

Cisco Collaborate with Confidence

Connect, Communicate, and Conduct Business Securely



What You Will Learn

This solution overview helps business executives understand how to mitigate network security risks in today's changing business environment. As organizations transition to become more collaborative and IT infrastructures move to virtualization and cloud computing, security must evolve and adapt to meet the current requirements.

This overview discusses:

- Security challenges in a decentralized and highly collaborative environment
- How Cisco® security solutions can help businesses reduce risk
- Products and services that enable confident collaboration

Challenge

Revolutionary collaboration and communication tools are transforming the way businesses interact and extend their services to partners and customers. Mobile devices and virtual platforms have torn down the already-wavering notion of a network perimeter, and the line between personal and professional lives continues to blur.

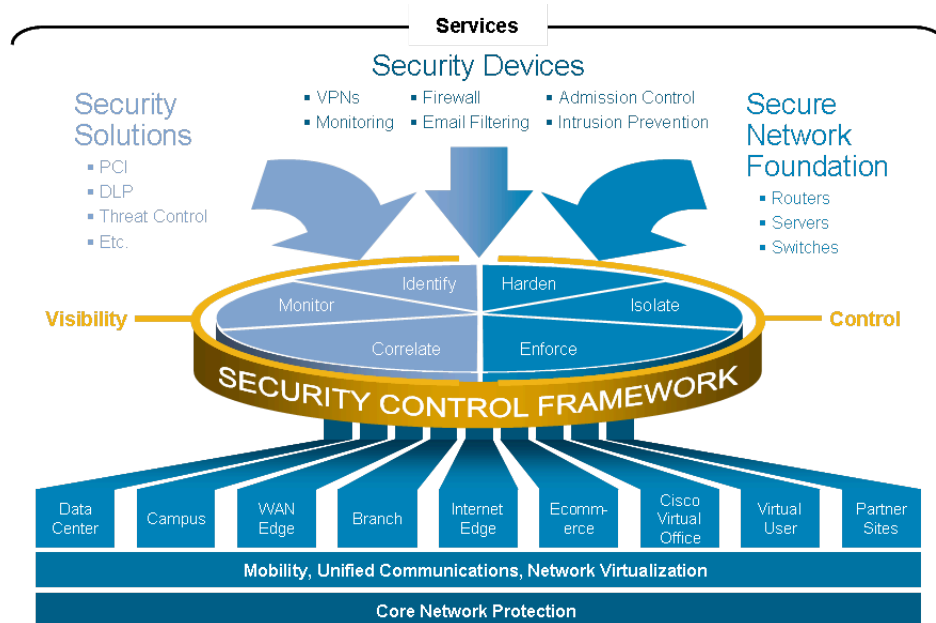
An increasingly collaborative and virtual enterprise brings unparalleled flexibility and potential, but introduces numerous risks as well. Security strategies must adapt to this changing, collaborative world. Organizations must re-imagine security as an enabling force that helps people connect and break down barriers. Security is no longer a question of how to keep people out, but how to let them in.

Solution

Cisco delivers a rich, highly secure, collaborative experience using the network as the platform, balancing protection with enablement so that users can collaborate with confidence. Through pervasive network infrastructure and security solutions, Cisco enables safe delivery of services and content, over a secure network, to protected devices.

The three advantages of Cisco security solutions are as follows:

- Comprehensive security intelligence:** Threats targeting vulnerabilities and new services continue to rise. Networks must be able to adapt to protect themselves from the rapidly evolving threats that surround them. Cisco protects organizations from the latest threats through intelligence stemming from Cisco Security Intelligence Operations. Hundreds of servers, technicians, and researchers analyze terabytes of threat data each day. This threat intelligence is used by the entire Cisco security portfolio, arming every level of network defense with a complete awareness of its environment. Combined with Global Correlation, the ability intelligently link threat data with reputation information, organizations are safeguarded from the latest threats.
- Breadth of business-enabling services:** Cisco's flexible solutions for unique business requirements include products, threat intelligence, and customized services. Options include standalone or integrated local appliance solutions, security software-as-a-service, or hybrid architectures that use both. Cisco professional services can help organizations identify and minimize redundant compliance efforts, improve security architecture and policy controls, and prioritize needs.
- End-to-end security:** Emerging forms of collaboration pose complex challenges for security architectures. Users can use many different devices to connect to the network from anywhere and access a variety of applications. Cisco enables businesses to see a complete picture of interactions, through end-to-end logical security and increased convergence between physical and logical security. Cisco simultaneously tracks personal identities, locations, devices, physical security activity and external threat activity to maintain a clear, current picture of risk. In addition, Cisco provides a security reference architecture that includes validated implementation designs and services to address the unique network security requirements for a campus, Internet edge, branch, or data center, to help you increase the security posture of your organization.



Solution Components

IT security faces a broad range of concerns, from direct threats such as mobile security and identity management to business risk management issues such as regulatory compliance and data loss prevention. Cisco security solutions address the risks faced by modern businesses.

Regulatory Compliance

Regulations add a new dimension of consequences to an already complex job. International frameworks place specific demands on many of an organization's functions and departments, such as finance, legal, and IT, from the server to the desktop, e-commerce, and online billing. Solving the problem piece by piece is not only costly and difficult to manage, but also fails to establish a cohesive security architecture. Cisco approaches regulatory compliance from the perspective of an already-integrated security infrastructure, which helps to lower costs and streamline processes.

Data Loss Prevention

Data can no longer be expected to remain in one place. Instant messaging, email, and FTP are only a few of the transmission mediums across which sensitive information can quickly travel. Data resides on laptops, USB thumb drives, and mobile devices such as smartphones. Cisco solutions do not restrict mobility—instead, they help ensure that data policies are enforced, regardless of where the data resides or travels.

Threat Management

Today's network threats are so diverse that no single solution can handle them all. Cisco takes a comprehensive approach to threat management, providing security solutions that identify threats at the endpoint, in the network, and within content by combining zero-day protection, vulnerability-guard signatures, and dynamically correlated and distributed security updates.

Secure Mobile Enterprise

No single development has shifted the traditional security paradigm more than the mobile enterprise. Sensitive data can travel from a multimillion-dollar data center to an employee's unprotected home Wi-Fi connection or cell phone in the blink of an eye. The Cisco Secure Wireless Solution protects mobile users and information with confidential communications, policy control, and comprehensive threat defense.

Identity and Access

In today's decentralized and virtualized world, a network address is no longer sufficient to properly identify a user. Cisco security solutions help enforce identity-based security and use logical and physical policies to protect sensitive information and critical business assets.

Business Benefits

Cisco can help you collaborate with confidence. The benefits of a comprehensive Cisco security solution are as follows:

- Cost savings associated with preserving brand reputation and retaining customers through mitigating the risk of data breaches¹
- Greater competitive advantage and customer satisfaction as a result of providing cutting-edge secure services

¹ Average cost of rebuilding brand and attaining customers after a data breach is \$6.6M, according to a 2008 Ponemon Institute study. <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/02/AR2009020203064.html?hpid=sec-tech>

- Savings on network infrastructure capital equipment and operating expenses through unified deployments or security-as-a-service options
- Increased workforce and user productivity by providing secure access to network resources and unified communications services
- Reduced IT security management resources through automated updates gathered from the latest threat intelligence
- Greater visibility into end-to-end security concerns through convergence between the network, logical security, and physical security
- Single-vendor service and support for unique architecture requirements

Cisco Security Infrastructure

To collaborate with confidence, security systems must support new and existing business applications. Cisco offers the following solutions to enable organizations to securely conduct business:

Network Security

No matter how much the world changes, the network will always be the bottom line. Cisco provides innovative integrated or standalone implementations of traditional network defenses such as firewalls, VPNs, and intrusion prevention solutions.

Endpoint Security

Security is no longer only about the perimeter: Endpoints such as desktops, laptops, mobile devices, or even the cloud itself must be secured as well. Cisco endpoint security solutions help ensure that end users can access and use data freely, regardless of location, while the information remains secure and policies are enforced.

Content Security

Today's world is defined by information and communication, from the web to email to IM conversations. Some of the most dangerous threats targeting end users and data come in this form, such as phishing, spam, and other social engineering attacks. Cisco content security solutions apply the latest advances in analysis and filtering to ensure confidence as users read, browse, download, and converse.

Application Security

With the focus on data, it is easy to lose sight of the tools used to access, create, and organize it. To protect against the "human threat," whether accidental or intentional, businesses need to be aware and enforce who uses applications under what circumstances. Cisco application security solutions help organizations monitor application vulnerabilities and tightly control application behavior on a situational, per-user basis.

Physical Security

Increased globalization requires organizations to extend networks and facilities to internal and external users around the world. Therefore, it becomes equally important for businesses to integrate physical security into the network to understand physical location as it relates to network collaboration. Cisco physical security solutions provide broad network-centric capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security.

Security Management

As an enterprise grows, overseeing its security becomes a progressively significant task, often resulting in efficiency drains that cost time and money. With Cisco security management solutions, policy can be written once and applied everywhere, multiple configurations can be managed by flexible tools, and the entire monitored infrastructure can be aggregated into a single feed. Through centralized management, organizations can lower operational cost, minimize errors, and maximize regulatory compliance.

Security Services

Cisco Security Services help organizations maintain their network health, protect and enhance their infrastructure investments, and create intelligent, trusted, resilient networks that allow them to collaborate with confidence. Cisco Security Services address all aspects of planning, deploying, operating, and optimizing the network to help shorten implementation times and reduce operating costs while helping organizations build networks that support their business goals.

Why Cisco?

With increased collaboration and fewer structured boundaries, organizations must rethink security as a way to enable productivity, innovation, flexibility, and customer intimacy while reducing risk. Cisco remains committed to neutralizing threats and maximizing the possibilities of the future. With a constant eye on the global landscape, services catered to unique business requirements, and the most comprehensive end-to-end security visibility, Cisco is uniquely positioned to help organizations eliminate the inherent risks involved with being connected—allowing confident collaboration.

For More Information

For more information, call your Cisco representative or reseller today, or visit us at <http://www.cisco.com/go/confidence>.



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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. 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. (0903R)