Telco Systems
A BATM Company

Protecting SDN and NFV Networks from Cyber Security Vulnerabilities

A WHITE PAPER FROM TELCO SYSTEMS

Telco Systems
A BATM Company

Contents

Introduction

All around the world, telecommunications operators and service providers are excited about the opportunities that Software Defined Networking (SDN) and Network Functions Virtualization (NFV) promise to provide. Through these technologies, end customers – enterprise organizations – can move many of their networking functions to the carrier network. For the enterprise, this represents an opportunity to reduce their IT expenses by reducing complexity. For telcos and service providers, the opportunity lies in providing more valuable services to their customers, thus transitioning from primarily delivering connectivity to delivering much more lucrative smart managed services.

Although operational use of these software-centric technologies in this industry is still in early stages, many providers are actively testing and evaluating solutions in their labs and formulating their strategies for deployment. Leading companies such as AT&T, BT and NTT Communications have whetted the broader industry's appetite for these emerging technologies through their success with actual use cases and by showing that the benefits are out there. For its part, AT&T has said it "aims to embrace SDN and NFV to improve the value of its network by driving improved time-to-revenue; providing cost-performance leadership; enabling new growth services and apps; ensuring world-class, industry leading security, performance and reliability; and facilitating new business and revenue models."[1] Indeed, AT&T is already offering multiple services to end customers based on its SDN/NFV adoption.

AT&T is certainly not alone in its pursuit of those benefits. Industry pundits believe that for many operators, deployment is a matter of when, not if. According to the OpenStack Foundation, 60% of telecommunication professionals are actively exploring NFV. [2] SNS Research estimates that by 2020, SDN and NFV will enable service providers (both wireline and wireless) to save up to $32 billion in annual CapEx investments.[3] And while individual operators could potentially save significantly on their capital expenditures, deployment isn't strictly about cost reduction. Even more enticing is the opportunity for new business and revenue models as operators provide higher value services to their customers.

SDN/NFV represents a new paradigm for service providers. The traditional networks that are still dominant today are built on infrastructures with closed platforms and proprietary equipment—just as they have been for the last few decades. However, operators that begin to adopt SDN and NFV will encounter technologies that are much more IT-like, built upon open source software and white box hardware. This opens the network to vulnerabilities that didn't exist before.

SDN and NFV present several challenges and risks from a cyber security perspective. These challenges aren't showstoppers, but rather just something to work through. Service providers' network security experts who are already working with the new technologies say the challenges are worth solving, and the risks worth mitigating, because the ultimate rewards of utilizing SDN and NFV are so compelling.

Telco Systems is working toward solving those cyber security challenges with a comprehensive solution that provides specific security measures to address the specific software defined infrastructure security holes. This paper outlines the concerns that operators' security experts have and describes the Telco Systems NFV CyberGuard solution now in development to address them.

The goal of NFV CyberGuard is to protect SDN and NFV based networks from cyber attacks on the network topology and data flow, and from other attacks relating to control and management planes.

NFV CyberGuard benefits to service providers are:

- Quickly detect and analyze advanced topology, flow and NFVi attacks
- Maintain uptime and performance of network and NFV services and minimize SLA penalties
- Reduce the costs resulting from data theft
- Ensure network consistency and availability resulting from human errors or self-service provisioning
- Rapidly deliver NFV services, increasing revenue from value-added services

[1] Signals and Systems Telecom, "The SDN, NFV & Network Virtualization Bible: 2014-2020," October 2013
[2] OpenStack Foundation report, " Accelerating NFV Delivery with OpenStack," January 2016
[3] Signals and Systems Telecom, "The SDN, NFV & Network Virtualization Bible: 2014-2020," October 2013

Network Functions Virtualization (NFV) and Software Defined Networking (SDN) complement each other, but solve different problems in different environments across different domains. SDN emerged to make network devices programmable and controllable from a central element. NFV is aimed at accelerating service innovation and provisioning using standard IT virtualization technologies. SDN requires new interfaces, control modules, and applications, while NFV typically involves moving networking applications to virtual machines (VMs) or containers that run on commodity hardware. NFV is highly complementary to SDN, but not dependent on it (or vice versa), although the two concepts and solutions can be combined and potentially greater value accrued.

Source – OpenStack.org

The Cyber Security Challenges of SDN and NFV

Traditional telecom networks are based on closed operating system infrastructures that can be effectively protected from hacking and other attacks. Migrating to SDN and NFV technologies for next generation network infrastructures offers benefits like openness, remote programmability, agility and other advantages of IT-like networks. However, the similarity to IT networks that makes SDN/NFV networks advantageous for communications service providers also makes them vulnerable to the full range of cyber attacks that target IT networks.

From NFV to Distributed-NFV

Initial NFV deployments in the telecom industry were similar to SaaS and cloud computing where all virtual functions would be placed at the data center to optimally utilize computing resources across applications and users. However, certain NFV use cases, such as virtualization of the customer premise equipment devices (vCPE), dictate that specific functions be placed on customer sites and/or on demarcation devices. The main considerations regarding placement at the network edge and customer perimeter access are security, performance, gateway functionality and quality of experience.

Protecting the customer network and data as well as providing end-to-end encryption and VPN require placement of the security function at the entry point to the customer network. Internal network traffic should remain local and not be sent to distant routers, which would result in high latency and increased utilization of the customer line. Gateway functionality such as session border controller (SBC) requires a device or function connecting the customer network and the carrier network. Quality of experience solutions for service activation, monitoring, and policy enforcement are effective only if measured and enforced over the entire route and all devices.

Figure 1 below illustrates the Distributed-NFV model, where virtual functions reside on CPE devices as well as other devices throughout the network: demarcation, aggregation and in the data center.

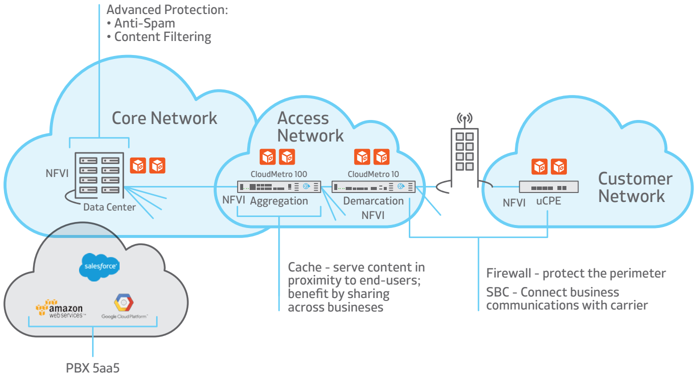

Figure 1: The Distributed-NFV model

The Potential and the Pitfalls of OpenStack for Telecom Networks

As network technology moves from proprietary single-purpose devices to computed elements with network functions provided as virtualized services (virtual network functions, or VNF) and which use open protocols like Linux, OVS and OpenStack, the infrastructure becomes exposed to cyber threats.

Consider OpenStack, for example. This open source software platform has become the de facto standard for cloud computing architectures for the data center, especially infrastructure-as-a-service (IaaS) deployments. For many enterprises, it is the preferred architecture to enable compute, network and storage with unlimited capacity and scalability without the costly overhead and hardware commitment requirements of the old data center model. Among the strengths of OpenStack are seamless scaling, interoperability and connectivity across vendors and networks, and cloud automation.

Recently, many heavy hitters of the IT world have made significant investments in OpenStack because they believe there are enterprise-class capabilities that aren't readily available with other architectures.

This has hastened the maturation of the platform to meet the demands for large, scalable data center cloud solutions.

The question is whether OpenStack is an appropriate technology stack for the telecom industry. According to Peter Willis, Chief Researcher of Data Networks at British Telecom, "OpenStack is seen as the strategic industry direction for managing cloud computing platforms, and since NFV is similar to cloud it is important we investigate reusing this technology." But there's a hitch to this proposition: OpenStack, as it is today, is not fully suited for Distributed-NFV.

OpenStack was created as a data center/cloud platform. As such, it assumes that both the OpenStack controller (which is managing and provisioning the OpenStack compute nodes) and the OpenStack compute nodes (which are running the VMs) are on the same network and in short proximity. However with Distributed-NFV, the compute nodes are outside of the core (as illustrated in Figure 2), which requires the operator to loosen the security rules between the controller and the compute nodes (from the core network to the access network). This slackening of the security causes some risks and challenges that must be addressed before OpenStack is suitable for telcos and service providers.

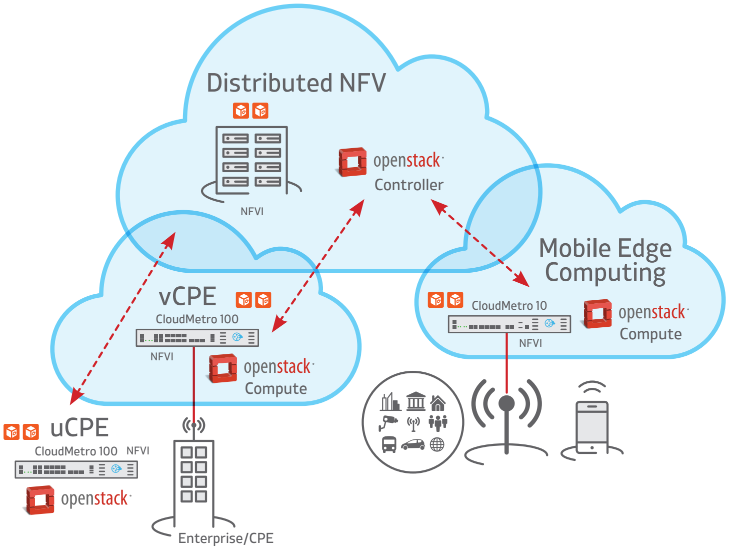

Figure 2: Security challenges with Distributed-NFV

All the OpenStack controllers need to run specific protocols, and rules in the firewalls must be configured in order to manage the flows. According to Peter Willis, BT did intensive tests of OpenStack where the company connected a compute node over the Internet to a controller in its NFV lab. This represented a realistic scenario for vBranch. They found that over 500 pinholes had to be opened in the firewall in order to allow the architecture of the distributed OpenStack to work. Clearly this type of architecture is one of the major challenges when speaking about how to protect and secure the NFV infrastructure.

The Main Security Challenges

The telecom industry research group Heavy Reading conducted a survey in April 2015 to ask service providers about their security concerns posed by various aspects of network virtualization. Among survey respondents who self-identify as security experts, 50% consider "security vulnerabilities in the hypervisor" to be a very high risk. None of the security experts rate this factor to be merely a low risk. Another major concern of this seasoned group of security professionals is "giving customers access to network resources via APIs"—yet this is the principle goal of allowing end customers to provision network resources for themselves. Clearly these are among the security risks that must be mitigated when migrating to the next generation network.

The main risks are categorized in four areas:

- Both the data plane and the control plane management are now in software and not hardware based microchips (application-specific integrated circuits, or ASICs). This software is much more vulnerable to denial of service (DoS) and distributed DoS (DDoS) attacks.

In the traditional environment, operators have devices or appliances that are dedicated to one task. The equipment usually contains some pieces of hardware that were created specifically for a single purpose or were optimized for that purpose. For example, on a switch, router or firewall, there might be an ASIC such as a packet processor that can provide a line rate or wire speed performance. It is very effective and very focused on the actual packet processing or, for example, on applying access lists on a firewall. These appliances containing these ASICs, network processors or other types of hardware are very stable. They are very good at handling peaks and increases in traffic and it's hard to break them by overloading them.

Now with NFV, the approach is to take the functions of the physical appliances and run them in software on an ordinary Intel CPU. Now, because the functions are running in software, they are much more vulnerable to increasing traffic loads—specifically the high volume loads that exist in DoS and DDoS attacks. It's much easier to make the software based devices fail when there is a significant increase in load.

- The control and management planes of each device and each function are open for remote operations as well as user self-service.

In a traditional environment, the control plane allows for the service provider to provision and control the hardware devices and appliances. However, the control plane is largely predefined and has only a few options to be configured; for example, to change some rules on a device. Now with SDN and also with NFV, an entire SDN device or NFV host can be programmed by an external controller. This provides the opportunity for those devices to be taken over by a malicious actor.

A second aspect is that some of the services are becoming self-service. In this mode, the end customer can go onto their exclusive portal and, for example, increase bandwidth on demand, or add a virtual function such as a firewall. These orders go to an orchestrator that controls and orchestrates the devices. This means that there is a connection between outside of the carrier world that goes up to the subscriber or user world that allows control of the network. This is another vulnerability or pinhole that can be exploited by attackers.

- Once a malware resides on the network (inside the perimeter), it propagates easily across VMs and hosts as there is no mechanism to monitor it.

In today's security schemes, much of the protection is applied at the perimeter. For example, there is a firewall or some other type of advanced protection that controls what goes in and out of the carrier network. Even with perimeter protection, it's possible that the network can become infected with some malware that might be harmful or might allow an unauthorized person to get access into the network.

The challenge with NFV is that now the entire network is made by hosting machines that run a virtualization environment. What's more, the virtual machines reside all over the network, from the data center out to customer premises, and in mobile sites as well. Compared to the traditional network environment where most of these devices are single-purpose and well hardened, now these devices are actually servers and they run in the virtualization environment. Each host actually has a virtual network that resides on it – a virtual switch – and the whole network is connected. Virtual machines are pieces of software that are frequently being instantiated (i.e., turned on and off). In this way malware software can propagate itself throughout the network by jumping from one virtual machine to another or from one virtual machine on one host to many other hosts.

- Each host has many VMs, and each represents a pinhole for attack and propagation of infectious items.

This is a security issue we discussed earlier, with the BT testing of Distributed-NFV in its lab. Connectivity openings need to be made in the virtual devices to allow them to communicate and for normal traffic to flow as needed. Each of these openings is a pinhole into the network through which malware can flow.

The diagram in Figure 3 demonstrates the threats on the data, control and management planes based on the interfaces across the planes:

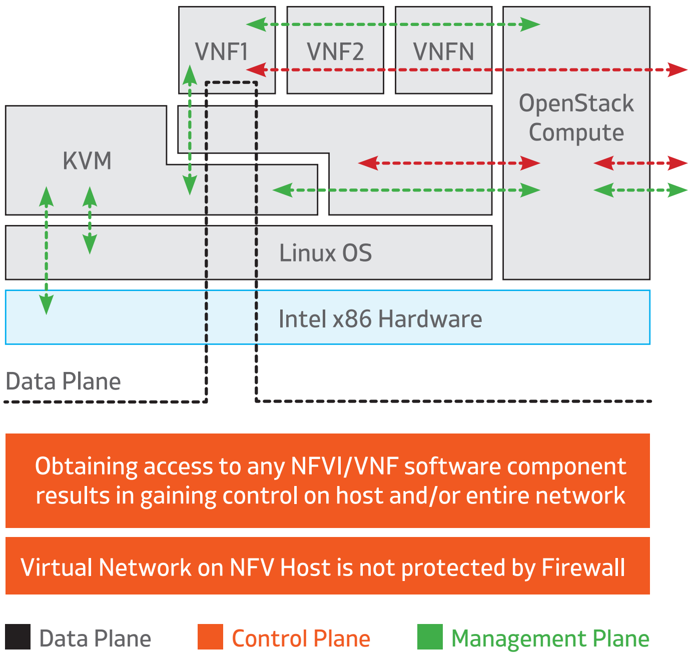
VNF1
VNF2
VNFN
OpenStack Compute
KVM
Linux OS
Intel x86 Hardware
Data Plane
Obtaining access to any NFVI/VNF software component results in gaining control on host and/or entire network
Virtual Network on NFV Host is not protected by Firewall
Data Plane
Control Plane
Management Plane

Figure 3: Threats based on traffic traversing the planes

To address these cyber security risks, the industry needs solutions that are able to handle the vulnerability, not only when it comes into the network but also assuming malware can already be present on the network. Security solutions need to be able to look at the points where malicious code can copy itself or communicate with the outside, which is on the NFV infrastructure; the layer that allows the virtualization, which is the hypervisor; the virtual switch, and so forth.

Telco Systems' Approach to Cyber Security

Telco Systems is working to address the specific cyber security challenges of SDN and NFV. The solution in development is NFV CyberGuard. The objective of the NFV CyberGuard solution is to protect SDN and NFV Infrastructure from control plane related attacks once the perimeter protection has been compromised. Perimeter based detection and prevention such as firewalls and intrusion prevention systems (IPS) are critical elements in IT security. Perimeter protection is frequently breached with zero day attacks, email based malware, download, physical upload (such as from USB) or other attack vector. The combination of such attacks together with the openness and dynamic nature of SDN and NFV brings new and unknown types of attacks to service providers and their customers. While firewall and IPS provide the first line of protection, NFV CyberGuard empowers threat detection and prevention on the second and third lines of the protection. The second line is the virtual network and its flows and the third line includes the VNFs and the inter-flows of VNFs.

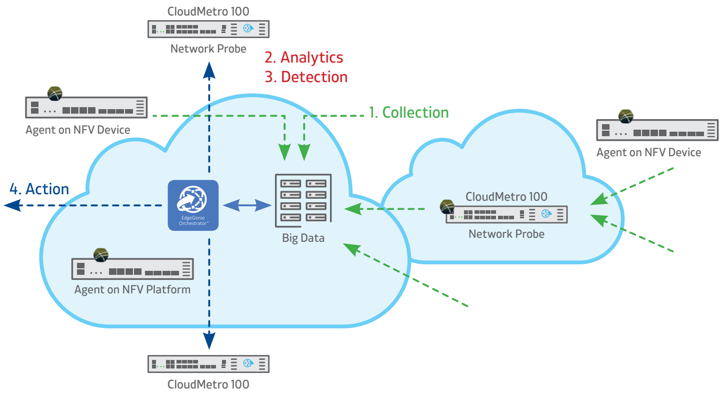

Figure 4: The NFV CyberGuard Solution

The CyberGuard dashboard is a web based and cloud based application displaying a summary of the open threats by type: critical and total. It also shows a list of most recent and most critical events:

- Threat Type
- Date & Time
- Severity
- Threat Highlights

The solution constantly monitors the virtual networks' control and management planes, their data flows and other APIs as well as other SDN and NFV infrastructure components. This information is used to build baselines of normal activity by network segment, service, VNF, chain of VNFs, users, and other characteristics. Baseline may be also a typical random behavior of users. NFV CyberGuard analytical engine utilizes behavioral analytics to identify outliers and threats related to control planes manipulation.

The target users of NFV CyberGuard are:

- SOC users - security operations center users receiving alerts on potential attacks, threat classification and immediate action
- SIEM operators - analyzing the root cause as well as correlating with data from other solutions
- Network operations - monitoring and maintaining network consistency and availability
- NFV service owners - including operations for residential, business and infrastructure services; focusing on the availability and SLA of the service
- Chief Security Officer – for overall visibility into SDN/NFV threats

Use Cases

Data Theft though Flow Manipulation (Destination Manipulation or Data Duplication)

Attack Scenario: The destination of specific traffic flow has been manipulated in order to forward the flow to an attacker's server. The source of such an attack may be the result of a flow table manipulation such as NAT change, redirect or destination rewrite.

The attack is performed in intervals, each with a short duration. The flow table entries used for the manipulation are inserted for the duration of each interval and removed immediately afterwards. The attack is performed in a changing pattern to hide it, including interval time, interval duration and size of the payload.

Due to the nature of the attack, the attack will not be reflected in the controller, orchestrator or the NMS.

The manipulation occurs on a single virtual network element or on multiple elements at the same time.

With NFV CyberGuard: The attack characteristic will be similar in each interval in terms of flow table actions, source and destinations and possibly the length of each interval. Unlike attacks, legitimate behavior will either be a discrete operation or have random behavior. Network administrator operations are discrete as they are based on trial and error and are committed once completed with no additional interactions. Flow table updates based on end-user traffic have a random behavior by definition. Users accessing unknown destinations such as new web sites or uploading files to customers, requiring the network element to acquire new flows from the controller, don't have a fixed pattern.

When the user clicks on Flow Events – Destination or a specific event on the dashboard, the solution will display charts showing the baseline for normal random behavior and the suspected attack with definitive behavior.

Network Topology Manipulation to Bypass VNF

Attack Scenario: The service chaining of the virtual network on a specific NFV host has been modified. The purpose of this attack is to bypass a security VNF protecting the network, applications or users' devices; to bypass a VNF responsible for encryption and/or authentication; or to bypass a networking function such as SD-WAN responsible for traffic steering.

With NFV CyberGuard: The bypass might be permanent, one time or intermittent. CyberGuard analytics can point out the following cases that are the result of malicious activity having occurred:

- Abnormal service chaining path of a specific network segment or use case of a device. For example, removal of a firewall VNF from a vCPE service chaining or bypass of an IPSec function in an SD-WAN type of service chaining.
- Normal profile of a vCPE host based on the signature of many other hosts
- Suspected host under attack with VNF bypass
- Suspected host under attack with path modification
- Recurring service chaining changes on a specific host
- Recurrence of a specific service chaining change affecting a different host of the same type each time
- One time or permanent service chaining modification with abnormal profile for the host type

Network Topology Manipulation on Specific Host to Insert Malicious VNF

Attack Scenario: A malicious VNF might be added to the chain in order to steer the traffic, capture the data, overload the host or create a backdoor for an outside intruder.

With NFV CyberGuard: CyberGuard will display a service chaining graph showing conditions before and after the insertion.

Disconnection from Management Controllers

Attack Scenario: Disconnection from the management systems such as controllers and orchestrators occurs on networks due to device or network malfunction. Disconnections also might be used by attacks in order to hide the manipulation of hosts and/or upload software to hosts.

With NFV CyberGuard: CyberGuard can identify the disconnection pattern, the affected network segments, the affected devices and similar characteristics.

Here's an overview of each stage of the process.

The Collection Stage

One of the main problems in cyber security today is that operators and IT professionals don't really have visibility into the network. Without this visibility, it's very hard to detect and prevent any kind of threats. What's needed is a centralized view of what is actually happening in the network right now.

In order to collect the data for the centralized view, the NFV CyberGuard solution starts with a series of embedded agents and smart probes that collect all the session flow data and extract metadata and context. There can be hundreds or thousands of agents and probes distributed over the operator network, and they can run in three different ways: as an independent hardware module, as part of the NFV infrastructure in the CloudMetro (Telco System's Distributed-NFV platform), or as software on all x86 platforms.

Data collection can be based on specific rules; for example, to just collect the data about the networking protocols or the routing protocols. All of the information that is collected allows for full session reconstruction. Working on a session by session basis, the solution can determine if a session in the network is legal or illegal.

The Aggregation Stage

All of the data collected by the probes and agents is passed into an aggregation site in a central location, and from there it is pushed into a Big Data reservoir. Big Data techniques for recording, indexing and analysis are applied in this stage to definitively identify and characterize threats. Data is filtered, re-aggregated, correlated and investigated using network situational awareness, information discovery, advanced detection forensics and real-time analytics.

A historical network database is maintained. This is very important for the cyber security side in order to make correlations between the behaviors of network elements in different parts of the network. This can help to reveal unusual behavior that could be indicative of an attack in one area of the network.

The Detection Stage

After the data is aggregated and indexed, the solution applies analytics using numerous sophisticated algorithms in order to monitor and recognize abnormal behavior or specific threats. NFV CyberGuard is able to pinpoint suspicious activity across the entire network. The information that CyberGuard collects also could be used by third party vendors which have specific algorithms, either for prediction of threats or for anomaly detection, adding further strength to the solution.

The Action Stage

Once suspicious activity is identified, characterized and located, it's time to take immediate action through the SDN/NFV network management and orchestration system. NFV CyberGuard provides centralized control and orchestration for actions such as remotely changing the IP/MPLS control plane, or altering routing to shut off flows, service VNFs and devices. Network bypasses are established and deployed to reroute and redirect data flows. Once the threat is mitigated, the system restores normal operations.

- To get more details about how Telco Systems' NFV CyberGuard solution will work, watch a recorded webinar.

Conclusion

SDN and NFV technologies will change the entire telecom industry in the coming years. As the technologies move out from the data center to the carrier network itself, they hold the promise of bringing cost savings and new business opportunities. However there are several threats and security problems that come with this technology migration. Operators and other service providers who are accustomed to a very closed and protected environment must now consider how to protect the open NFV infrastructure that punches holes in the traditional separation between the control plane and the data plane.

Telco Systems is developing a cyber security solution that does extensive collection and inspection of all the network traffic coming from the edge to the closed end point. Using the cloud and Big Data, the solution is able to get a centralized view of all the applications and all the NFV infrastructure. From there threats can be detected via sophisticated algorithms by doing the reconstruction with all the metadata that is sent to the Big Data database.

All of this integration with the SDN controller and the NFV manager can take the smart actions to block threats throughout the network. Complete cyber security is dependent upon having the full view of the network, the full view of all the VNFs and all the protocols, and having the ability to do the correlation between the NFV infrastructure and the network itself. Telco Systems' solution is further enhanced with open APIs to external third party applications and algorithms to provide additional threat detection capabilities.

Get Started Today with Telco Systems

Telco Systems is already actively engaged with numerous operators and service providers who are taking the journey with us to fully develop all the capabilities of NFV CyberGuard. These early adopters will be among the first to enjoy the full benefits of a Software Defined Network with virtualized functions. Get started today:

- Visit Telco Systems' website at http://www.telco.com/
- Learn more about the NFV CyberGuard Solution
- Read the press release about NFV CyberGuard
- Watch a recorded webinar
- Contact us at sales@telco.com to start an engagement with Telco Systems

About Telco Systems

Wherever you find advanced, carrier-grade telecom networks, you find Telco Systems delivering innovative solutions to today's and tomorrow's networking challenges. Established in 1972, Telco Systems brings over 40 years of experience to the design and development of advanced, high-performance telecom network communications solutions.

Our market-leading solutions enable service providers to create and operate high quality, service assured, carrier-grade, intelligent networks. They provide the capabilities for service differentiation that enable new forms of revenue production, maximizing network profitability. Service providers, large and small, depend on our consistent delivery of advanced solutions, enabling them to stay ahead of the capacity crunch while keeping total cost of ownership to a minimum. Telco Systems is a subsidiary of BATM Group.

Telco Systems
A BATM Company

Contact information

International Headquarters
13 HaYetzira St., Yokneam Ilit,
20692, Israel
Tel: +972-4-993-5630
Fax: +972-4-993-7926

North & Latin America
15 Berkshire Rd
Mansfield, MA 02048
Tel: +1-781-255-2120
Fax: +1-781-255-2122

Asia Pacific (APAC)
10 Anson Road,
#17-03 Intl Plaza
Singapore, 079903
Tel: +65 6224 3112
Fax: +65 6220 5848

Europe, Middle East & Africa (EMEA)
Peterstr. 2-4,
52062 Aachen
Tel: +49 241 463 5490
Fax: +49 241 463 5491