
- Customer renews through Indirect Partner
- Indirect Partner and/or Channel Manager engage CTL Indirect Security Sales