BROCADE

The New IP Sets a High Bar for Cybersecurity

IDC identified the Third Platform as an area of innovation and growth, defining it as technology built on the pillars of mobile computing, cloud services, Big Data, analytics, and social networking. Cybersecurity countermeasures become increasingly critical as the Third Platform era enters the critical innovation stage.

The New IP is a modern approach to networking that emphasizes open, automated, software-defined elements to increase agility and reduce costs while meeting the challenges of the Third Platform. And the great news is that the New IP provides a new way to architect networks that accelerate business changes and growth while maintaining or increasing high levels of security.

New IP Security Principles

Old IP networks are highly vulnerable to security attacks due to their relatively static nature as well as the cost and inefficiencies of hardware only-based security. Layered security for defense-in-depth is significantly enhanced with a New IP architecture because security is:

- Designed in, not bolted on
- Open, not closed
- Based on behavior, not just identity
- Self-learning, not static

This cybersecurity brief discusses these New IP security principles and:

- What they mean to your business and network
- How Brocade employs these principles within its strategy, partnerships, and product/solution capabilities
- How Brocade uniquely enables you to solve the greater security challenges of the Third Platform more effectively

Security Is Designed In, Not Bolted On

Part of the problem with old IP networks is that security is infrastructure-bound, implemented by devices that are deployed at the edge. In fact, security might have been a separate deployment bolted on at the edge of the network (i.e., perimeter security) representing a single point of failure intended to secure the entire network. But in the cloud era, in which the data center and networks converge and the lines of demarcation blur (and access becomes increasingly mobile), the concept of the perimeter disappears.

Hence, the New IP abstracts security from the underlying network infrastructure. There are no boundaries. In theory, all parts of the network need to have security enabled and need to play a role in defending the network against attacks. The New IP allows you to deploy security in this manner so that the network itself can be pervasively vigilant, ensuring the security of both data-at-rest and data-in-flight. This pervasiveness is accomplished in the following ways:

- **Improve Security with Network Virtualization while Lowering Costs:** The cost and complexity of securing the network's perimeter presents challenging cost, performance, and security compromises—leaving you to rely on a few security devices deployed at select strategic locations to secure your entire network. Deploying services as Virtualized Network Functions (VNFs) is a simple but powerful approach.

This delivers significant OpEx and CapEx savings (up to 90 percent reduction in capital). Moreover, virtualized services—such as routing, load balancing, application delivery and security, Web and network firewalls, VPN, and enhanced security—can be moved in real time and through remote management that does not require physical redeployment and human capital.

Because of the cost savings, you now have the ability to distribute functionality more appropriately, and you achieve the same performance of physical implementations with the flexibility of software. Security can be distributed where needed or even distributed ubiquitously. Similarly, you can remove the services when they're no longer needed. This gives you the ability to truly customize security at various levels—by geography or location, by function, by group, by individual or by application.

This level of embedded security allows organizations to address compliance assurance from site to cloud, employee to application resource, and tiering of security between application tiers through the use of IPsec encryption, remote access VPNs, stateful firewall, and Web application security capabilities embedded inside of the Brocade® vRouter and Brocade vADC products.

Also, with the New IP, every user or every application can get its own network. This means it is now possible to provide every user or application with its own virtual network, including unique router, firewall, application delivery controller, security protection, and other services. This means you can also generate a secure network for each user or application to improve security, control, flexibility, and customization. Attack points in such a network become fragmented and harder to infiltrate en masse. This micro-segmentation of services shrinks the security domain so that if one virtual network instance experiences a successful cyberattack, it doesn't bleed into the other virtual networks. In this every-user-gets-a-network model, every service (security-related or not) within the user's virtualized network plays a role in improving security.

- **Security and Analytics Applications on an SDN Controller and/or Analytics APIs to the SDN Controller:** Leveraging flow technologies (such as sFlow) and an SDN controller with programming capabilities (via extensible APIs) allows a centralized view of network behavior. It also provides the ability to take action and push policies to the network in real time. This centralized real-time view of the entire network provides a critical capability to recognize and immediately react to security threats within the infrastructure.

  The benefits of this implementation are further magnified when used with advanced messaging approaches such as Pub/Sub (Publisher/Subscriber). Unlike SNMP, where devices are pinged or polled to get a response about their device status, Pub/Sub enables every element in the network to automatically generate its state and condition and push it to a centralized repository so that analytics can be performed. The elements are self-responding, not polled. With all the elements pushing information automatically, you get real-time visibility into the entire network, not just points in the network. This provides increased sophistication in orders of magnitude and is a stepping stone in the path toward security empowered by machine learning.

- **Inherently More Secure Fabric Architecture:** Using an underlying network fabric, such as an Ethernet fabric built with Brocade VCS® Fabric technology, you can create a simplified flat network topology, even when adding VNFs. A fabric allows the east-west traffic among Virtual Machines (VMs) to be isolated and contained within a single plane instead of transiting through multiple segments of the network. This eliminates the need for traffic to transit from top of rack, to aggregation, to core, and then back up to some other part of the compute environment. This simplified architecture inherently increases security by design.

  The underlying fabric is also VM-aware. The awareness of the VMs, the number of virtualized services and types of virtualized services, and the behavior of those virtual machines, is important in securing those services.

- **Network Devices Encrypt Data-in-Flight:** A key aspect of data protection is securing data-in-flight. With networks constantly under attack, securing data through encryption is an effective countermeasure to ensure data security. In the data center, LAN, and WAN, incorporating native encryption for both Layer 2 (MACsec) and Layer 3 (IPsec) directly into the hardware forwarding path can protect data going across a link. This can be done without impacting performance or introducing the cost and complexity of backhauling traffic to specialized devices. This is especially critical when the network links are not under an organization's physical control, such as between data centers, between sites, and between sites and the cloud.

  Brocade MLXe Routers and Switches support inline, port-based, wire-speed encryption for both Layer 2 (MACsec encryption with 128-bit keys) and Layer

3 (IPsec Suite-B encryption with AES 256-bit keys). Brocade ICX® Switches support MACsec encryption today, and will support IPsec encryption in a future release. In addition, the Brocade vRouter supports IPsec encryption today. This comprehensive approach to encrypting data-in-flight enables you to deploy network infrastructure that can provide security for data-in-flight across the campus, between data centers, and across the WAN, and to workloads deployed in public clouds.

- **Application and User Awareness for Client-to-Application Security:** Accessing critical business applications requires multiple layers of protection with awareness of who, why, and what. With the migration to the Third Platform, the interaction from business to consumer is increasingly more focused on Web-based transactions.

  The requirement to ensure secure access to the lifeblood of a business through a Web-based application is compounded by the increased volume these applications now consume. The applications need unique application delivery controllers capable of handling the increase in the magnitude of SSL-based traffic while simultaneously having an integrated Web application firewall capable of intelligent self-learning techniques to help ensure and maintain high levels of availability and customer satisfaction. A level of flexibility is needed to target individual users or groups of customers with unique security requirements per application.

  The Brocade Virtual Application Delivery Controller (vADC) supports high-speed encryption services and application-layer security with SSL offload and automated analysis and remediation for Layer 7 threats with the integrated Web application firewall. This allows for a native extension of security into the application on a per-application basis.

Security Is Open, Not Closed

With old IP networks, point security appliances such as firewalls, IPS/IDS, DPI, analytics tools, encryption-at-rest and encryption-in-flight, etc., each solve specific and distinct security challenges. There is no information exchange and collaboration between these security silos, and there is no security services abstraction layer that takes advantage of the key learnings from all sources to better and more rapidly address security issues.

Interoperability is not the same as being open. True openness happens when a community exchanges information, there are stable and programmable inputs, and there are standardized formats and languages for communication, such as APIs. Every element has a vested interest in contributing to the community and being part of solving the security challenges.

The New IP brings together the best of hardware and software, offering a hybrid implementation that delivers outstanding performance enabled by hardware and agility and flexibility enabled by software. There is a standardized way to interact and communicate with any device or sensor (physical or virtual) with an SDN controller such as the Brocade SDN Controller.

All the data from the sensors can be collected and delivered to an analytics engine for visualization, identification, and action. You can change the behavior of any device because you can communicate, program, and write to it. You have the ability to extract data from the network and understand the network as one system. The power comes from

THE OPEN BROCADE SECURITY FRAMEWORK

Brocade's successful business model is built on expertise, experience, and a commitment to building world-class partnerships as well as driving and participating in open, collaborative ecosystems. As the company has done with storage, data center, campus, and software networking, Brocade continues its work in forging these collaborative partner relationships with the New IP, particularly in the area of security.

A closed system is like Encyclopedia Britannica, where the content is mainly authored by the company. It is written and remains static until the next volume release. On the other hand, in an open system such as Wikipedia, many "experts" on the various topics contribute in creating and updating the content on an ongoing basis. The openness of the New IP helps ensure a richer and more dynamic cybersecurity solution.

As part of an open security strategy, Brocade is committed to sharing relevant data from elements and sensors to third-party security and analytics applications to turn data into meaningful and actionable information. Brocade has an open security data exchange and APIs that allow for interaction with various security elements for more extensive security data collection, correlation, and enforcement. This open security framework allows Brocade and its partners to see the entire network, as opposed to points in the network like current inline devices do.

the system's ability to communicate what it's seeing, the knowledge that visibility imparts into how all the adjacencies are working with and enhancing each other, and the power to take action and make changes through software.

This new approach has spawned innovative applications and technologies to ensure the standardization of New IP architectures and to help companies confidently move forward into this new era of networking. The transformation of the underlying network infrastructure to incorporate white-box or hybrid black-box elements will energize the use of OpenFlow for granular network programming through a centralized controller offered through projects such as OpenDaylight. This shows how open approaches provide standardized methods for visibility into individual packet flows and the ability to react to security breaches.

Security Is Based on Behavior, Not Just Identity

The New IP offers a higher security posture than old IP networks because New IP networks can take into consideration *behavior* (what, when, where, and why) rather than just *identity* (who) when applying security policy. With behavior-based security, the system gets deeper insights into typical and atypical actions and into preliminary steps in the attack process, allowing it to not only mitigate or stop attacks already occurring but prevent potential attacks. Additionally, since most breaches have an inside element, identity management cannot be relied on to detect an attack. You need a means to detect insider attacks, protecting the system against those who have legitimate access. Behavioral analysis of risk factors, indicators of what is abnormal activity, and detection of out-of-context behavior is crucial.

The Brocade Flow Optimizer is an SDN application for OpenDaylight (running on an SDN controller such as the Brocade SDN Controller). It addresses network challenges in application-centric environments where security is an increasingly important issue. The Brocade Flow Optimizer application identifies and controls Layer 2 to Layer 4 flows based on application or business policy. It identifies high-volumetric traffic attacks and stops them. At the same time, it can endorse trusted flows, which can bypass slow security appliances and improve overall network performance and security. In this case, the network itself is providing the ability to identify and mitigate some attacks.

Here's an example of how it works in live implementations. Brocade MLXe routers or Brocade ICX switches send sFlow monitoring reports to the Brocade Flow Optimizer. The sFlow information is analyzed and, as a result of policies that the security administrator sets, the solution identifies out-of-policy traffic and proactively takes action on it, if necessary. The application can discard dangerous traffic to prevent it from traversing the network, rate-limit the traffic to improve performance, and re-mark the priority of the flow. It can also redirect the traffic to an isolated port for further diagnostics.

Additionally, the Brocade Network Visibility solution provides packet broker capabilities to expand the ability to capture data out of band from the network and deliver it in real time to tools for analysis and action. This capability can dynamically send threat mitigation policies into the network via SDN, REST, and other interfacing mechanisms while its agile Network Functions Virtualization (NFV) architecture offers elastic scalability as traffic surges or drops.

In addition, the Brocade Virtual Web Application Firewall (vWAF) employs self-learning techniques to identify unusual behavioral patterns for entry and exit to a business application. Associating this intelligence and combining it with application business logic allows for a high level of fine-grained visibility and enforcement.

Security Is Self-Learning, Not Static

The security system in New IP architectures is continually learning and self-optimizing. As it monitors behavioral patterns and looks for preliminary attack activities, the system can predict the likelihood of an attack. This is unlike traditional systems that rely on pattern matching with databases that get updated periodically. In that case, if an exploit doesn't fit into any of the patterns, the security system doesn't recognize it as a threat. New IP architectures are more agile and can self-improve in that regard.

Applying Big Data and machine learning concepts to network behavior allows you to go from a reactive to a proactive security posture, from descriptive to predictive analytics, and ultimately, from a static to a self-learning or adaptive network.

In a self-learning system, devices can be hardened or programmed to increase the security posture against a predicted threat, not merely an actual threat. Rather than dealing with Day-Zero exploits, you can deal with Day-Minus One (or more) to protect against a developing attack. As an example, you might decide to spin up a virtual DMZ or push certain policies to limit or block a port in advance of an attack or to halt a developing attack. This is nearly impossible to accomplish in real time with old IP networks and hardware-only solutions. The self-learning, with predictive analytics, and on-demand capabilities create a more secure network.

The Brocade solution has the ability to reprogram the analytics network to fine-tune the data it receives to more effectively manage and detect changes. When anomalous traffic patterns are detected, it can trigger notification to operations personnel to take action based on the policies that have been set.

Improved Security through Storage Networking Best Practices and Secure Capabilities

Any comprehensive cybersecurity strategy must include the network that provides or denies access to your crown jewels (your data): the storage network. The storage network is potentially your last line of defense if perimeter security has been compromised.

If you combine New IP security principles with the storage networking best practices of isolating storage traffic (building separate storage fabrics for IP or Fibre Channel), encrypting data, and instrumenting capabilities within the storage network, you will improve your overall security posture.

- **Dedicated Storage Fabrics:** Dedicated storage fabrics are becoming the standard for mission-critical and business-critical workloads. This allows you to have predictability for the workloads and higher security. In a classic shared-network design, a number of services share the same network. This is problematic when anomalies occur. And it's very challenging to determine the root cause. Dedicated fabrics built on Brocade Gen 5 Fibre Channel switches or Brocade VDX® IP storage platforms provide physical isolation between networks and allow the architecture to determine in real time what is going on within the network. Brocade has been delivering highly secured storage fabrics for over 20 years and continues to evolve to be protocol-agnostic.
- **Storage Replication with Security:** Mission-critical and business-critical workloads are now being replicated between data centers. You need to maintain high levels of performance but also improve data security while the data is in transit. Since data is the most important enterprise asset and a key target of cyberattacks, you need to encrypt closer to the storage fabrics. The Brocade 7840 extension switch encrypts in-flight data between fabrics without compromising performance. Because the switch has tailored the TCP/IP protocol to be storage-aware (meaning it understands streams, block sizes, timeouts, etc.), it can also apply the appropriate services (such as compression, protocol acceleration, etc.) prior to encryption. Ultimately, it improves network utilization and increases the security posture while meeting business requirements such as compliance for business continuity and disaster recovery.
- **Analytics and Instrumentation:** Analytics have become critical in every aspect of the IT infrastructure, especially storage. The old practice was to insert physical taps into the data path to look at performance, latency, and error reporting. That entailed a copy of all the frames and data leaving the fabric—clearly a potential security risk. Anytime you have data going into a third-party device, it leaves the architecture open for vulnerabilities or data snooping. The Brocade Analytics Monitoring Platform (AMP) allows you to look at analytics in a new way. You are able to do all of the monitoring and analytics by capturing and inspecting just the headers of the frame. You never need to mirror the data flows into another device, eliminating the threat to your data.

Why Brocade Is the Key Enabler for Cybersecurity

Brocade was founded in 1995, which coincides with the start of the last big transition in the computing industry. Unlike other networking companies, Brocade started with a focus on the data center with an understanding of how to control packets and move data as efficiently as possible.

Today, Brocade is a $2.3 billion company with the highest market share in the SAN switching market and the #2 overall company in data center networking. Brocade is a clear leader in these areas because no vendor is better at helping you connect heterogeneous data storage environments and move your data among different devices and protocols. EMC, HP, IBM, Dell, HDS, and others sell Brocade networking products and technologies as part of their data center storage portfolios—a key reflection that partnering is at the core of Brocade. And partnering is a mandatory requirement to building an open security ecosystem and enabling a higher security posture today.

Nearly every Fortune 500 company and major organization in the world relies on Brocade technology in the data center, especially for applications that require the highest levels of performance, availability, and security in mission-critical environments.

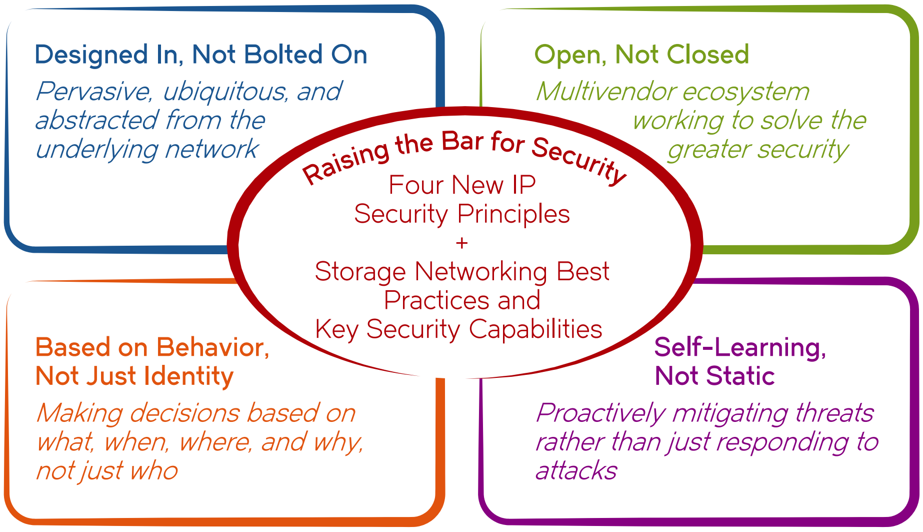
Brocade understands that the market pressures on you and your teams are mounting. Cloud, mobile applications, the drive to be a digital business, and cybersecurity concerns have strained old IP networks. These same factors are also constraining business innovation, forcing you to rethink your infrastructure strategies.

Brocade made an early investment in open technologies and software networking, and is focused on leading this market transition. The Brocade strategy is built around the New IP, with hardware and software that is designed to take full advantage of the trend toward open, virtualized IT infrastructures.

Working collaboratively with customers, vendors, and partners around the world, Brocade has built a solid foundation to set a new standard for cybersecurity countermeasures.

Brocade products and the roadmaps for routing, switching, software, and network visibility and analytics networking products employ the key security principles for the New IP. More importantly, Brocade is committed to exchanging information and contributing to an ecosystem that solves the most difficult cybersecurity challenges. This includes providing traffic knowledge, threat information, and breach data to analytics, enforcement, and compliance engines, for example. That's because cybersecurity is not a single-vendor challenge or solution.

New IP Security Principles



Designed In, Not Bolted On

Pervasive, ubiquitous, and abstracted from the underlying network

Open, Not Closed

Multivendor ecosystem working to solve the greater security

Raising the Bar for Security

Four New IP Security Principles
+
Storage Networking Best Practices and
Key Security Capabilities

Based on Behavior, Not Just Identity

Making decisions based on what, when, where, and why, not just who

Self-Learning, Not Static

Proactively mitigating threats rather than just responding to attacks

Moreover, combining New IP security capabilities with storage networking expertise allows Brocade and its partners to further improve the security posture of networks—securing applications (regardless of where they reside in the network) all the way to the storage arrays that hold data. This is true defense-in-depth at all layers of the network, including having the last line of defense for your data, in case your perimeter security is compromised.

A New IP architecture and the enhanced security it creates—plus best practices and key capabilities in storage networking—are essential to support a broader move to the Internet of Things, the cloud, and digital business models.

Applying New IP principles of security is an evolution, not an overnight transformation. But the good news is that your evolution can start today, along with that of the many organizations already using the proven technologies, products, solutions, and implementations described in this brief.

For more information, contact a Brocade sales partner or visit www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment features, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This information document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

BROCADE