

Cisco's Security Vision for the Borderless Enterprise Making Web 2.0 Safe for Business

Remote and mobile working. Mobile devices with multimedia and PC-like capabilities. Internet-based collaborative work tools. Social networking, instant messaging, and Skype. Virtualization, cloud computing, and Software-as-a-Service (SaaS). Cisco® WebEx® and Cisco TelePresence™. These Web 2.0 trends, technologies, and tools allow people to work far more efficiently, and be more connected to information and to one another, than ever before.

And with every advance in technology that enhances connectivity and communication, there's an acceleration in the migration from the "traditional" office environment, where work happens behind fortified network walls. In fact, every user today is, in some way, a mobile user—whether the user is connecting to the network or the Internet via a web-enabled smartphone or a laptop with a VPN connection.

With the clearly identifiable boundaries of the traditional corporate perimeter quickly dissolving, many organizations find they are at a critical crossroads: whether to fully embrace the value of mobility and Web 2.0 or to cling to the safety they believe is provided by their well-established security fortress.

Rethinking Enterprise Security

As business operations, behaviors, and ideas transcend both physical and network boundaries, they are shared in ways that may not be accounted for by current security models. These changes require a new way of thinking about enterprise security so threats can be averted, and those things most important to the organization—its people, operations, and assets—are protected. Anytime, anywhere, from any device.

It is security's role to help ensure that the correct people, using the right devices, are accessing the appropriate resources, while having a highly secure yet positive user experience. But effective security solutions that enhance the end-user experience require security systems with sufficient intelligence and granularity, so they can enforce policies that are much more user-oriented.

Cisco has a vision for the next-generation security architecture that is built around users, and will secure the emerging borderless enterprise. These tools are identity-, application-, and content-aware. Simply put, they can tell the difference between CNN and Skype and Oracle. They recognize users and directory structures: John Smith is in sales and can access sales force data in a cloud-based application. Jane Smith is in engineering and can access source code on an internal server.

Cisco Secure Borderless Network Architecture

Cisco defines the emerging "borderless enterprise" as "the delivery of business capabilities on demand through an architecture of virtualized resources and services that optimally provides secure, context-aware, rich media information to mobile, seamless communities of employees, partners, and customers."

The Cisco Secure Borderless Network architecture, designed to support the security needs of the borderless enterprise, is comprised of five major components:

Scanning Engines

A "supercharged" security enforcement array in the Cisco Secure Borderless Network architecture combines the best capabilities of a web proxy, a firewall, and an intrusion prevention system (IPS) to provide effective, granular security.

This is the foundation of security enforcement, and is at the heart of the new, more intelligent policies required to safely embrace Web 2.0 and the borderless network.

The security enforcement array is able to identify users and their roles in the organization and make decisions on a high level by understanding applications and content. It can permit a policy such as, “Allow Outlook web access, but when users are coming from an unmanaged endpoint, don’t allow downloads.” And it can enforce a policy that says, “Allow YouTube video streaming for marketing, but don’t let it interfere with WebEx sessions.”

Flexible Form Factors

An effective security enforcement array relies on a spectrum of form factors. Intelligent scanning elements run in a traditional appliance, or as a software module running on a router in a branch office, as a hardware blade in a data center switch, or as an image running in Cisco’s security cloud infrastructure. Regardless of the form factor, however, the scanning capabilities, policy enforcement and management, and the reporting system are consistent.

A customer might choose to put appliances in their headquarters, use integrated security modules for their branch office routers, and have hosted cloud images for mobile users. These flexible delivery options, coupled with higher-level application- and identity-aware scanners, enable policy enforcement to be abstracted from the physical network. Users get the same policy enforcement regardless of whether they are on an iPhone in India or a desktop in Denver.

Cisco Security Intelligence Operations (SIO)

The next generation of security intelligence also requires a broader look at Internet traffic patterns. Using techniques such as Cisco’s Global Threat Correlation, the ever-sophisticated and persistent waves of attacks by cybercriminals can be stopped based on the nature of the attacker, not just the nature of the attack. The foundation of this approach is having security telemetry—statistical data about the behavior of the network—built in to all scanning elements in a bidirectional exchange.

Traffic data is sent into Cisco SIO and new rules are pushed out, almost in real time. Today, Cisco SIO has the largest threat database in the world, generating more than 875,000 rules per day, and stopping new malware outbreaks, on average, more than 12 hours ahead of traditional signature availability. All devices in the Cisco Secure Borderless Network architecture deliver this proactive protection.

Policy Management Layer

This layer is distinct from the supercharged scanners that enforce policy. In the Cisco Secure Borderless Network architecture, policy management is a higher-level function that can span multiple operational devices. Cisco’s vision is to make the interface between policy and enforcement systems open and built on industry standards. Therefore, if a customer chooses to use a Cisco application entitlement system and an enterprise data loss prevention (DLP) policy manager from RSA, both should work smoothly with existing network infrastructure. This significantly reduces operational complexity for our customers because one set of policies can be enforced across a wide variety of infrastructure.

The Intelligent Endpoint

Mobility demands a different, redefined approach to security. An anti-virus suite is not the answer. Instead, an intelligent “connection manager” that sits on the edge of any device—a smartphone, a laptop, a desktop, a netbook—is what can deliver security to mobile users.

The Cisco Secure Borderless Network architecture relies on a very lightweight, pervasive endpoint. Its role is not to scan content or run signatures, but to focus on making sure every connection coming on or off the endpoint is intelligently pointed at the optimal security enforcement array element, whether an on-premise device or somewhere in the Cisco cloud.

The security enforcement array element is capable of running many more layers of scanning than a single endpoint possibly could: multiple layers of malware signatures, zero-day heuristic analysis, DLP policies, application and content categorization, and more—all in real time.

This intelligent endpoint, the Cisco AnyConnect Secure Mobility client, represents the new perimeter of the de-perimeterized network. It handles all network connections while also enhancing the end-user experience. When a user is behind the firewall, the client “oversees” the process of endpoint and user authentication. When a user closes his or her laptop at work, and then goes home and opens it back up, the AnyConnect Secure Mobility client “wakes up” and realizes it is no longer behind the firewall. It then automatically finds the nearest network attach point.

These attach points can be in any form factor. They can be appliances at corporate headquarters, a module in a branch office router, or an image in the Cisco worldwide security cloud. All of this is invisible to end users, who only know the process works and it’s easier than before. No more fumbling with passwords and authenticating repeatedly. No more struggling to establish a VPN connection. From their perspective, they feel they are always on the LAN. From IT’s perspective, they now have control and policy enforcement no matter where an end user might go: on a PC behind the firewall or on a smartphone in Timbuktu.

Broad coverage. Persistent connectivity. Advanced security that’s always on—always protecting users who are connecting to the network from any device, anywhere, anytime. This is Cisco’s security vision for the borderless enterprise.

For more information about the Cisco Secure Borderless Network architecture and Cisco Secure Mobility, please visit: <http://www.cisco.com/go/securitysolutions>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)