

## Highlights

Traditional Data Centers are being increasingly side-lined when it comes to new and emerging Campus-based applications and flows.

Enterprises need to decentralize and distribute DC-like functions capabilities through the Campus network: DC-grade trust, control, automation of network functions chaining.



## Extreme Networks Pivot™ Operating Platform

The Everywhere Data Center, that emerging phenomenon driving never-before-seen east-west traffic patterns within the Campus, demands a radical re-think of conventional approaches to network security. This new reality drives a requirement for distinct security tiers, and a means to safely and efficiently interconnect a mass of users, devices, and applications.

IoT, Big Data, and Digital Transformation are the trends at the heart of the Everywhere Data Center. Everyday examples include second-generation IoT solutions that integrate full-service compute capabilities, edge-based business decision applications that rely on real-time analytics, and evolving transformational solutions that leverage locally cached data stores.

### Cause and Effect

Traditionally, application flows pass north-south between Campus-based users, allocated to generic VLAN-based zones using Network Access Control, and IT's Data Center-based compute and storage resources. This allowed IT ample opportunity to inspect and regulate as traffic passes through the Firewall/Unified Threat Management systems deployed in the boundary between these two environments. However, as new-age computing transitions into the Campus, resulting in more and more east-west flows between Campus zones, the conventional approach breaks down.

### Everywhere Data Center : a definition

Where the Campus hosts applications sending, receiving, and executing data between endpoints that are beyond the reach of conventional trust models, involving flows that do not transit the conventional DC, for applications that are outside the scope of the value-add controls designed into conventional architectures.

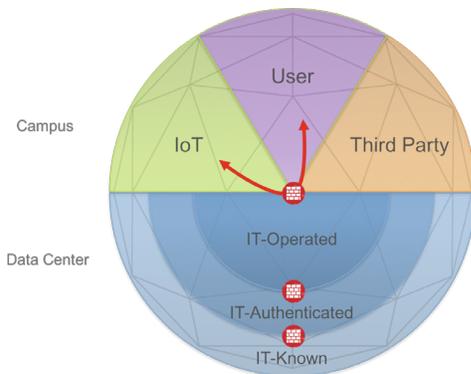
As the prevalence of Everywhere Data Center computing becomes entrenched and more wide-spread, the problem only becomes worse. Forcing all of the Campus' inter-zonal flows through IT's traditional security demarcation solution - the "trombone" approach - results in an ever-increasing traffic load, burgeoning rule complexity, and untenable single-point sensitivity.

### Scale and Automation

Deploying standalone Firewall/Security appliances directly into the Campus, regulating application flows between security zones, is cumbersome, costly, and requires complex integration with the underlying network design. These approaches require network integration at both Layer 2 and Layer 3, are often static in nature and therefore introduce their own resiliency concerns, and are clumsy and inefficient to administer and manage. Further complicating matters, elements of the application flow may relocate or expand, necessitating complex and time-consuming physical reconfiguration.

### Security

Even assuming that distributing standalone security appliances widely throughout the Campus were economically feasible, manually provisioning these, hop-by-hop, is a cumbersome exercise, prone to human errors, inevitably leading to performance issues and unknown security gaps. Black-listing known threats is relatively easy, although inherently less secure, while white-listing is theoretically more secure but an administrative nightmare.



### Net Result

To support the Everywhere Data Center, businesses first need to implement DC-style security tiers into the Campus. Used together in combination with conventional user and device zonal classification, this approach creates the layered defense necessary to secure the enterprise from digital-age threats. Next, IT needs the capability

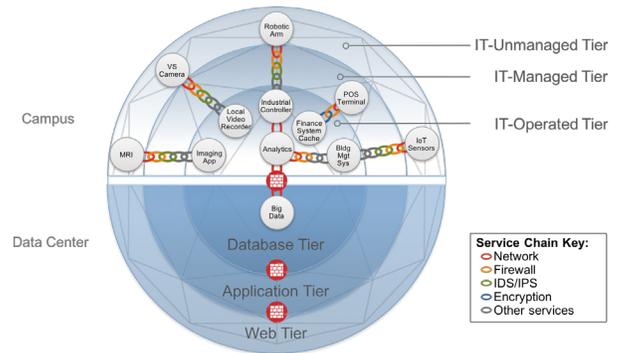
to dynamically implement a versatile mix of networking functions, architecturally proximate to the sources of Campus east-west application flows.

Going forward, the Campus needs to have a DC-like network virtualization capability, DC-like tiered approach to layered security and threat mitigation, DC-like service chaining for virtualized network functions (VNF), and a system of DC-like orchestration and automation. The simplistic analogy is that the Campus needs a DC make-over.

## Solution: Pivot Operating Platform

The Pivot operating platform, in combination with Extreme Networks Arc™ orchestration engine, offers an automated solution to deploy full-stack advanced networking and security functions throughout the Campus. Pivot provides an agile and elegant solution to the security challenges created by the Everywhere Data Center, while also reducing manual configuration, the cost and complexity of standalone appliances, and scaling restrictions.

Pivot negates the need for manual or physical provisioning, removes location constraints, and greatly reduces security gaps caused by human errors or architectural limitations. Individual elements of the stack, including network virtualization and best-in-class advanced services, can be selected based upon the unique requirements of the subject application.



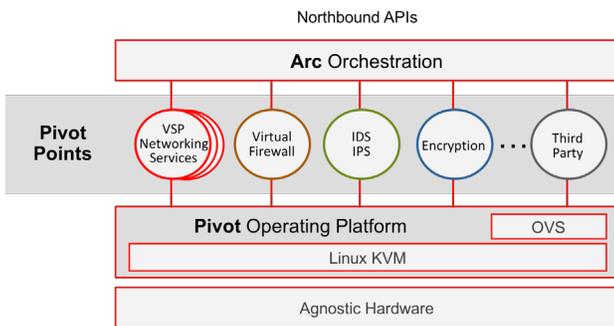
Introducing platform virtualization to networking infrastructure enables flexible delivery of traditional and emergent virtualized network functions, and creates a path for effective chaining: Linux containers supporting multiple, mission-specific virtual functions can be chained, orchestrated, and automated. Pivot is an open and extensible operating platform that is hardware independent and network function agnostic: Pivot solutions can support a variety of Extreme Networks-developed or third-party network functions, orchestrated into full-featured service chains.

Pivot defines a new approach that delivers full-service networking, but is neither simply a new type of networking node nor a new server-based networking stack; Pivot combines the ubiquity of networking with the flexibility of compute.

The Pivot operating platform does for the network what the Hypervisor did for the Data Center: de-coupling and abstracting operating system from hardware, virtualizing networking, supporting additional advanced functionality, adding an orchestration capability, and empowering automation.

### Pivot: Beauty in Simplicity

In short, Pivot implements, what is in effect, a Linux overlay deployed on a base hardware platform that delivers a virtualized network functions capability and empowers service chaining. This abstraction creates a common-use host that allows for multiple guest networking functions to be supported and, where appropriate, orchestrated into chains and automated. It's simple, logical, analogous to widely-deployed compute virtualization, and has already been demonstrated: the Extreme Networks Surge™ solution for IoT is proof-positive of the Pivot concept.



### Pivot Host Platforms

Being a Linux-based software shim, Extreme Networks Pivot can be implemented in multiple conventional and unconventional hardware platforms.

The latest crop of networking products leverage powerful control and network processors: with Pivot, the traditionally closed architecture and proprietary operating systems are bypassed, allowing access the processing power that's of these devices. Extreme Networks is actively developing a new range of networking products that will support Pivot and incorporate the resources necessary to deliver a variety of chained network functions.

Somewhat less conventional, Pivot will also be supported on hardware such as the Extreme Networks Open Networking Adapter, third-party Pivot-certified networking hardware, and Pivot-certified x86-based compute hardware.

### Pivot Guest Functions

Pivot-ready host platforms are capable of, depending upon individual processing and memory capabilities, support a wide variety of virtualized networking, security, and advanced Layer 4-7 functions. Examples, developed both by Extreme Networks and third-parties, include:

- Extreme Networks VSP Operating System Software
- Extreme Networks HyperSec Gateway
- Extreme Networks SDN-based IoT Controller
- Extreme Networks Virtualized Open Networking Adapter
- Application Firewall
- Encryption
- Load-Balancing
- TCP Load-Sharing
- SD-WAN and WAN Optimization
- Address/Name Services

## The Unique Value of Pivot

The Pivot operating platform breaks the convention of the network control and forwarding planes being intrinsically linked in hardware. Empowering network functions to operate independently, across diverse platforms, enables truly distributed next-generation networking and security. Additionally, Pivot complements the reality of “small is more”: strategically placed infrastructure elements that are compact and agile, maximizing performance, availability, and deployment flexibility.

The benefits of Pivot are significant and represent a quantum advancement in the economies of scale that network infrastructure can deliver:

**Accelerate Service Delivery.** Services characteristics are becoming increasingly sophisticated as applications break with conventional rules, roles, and locations. Network functions service chaining is the key to effective delivery; however, this can only be enabled when the infrastructure is virtualized and agile.

**Maximize Infrastructure Efficiency.** Traditional sole-use networking nodes are notoriously difficult to right-size for a given deployment scenario and inhibit service agility. Virtualizing the infrastructure and opening it up to multiple network functions both maximizes its efficiency and empowers simpler orchestration of high-performance service chaining.

**Reduce Capital and Operational Costs.** Unlocking to latent resources of network appliances, leveraging generic x86 platforms, and unlocking the network infrastructure to third-party functions creates a genuinely open environment that reduces the total bill of materials while consolidating and minimizing the management overhead.

Pivot addresses the challenges of the Everywhere Data Center. Its overarching value to organizations is its ability to quickly assimilate open out-of-the-box services into a networking control platform that extends the regulate and protect new-age application flows. Pivot-hosted services can – conceptually – be anything, they can range from the obvious network operating system and network security services, to the more abstract data inspection and analytical engines.

The Pivot operating platform is portable across any purposeful platform such as an advanced Network Switch or x86-based hardware platform. The Extreme Networks Arc orchestration layer coordinates networking service chains, while northbound APIs allow programming into other Enterprise systems.

Since Pivot is an operating platform that extends advanced functions into all areas of the network – Campus, WAN, and into the traditional Data Center – services do not need to be collapsed onto overloaded centralized nodes: complexity is reduced and network efficiency is improved.

Crucially, Pivot is a strategic architecture that addresses the demands of IoT, Big Data, Digital Transformation and the challenges presented by the Everywhere DC.

## Additional Information

To learn more and to obtain additional information about the Pivot operating platform, or Extreme Networks in general, please contact your Extreme Networks Account Manager, Authorized Partner, or visit us at [www.extremenetworks.com](http://www.extremenetworks.com).



<http://www.extremenetworks.com/contact> / Phone +1-408-579-2800

©2017 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see <http://www.extremenetworks.com/company/legal/trademarks>. Specifications and product availability are subject to change without notice. 12083-0617-28