White Paper

The Future of Borderless Network Security

By Jon Oltsik

June, 2010

This ESG White Paper was commissioned by Cisco Systems and is distributed under license from ESG.

Contents

Executive Summary

It's easy to be skeptical about the technology industry vision du jour, so it is no surprise that many IT managers don't know what to make of the new "borderless network" rhetoric coming from Silicon Valley. Does this term signifiy a new network architecture built for new cloud computing requirements or is it just a new label for today's LANs, WANs, and public network infrastructure? While market cynicism is certainly understandable, borderless networks isn't a Madison Avenue creation; rather, this trend is extremely important and already well underway. ESG offers this warning to IT and business executives: ignore the borderless network evolution at your own peril!

This white paper provides a brief overview of borderless networks, discussing why this transition is an inevitable outgrowth of current business and technology trends. It also addresses a critical question: if borderless networks are already evolving, how can they be secured? ESG concludes:

- **Current security defenses are a mismatch for borderless network security requirements.** Today's security point tools create "islands of security" constrained by independent threat, systems, and policy management. These disparate point tools are antithetical to the dynamic and integrated security required for borderless networks to fulfill their "any user, any content, any location, any time" promise.
- **Borderless network security demands an architectural approach.** Borderless network security demands the teamwork and cooperation of a symphony orchestra where all of the individual instruments come together to achieve a common goal. Accordingly, disparate security technologies must take advantage of the value of a common network by sharing information, setting up trust relationships, and acting on common policies. Given the "borderless" aspect of borderless networks, security defenses must also extend beyond the enterprise network to mobile devices and cloud services.
- **Borderless network security architecture demands strong leadership and industry cooperationeffort.** Borderless networks are all encompassing—corporate LANs and WANs must coordinate activities with service provider networks, distributed endpoints, and the Internet itself. No one vendor has all of the security products or resources to tackle this challenge alone; borderless network security will require industry ingenuity and collaboration. Leading security and networking vendors will form tight partnerships. Eventually, the fruits of this labor will be extended to the networking and security industry at large.
- **The borderless network architecture will evolve in phases.** As mentioned above, the borderless network architecture demands a concerted multi-vendor effort over time. Therefore, ESG believe it will evolve through three phases:
    1. The partnership phase where leading vendors integrate and validate solutions, cooperate on go-to-market programs, deliver solutions guides, and coordinate on customer education.
    2. The systems phase where vendors build advanced borderless network security functionality on top of a coordinated multi-vendor platform.
    3. The architectural framework phase where a number of vendors collaborate on common services, standard APIs, and a consistent data model. Ultimately, many of the aspects associated with this framework will be adopted by the entire networking and security industry.

Borderless Networks: The Time is Now

There is an old hypothesis in the IT industry, referred to as the "network effect," which states that the value of a communications network is proportional to the square of the number of users connected to the network. In more pedestrian terms, more users lead to more possible unique connections and thus more types of potential interactions.

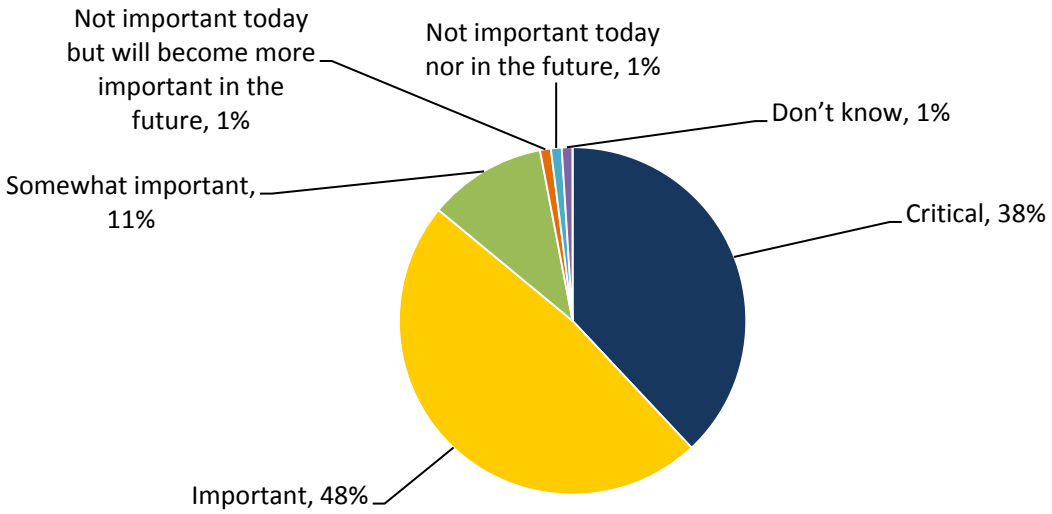
The network effect assumes connections and basic communications, but today's Internet offers far more than the exchange of TCP/IP packets. Network effect benefits are now super-charged because of:

- **Rich content use.** Early exchanges of TCP/IP packets and HTML pages have given way to Web 2.0 applications, IP telephony, and video. In fact, video content makes up about 60% of all Internet traffic today and, by 2013, video traffic will grow approximately 500% and make up about 90% of all global consumer traffic. Rich content amplifies the network effect by providing new ways for communications, collaboration, education, and entertainment.
- **Mobile users and devices.** Wireless broadband networks and mobile devices are everywhere. Many companies now purchase more laptops than desktop computers. Additionally, laptops are being joined by an army of Internet-ready mobile devices. It is estimated that over the next three years, 1.3 billion new mobile devices will be connected to the Internet. Businesses are using mobile devices in a myriad of ways. According to ESG research, large organizations are using or plan to use mobile devices for e-mail, Intranet access, custom applications, industry-specific applications, and many others. Far from a novelty, large organizations now consider mobile devices as either critical or important to their business processes and productivity (see Figure 1).
- **The consumerization of IT.** Cheap technology and the Internet are working together to democratize IT as we know it. New workers tend to be more techno-savvy than their predecessors as they have grown up with PCs, Internet connectivity, social networks, and mobile devices. This has led to the consumerization of IT—the latest and greatest applications and innovation comes through the corporate door via the workforce, not the CIO, application development team, or IT analyst.

Taken together, these trends are driving consistent innovation of network-based business processes as the Internet morphed from a network to a platform for integrating supply chains, exchanging information for business intelligence, outsourcing entire business functions, and establishing new relationships. This trend will only accelerate as cloud computing matures.

Figure 1. Large Organizations Consider Mobile Device Use "Critical" or "Important"

How important would you say the use of mobile devices by employees is to your organization's business processes and productivity? (Percent of respondents, N=174)



Source: Enterprise Strategy Group, 2010.

Internet Business Models Demands a Borderless Network

The trends described above have led to unprecedented business creativity where smart firms look for new connections for driving revenue, increasing productivity, or cutting costs. In this model, traditional enterprise network borders inhibit network business process potential. To participate in rather than hinder business progress, large organizations are already moving to a new model known as "borderless networks." Cisco Systems, one of the pioneers of this concept, defines borderless networks as:

> *Cisco's next-generation architecture to enhance customer relationships and lower operational expenses, connecting anyone, anywhere, using any device, to any resource – securely, reliably, and seamlessly.*

In parsing this sentence, the term "borderless network" is not a marketing label for existing network infrastructure. Rather, borderless networks represent a new:

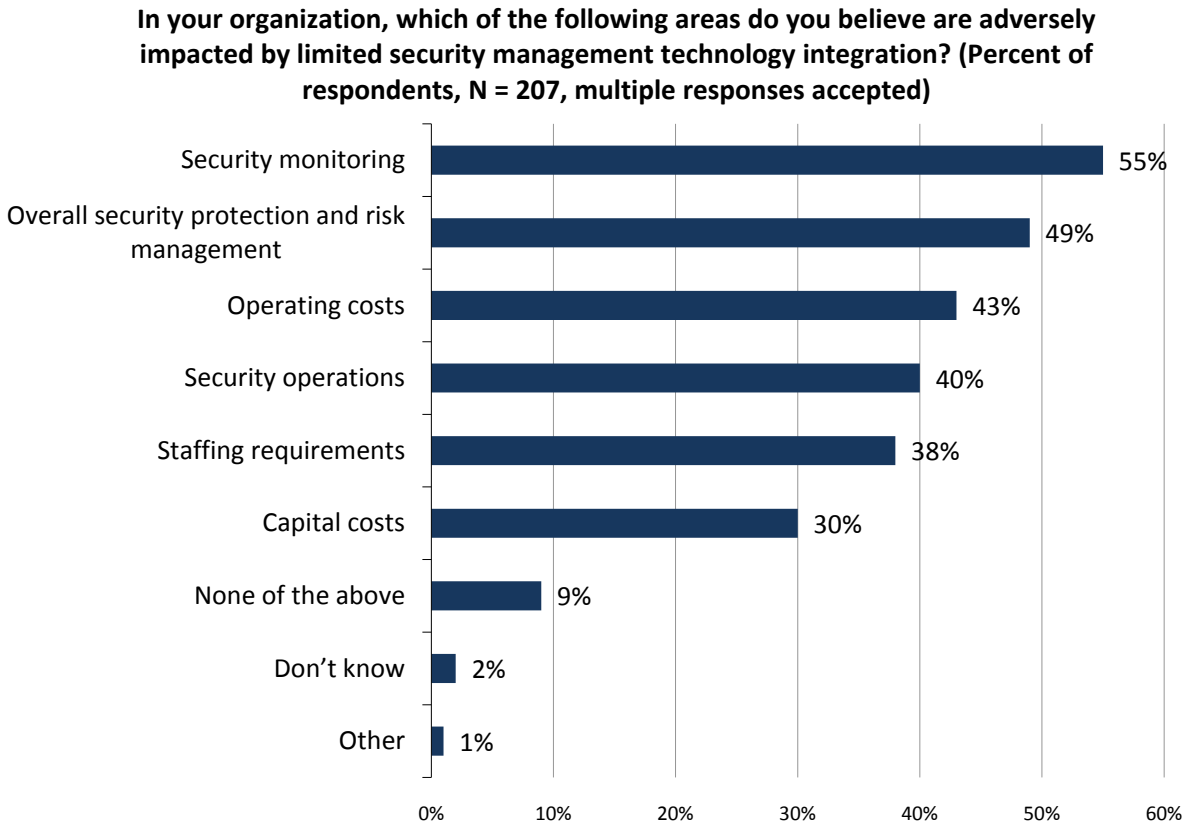
- **Network architecture.** Borderless networks are made up of physical and virtual components and integrated services that interoperate and cooperate to deliver content from any network node to any other network node regardless of whether the nodes are users, applications, or IT equipment.
- **User- focused security model.** "Borderless network" is a bit of a misnomer in that a border still exists. Rather than living on the network, however, the new border now surrounds the actual users and his or her computing devices. Borderless networks can enforce policies and protect users by understanding their identity, location, and activity.
- **Method for network performance.** Borderless networks are context-aware, meaning that they understand both the user and what's happening at Layer 7. As a result, borderless networks can then make real-time decisions in order to prioritize latency-sensitive video content while throttling e-mail traffic.
- **Transparent user experience.** The goal here is to get the user what he or she wants from any network location at any time—without user intervention. With borderless networks, the network does the technical work, freeing users to be more productive, creative, and happy.

What About Borderless Network Security?

While the business vision around borderless networks is certainly compelling, it will scare the pants off of security professionals. At its roots, borderless networks consider all IP networks as an extension of corporate LANs and WANs—in other words, one global untrusted network for transporting sensitive and non-sensitive content to employees, suppliers, business partners, and customers. Yikes!

CISOs have just cause for this trepidation—today's security is no match for the dynamic nature of borderless networks. Why? Most large organizations built their cybersecurity defenses in a piecemeal fashion. Early implementations of firewalls and PC antivirus software were joined over time by IDS/IPS, e-mail security, URL filtering, and a potpourri of other security software and appliances. The result of this organic growth is islands of security rather than a security architecture. According to ESG research, limited cybersecurity integration can lead to lots of problems with security management in areas such as monitoring, risk management, operating costs, etc. (see Figure 2). Given the scale of borderless networks, these issues will grow exponentially.

Figure 2. Security Management Problems



Source: Enterprise Strategy Group, 2010.

Borderless Network Security Demands an Architectural Approach

In spite of CISO pleas, creative organizations will rapidly embrace new Internet-based business models, applications, and rich media. Smart CEOs will recognize that these opportunities do come with increased risk and instruct their IT teams to build a security infrastructure to address the governance, risk management, and compliance requirements commensurate with the new borderless network model.

It is important to recognize that this challenge must not be addressed as cybersecurity business as usual. Rather, CISOs must implement a borderless network security architecture that maps to the user-centric, context-aware, rich media properties of borderless networks themselves.

What will this architecture look like? First, borderless network security will be made up of several foundational technologies that resemble existing safeguards, but are tailored for the new borderless needs (see Table 1). These technical pillars include:

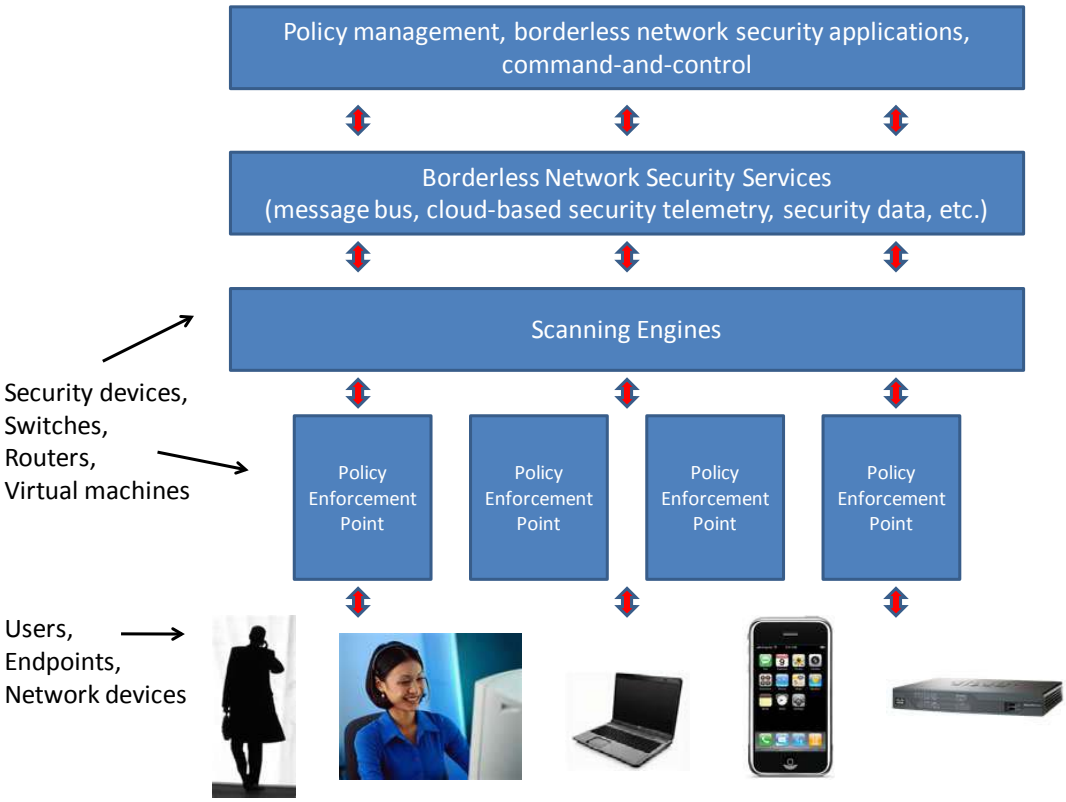
- **Scanning engines.** Borderless network scanning engines inspect network content from Layer 2 through Layer 7, assuming the role of firewalls, IDS/IPS, network proxies, Web gateways, etc. These scanning engines will be located throughout the corporate network, but will also rely on cloud-based services for security intelligence, real-time updates, and scanning support for mobile users, remote offices, and public network-resident devices like network sensors or SCADA systems.
- **Security everywhere.** Rather than rely on dedicated appliances, security will be "baked" into the network—in routers, switches, security devices, and virtual servers. The objective is to layer security throughout the borderless network to protect users, IT assets, and data.
- **Distributed shared security intelligence.** Log files, vulnerability scanning data, system configuration, and event data will all be available on a "publish and subscribe" basis in industry standard formats. Additionally, on-site security information will be supplemented by security telemetry in the cloud. All of this data will be available to analysts for event detection and forensics, but the network will also consume this data itself in order to react to anomalies, enforce policies, or block attacks in real time.
- **A policy management layer.** Security policy will be managed in central locations and then enforced throughout the network based upon context-specific variables. When an executive on an untrusted network in Moscow checks e-mail via Outlook Web Access (OWA), she can view messages but precluded from downloading attachments.
- **Intelligent devices and endpoints.** PCs and mobile devices will be active participants in borderless network security in several ways. All endpoints will authenticate themselves to the network and submit to a health and configuration check before gaining access. This will be true for employees as well as third party users. Once admitted to the network, endpoints and users will be given access to specific applications and data based upon parameters like user role, location, time of day, etc. This will not require multiple authentications; rather, the network will understand whether a user is working at her desk, her home PC, or from an untrusted network around the world and then enforce policies for access controls, data confidentiality, and encrypted transport accordingly. Finally, endpoints will continue to have onboard security defenses, but this will evolve from today's fat client software to a cloud-based model—especially for mobile devices with limited resources.

Table 1. Foundational Security Technologies of Borderless Networks

Security Technology	Current Characteristics	Borderless Network Characteristics
Scanning engines	Deployed as independent devices on top of the network. Separate administration, operations, and policy management.	Deployed across the physical network with integrated visibility, administration, operations, and policy management.
Form factor	Typically stand-alone hardware appliance or UTM. Security scanning makes the network architecture more complex.	Built into networking equipment, but also deployed as security appliances and virtual machines. Security integration into the network simplifies the network architecture.
Security intelligence	Distributed on the enterprise network. Independent security devices make security intelligence extremely difficult to coordinate, consolidate, or act upon.	Distributed on the enterprise network and in the cloud. Standards-based information interoperates with messaging middleware for information sharing across the network, cloud, and security applications.
Policy management	Built into individual security technologies with their own policy enforcement. Independent of the actual network.	Central policy management with distributed shared enforcement. Tightly integrated with network.
Intelligent devices and endpoints	Limited device authentication. Security of devices relies on resident security software and signature updates.	Ubiquitous device authentication and policy-based enforcement. Device security depends upon lightweight agents and cloud services.

All of the security technology pillars described above work in lockstep with the network itself in order to accelerate business-critical traffic while blocking malicious code or policy violations. To accomplish this, borderless security depends upon an architecture featuring distributed security enforcement, open APIs, industry standards, common services, data sharing, and central policy management and reporting (see Figure 3).

Figure 3. The Borderless Network Security Architecture Stack



Source: Enterprise Strategy Group, 2010.

Borderless Network Security Must be a Cooperative Effort

The objective of borderless networks is to provide any users with access to any service from any devices on any network at any time. This in itself is quite an ambitious technology goal, but when you also want to accomplish these tasks with guaranteed security, it can seem absolutely daunting—yet this is exactly what is needed to enable a continuous evolution of network-based business processes.

Given the lofty goals inherent in borderless networking, no single security vendor can possibly provide all of the components necessary for integrated security architecture. Even large security vendors offering integrated security suites don't go far enough. These vendors will certainly have a big footprint, but no one vendor has everything from network access control to identity management, to cloud-based threat management, nor will they provide security functionality that integrates with network devices and virtual appliances throughout the network. Finally, while borderless security architecture is a new model, it must not force users into "forklift upgrades." Rather, large organizations must be presented with graceful migration strategies, investment protection, product choices, and implementation solution guides.

Borderless Network Security Evolution

Large organizations and savvy security vendors already understand that borderless networks will require industry collaboration and evolutionary development. ESG believes this will occur over three distinct phases (see Table 2):

1. **Partnership phase.** Leading networking and security vendors will form tight partnerships in order to integrate best-of-breed solutions. Early on, this will focus on vendors creating validated solutions and solutions guides for borderless network security deployment and operations. Vendors will also cooperate on go-to-market activities (i.e., sales and marketing), cross-training, field engineering, and technical support. Successful vendors will recognize that limiting the number of partners they work with is necessary in order to do appropriate solutions testing, configurations, and customer education.
2. **Systems phase.** After an initial period, vendors will begin to develop more advanced borderless network security functionality on top of mutual security systems. This will include tighter integration, data sharing, and common command-and-control. As this occurs, vendors will reach out to the broader security and networking industry and begin to promote standard protocols and APIs.
3. **Architectural framework phase.** Finally, network and security industry leaders will come together to create an integrated security framework for integration, policy management, data formats, real-time data exchange, and security policy enforcement. A good deal of focus will be on defining and implementing common policy management and distributed policy enforcement.

Table 2. The Three-Phased Evolution of Borderless Networks

Phase	Focus	Deliverable
Partnership phase	Borderless network security partnerships established by leading security vendors. Work will focus on product integration, go-to-market, education, and deployment.	Validated solutions, solutions guides, training, technical documentation.
Systems phase	More advanced product integration. Development of new borderless network security functionality on top of multi-vendor platform.	Complex validated solutions with specific use cases, initial delivery of common services, data models, and APIs.
Architectural framework phase	Broader industry effort to define how disparate products communicate and interoperate with each other. Distinct effort on policy management and enforcement.	Industry standards, RFCs, reference architecture, NIST/ISO support.

While borderless network security ultimately demands multiple vendors and, ultimately, industry support, security and networking vendors will come to this realization in different ways. Some will try to put a proprietary stamp on borderless network security, some will be dragged reluctantly into partnering and industry collaboration, and some will see the writing on the wall and approach borderless networking security as a cooperative effort from the start.

Cisco Systems, a networking and security leader, is already marching down a collaborative path to make borderless networks and a borderless network security architecture a reality. Cisco has already recruited partners such as ArcSight, Credent, LogLogic, Lumension, netForensics, RSA Security, Sophos, Splunk, and Trend Micro to deliver validated complete solutions that address its customers' business problems. Cisco is also building borderless network security into its broad portfolio of networking and security products and offering specific new borderless network security products like its AnyConnect client security agent and TrustSec for network authentication and access control. Finally, Cisco's recent acquisition of ScanSafe provide a cloud-based security foundation that can be used by other Cisco and partner products.

Cisco plans to move forward from its current products and initiatives with additional borderless network security products, multi-vendor validated solutions, and ultimately an open framework for creating an end-to-end borderless network security architecture that can accommodate Cisco and partner products.

The Bigger Truth

Skeptics may point to borderless networks as nothing but the latest technology industry fad, but this attitude dismisses real innovation and progress. Large organizations are adopting rich media applications. Consumers and employees are embracing new consumer technologies and mobile devices. New network-based business processes arise each day. Call it what you want, but the concepts around borderless networks are real and hard to ignore.

Since all evidence points toward a future of borderless networks, it is critically important that we figure out how to secure them. The current "islands of security" model doesn't work well today, so it is a mismatch for the scale, rich media, user-centric, and context-aware needs of borderless networks.

ESG believes that borderless network security will require a completely new model—one that comes together as an architecture rather than a series of fractured components. Furthermore, no one vendor will offer a "soup-to-nuts" borderless network security architecture on its own, rather the architecture will evolve as leading anchor vendors cooperate to offer validated solutions, solutions guidelines, technology standards, and finally a comprehensive borderless network security framework applicable for the broad networking and security industry at large.

CIOs, CISOs, and networking executives must recognize that borderless networks will demand profound security changes and plan accordingly. Smart IT managers will map out a phased transition strategy, peruse vendor borderless network security roadmaps, and work with industry product and thought leaders in this evolution.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com