SOLUTION BRIEF

High Performance Security and Hosted Virtual Equipment

Virtualized security performance scales with best-in-class density

- Hosted equipment eliminates proprietary single-purpose systems
- MaxCore Edge Compute platform hosts FlexRAN and edge compute applications
- Ultra-high user density: up to 7700 instances per 3U system (vSEG)
- 400Gbps firewall per 3U system
- vCPE framework enables unified customer “equipment”
- Superior maintainability and upgradeability with no service calls
- 90% reduction in OpEx compared to RMS-based solutions
- No need for Top-of-Rack (ToR) switching to distribute across CPU complexes

Security continues to be a top-of-mind worry for businesses, government and consumers alike. Recent events around the world have strengthened this worry. In response to this need, Clavister and Artesyn Embedded Technologies have teamed to create scalable, virtualized network security, delivering broad scalability and high density.

By virtualizing the security function, communication network operators (CNOs) can spread performance over a cloud of cores, resulting in high scalability and high throughput. When combined with a platform that has the ability to hold up to 360 Intel® Xeon® cores in a 3U footprint, carriers have the ability to place dense, flexible, and secure computing in their network where it makes sense rather than where it fits physically.

As carriers and enterprises increasingly deploy with multiple new applications in multiple environments, security and compliance become more difficult to maintain. The Clavister virtualized software solution offers carriers standardized security across multiple services.

The innovative Artesyn MaxCore™ family of platforms is the ideal environment for virtualized security, virtual customer premise equipment (CPE, vCPE), and virtual mobile networks, as well as other virtualized applications. Use of low power Intel® processors in the Artesyn system dramatically reduces power consumption while maintaining high core count. As operating costs are now far larger for network operators than capital costs this means increased performance while reducing operating costs.

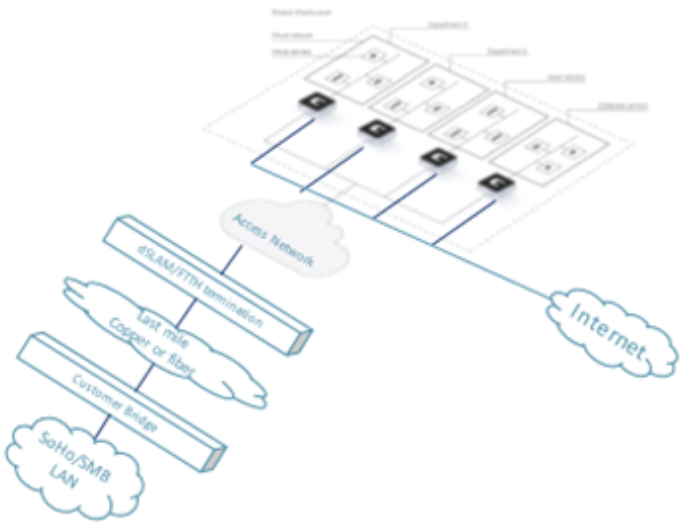
Artesyn hardware, Linux/KVM and Clavister Security software creates an extremely secure network and execution environment, able to handle any type of network function virtualization (NFV) environment, setup and the ability to scale up/down without sacrificing any integrity, privacy and robustness. Let Artesyn and Clavister show you how next-generation edge security and equipment hosting is going to look.

intel experience what's inside
INTEL® NETWORK BUILDERS PARTNER

clavister®

ARTESYN™
EMBEDDED TECHNOLOGIES

Clavister Virtual Security Gateway



Edge Computing and Hosted Virtual Functions

Edge computing is the complement to the cloud that will shape next generation networks. The cloud will continue to grow driven by optimization of business models, on demand compute, and CapEx & OpEx efficiencies. However, as an increasing number of devices connect to the network the need to optimize network traffic increases. This need has given rise to intelligent edge computing.

Key attributes to effective edge computing are intelligent nodes, which can determine whether a workload should be processed locally or offloaded to the cloud, and virtualization, enabling flexibility and efficient compute resource usage.

FlexRAN

The FlexRAN architecture encompasses virtual and cloud RAN architectures as well as hybrid implementations. As 4G and 5G networks evolve toward Ethernet fronthaul the FlexRAN architecture can enable more scalable, flexible, and cost-effective base station implementations. FlexRAN relies on a virtualized edge compute architecture with the ability to process functions which need immediate results or low latency while off-loading to the cloud those functions which do not require real-time processing. This enables scalability in compute power while cost-optimizing the network.

In the MaxCore FlexRAN architecture portions of L1-3 are done locally while other compute portions are processed in the cloud. Companion applications such as security or low latency applications such as video are also processed using the local edge compute capability. In the future the presence of the compute portion of the L1 function will enable location aware services which will drive new revenue streams for operators and their customers.

The Artesyn MaxCore platform is designed to enable co-hosting of both FlexRAN and edge compute applications.

Virtual Hosted Equipment

Virtual hosted equipment or virtual customer premise equipment offers the ability to resolve many of the issues associated with traditional, fixed-function appliances. When refreshing network edge platforms the use of vCPE increases the opportunity to quickly deploy alternative services to end users. Compared to hardware based CPE, vCPE enables greater flexibility and efficiency and gives carriers greater control of service delivery options.

Virtualized CPE increases the agility of networks, enabling them to respond to changing needs more rapidly while reducing the costs of adding new functions at the edge. When it comes to managing the equipment required to deliver todays services carriers are faced with an ever-increasing array of boxes, routers, and converters, each of which has limited functionality.

In addition, the existing customer equipment is rarely fully utilized, resulting in wasted computing resources, an inefficient way to provide services. Carriers must also bear the costs of service technicians for installation and the cost of obsolescence of older equipment. The result is either lost profit or increased costs to customers, or both.

Clavister's virtual security implementation is one of many offerings which can be provided by communications service providers (CSPs). It can protect a wide array of vCPE functions but can also be a Security as a Service offering. This SaaS offering can include virtual firewalls and dynamic access controllers, enabling businesses to securely interact with their customers or securely access Internet functions.

Additional vCPE services could include web filtering, parental control, and threat prevention for consumers. For enterprise customers services such as web filtering, e-mail control, threat prevention (including malware, intrusion, denial of service, spam) and VPN tunneling could all be offered.

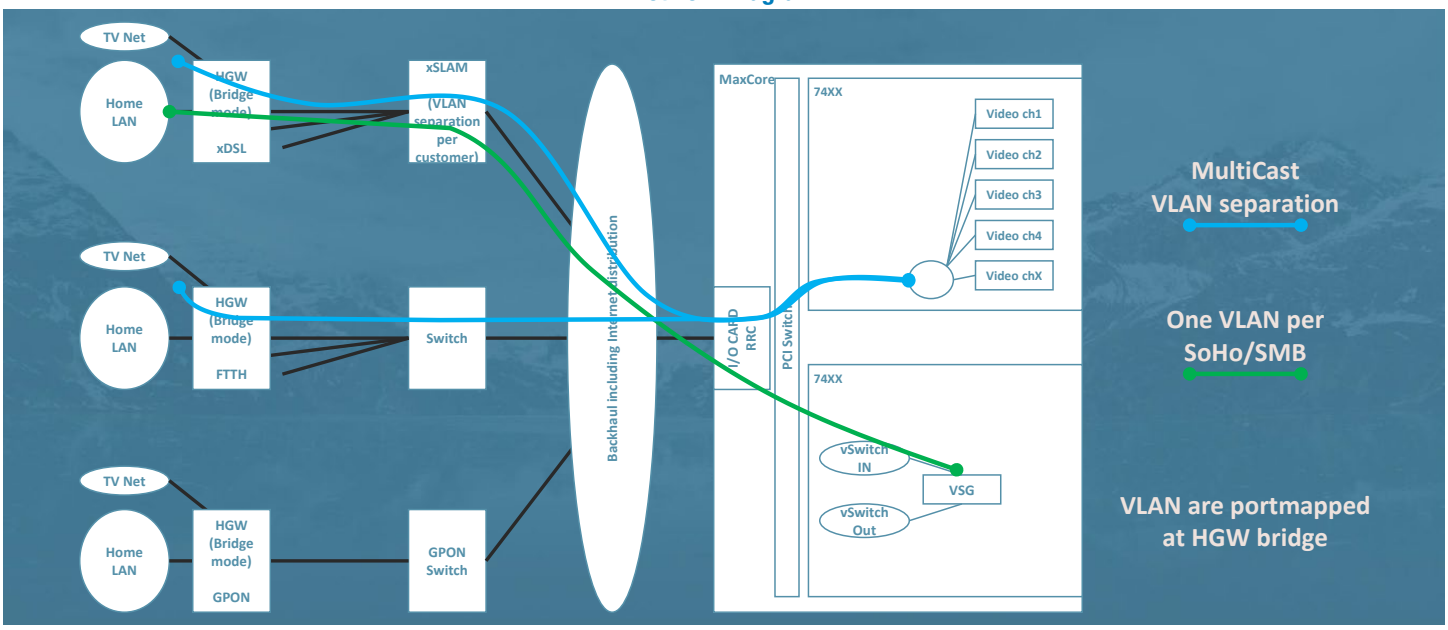
Clavister Virtual Security

Clavister Security solutions are designed to meet the changing needs of today's networks. The virtual security gateway includes full customer isolation where each customer has their own environment. Full memory separation results in no impact between customer environments. Configuration changes occur without service interruption to other customers.

This complete vCPE feature set makes it possible to offer multiple services in the same vCPE installation with as many as several hundred vCPEs per CPU.

ARTESYN™
EMBEDDED TECHNOLOGIES

Network Diagram



Compared to virtualized solutions using a hypervisor or even containers the Clavister vCPE is a superior environment and enables more instances per CPU and more concurrent users per platform. Clavister cOS Core includes an optimized small footprint with no bloated standard OS. The cOS Core features low startup and restart time and low memory usage resulting in more customers per rack unit and less wasted CPU cycles.

# of users per CPU	# of users per system	Packet size	Mbps per VSG	Total throughput (Gbps)
350	7700	1448	24	8.4
350	7700	512	11.7	4.1
350	7700	64	1.17	0.406

Notes: Above performance in 3U footprint
Total system firewall performance 400Gbps (full duplex)
Total system IPsec performance 294Gbps

Clavister security software offers flexibility in feature set and scalable performance, centralized OA&M for all platforms and supports OpenStack software for cloud deployments.

State-of-the-art, scalable and future proof.

Virtual security and hosted equipment solutions available from Clavister and Artesyn.

The Artesyn MaxCore™ Platform

Artesyn brings the densest and highest performance platforms in the industry to the security segment. Built on open standards, they enable multi-party sourcing and cost-effective scalability. Further performance increases are available with new cryptographic acceleration techniques including the Intel® Xeon® AES instruction set and add-in PCIE cards.

The extremely flexible and cost-effective Artesyn MaxCore platform implementation for distributed and centralized environments enables industry-leading performance, low-latency, rack space reduction, and OpEx savings. The MaxCore platform also enables a scalable, high-density implementation for hosting security and other vCPE functions. The high bandwidth and x86 core density create a cloud at the edge, optimizing cost per customer and network bandwidth.

- Highest Intel Xeon core density – Up to 360 Intel Xeon cores in 3U chassis!
- Highest flexibility – 15 slots for dual Intel Xeon D, E3, I/O or any PCIe cards
- Up to 400Gbps I/O shared by all processors
- Switching and load balancing in platform
- Open Stack, OpenFlow integration
- Edge 3U and Cloud CG OpenRack 19 & Hyperscale form factors available

www.artesyn.com

+1 888 412 7832 or +1 602 438 5720

High Performance Security-SB February 2017

ARTESYN™
EMBEDDED TECHNOLOGIES