

Building an Architecture of Trust: The Network's Role in Securing Cyberspace

A Framework for Cybersecurity in the Public Sector

Introduction

Governments worldwide are challenged with providing higher levels of service to their citizens while constraining or even reducing the cost of delivering those services—what we call the “cost/reach” equation. At the same time, technologies such as web services, collaboration, mobility, and cloud computing hold significant promise to help governments transform the way they protect the safety, health, and economic well-being of citizens while responsibly managing taxpayer dollars.

In this paper, you'll learn more about the powerful forces driving change in the cybersecurity landscape. We'll describe an innovative, architectural approach to cybersecurity we call the “Architecture of Trust,” and discover the critical steps any organization can take today to incorporate trust, visibility, and resiliency into their IT systems.

Providing Information Security in a Networked World

As networked IT systems become essential for managing the cost/reach equation, they must maintain the highest levels of service availability, data integrity, and data privacy. Networked IT systems enable connected work environments where business is conducted far beyond traditional office walls and a closed enterprise network. Employees use smartphones, handheld devices, and computers running various operating systems to work from anywhere—airports, cafes, hotels, their homes—and to access enterprise assets. Increasing numbers of nontraditional devices, such as cameras, sensors, and power meters, are being connected to networks as well.

Today, it is difficult to read a newspaper without seeing some reference to cyber crime, cyber espionage (either economic or military), and even cyber warfare. Before the days of the connected work environment, network security was simply a matter of tightly controlling the few entryways into the networks. Organizations relied on point solutions for protection against cyber threats, adding a firewall or security appliance to a network to ensure the safety of vital information. This was an adequate approach when employees were not on the move, and devices were overwhelmingly PCs running Microsoft Windows.

Now, workforce mobility and the explosive growth of connected devices mean that a network security strategy based only on securing the endpoint is no longer sufficient. There are simply too many devices and operating systems to rely on patching and virus protection alone. This shift is driving a transition in how we provide network security: from the “overlay” model of the past to security embedded in the network fabric itself.

What Is Cybersecurity?

When we refer to protecting cyberspace in the public sector, it's important to understand that we are talking about something subtly different from the Internet of popular culture. While the term "cyberspace" is rarely used in the corporate world, governments have embraced the term to refer to the networked IT systems used to provide services, coordinate operations within and between agencies, and protect national security. Although cyberspace has been a key part of national defense for at least a decade, many consider cyberspace to have cemented its position as a new, fifth military domain (after land, sea, air and space) in 2007, when various organizations in Estonia, including government agencies and media outlets, suffered through denial-of-service and spam attacks.

Forces Shaping the Cybersecurity Landscape

While the challenges associated with securing cyberspace are often discussed primarily in technology terms, there are at least four global forces driving the need for a new approach to cybersecurity. In addition to the mobility of devices, data, and people, government agencies are wrestling with the impact of globalization, the shift to virtualized and cloud-based services, and the changing demographics of the workforce. These powerful forces are rapidly forming a new landscape in cybersecurity and have largely upended our old notions of how to secure information systems against aggressive action by cyber criminals.

To combat cybersecurity threats and respond to these forces of change, organizations must supplement their reliance on endpoint security with a more effective and integrated architectural approach—one that encompasses all of the technology, people, and processes required for the privacy, integrity, and availability of network information and resources.

It's interesting to note that government organizations have historically faced special challenges in preventing cybersecurity incidents. Often, governments must cope with an acquisition and deployment cycle of many months or even years, which almost guarantees that any technology is obsolete as soon as it is put into use. This slow implementation can be exacerbated by regulations and complex legal requirements governing the implementation of new technology.

As in the private sector, government agencies often face delays in adopting the latest and smartest cybersecurity solutions because they simply don't have the talent on hand to bring about these dramatic advancements. Many government agencies struggle to compete for top talent as the demand for cyber professionals grows across many sectors.

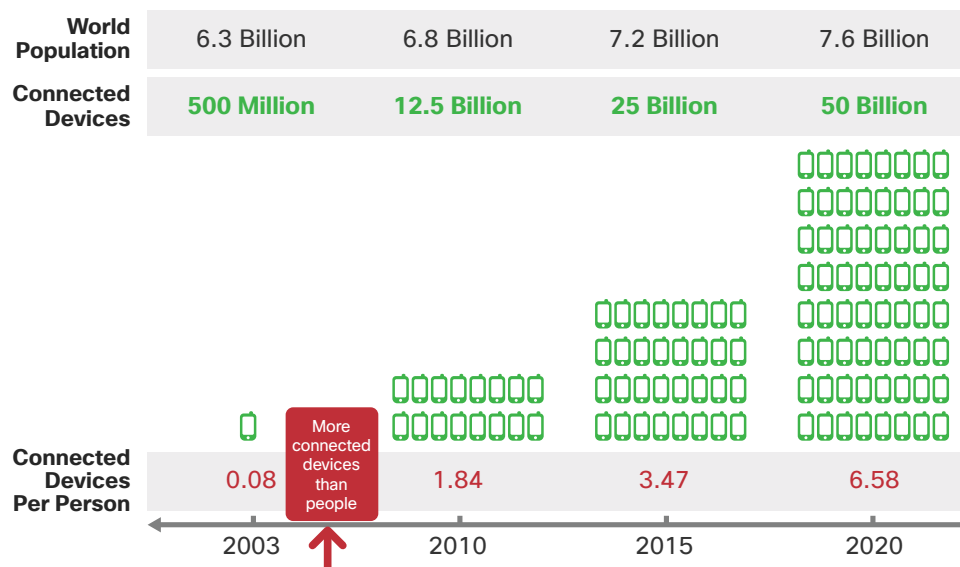
Along with these perennial challenges have come dramatic changes that are reshaping the way IT professionals manage and interact with information. These changes have a significant impact on how we must approach cybersecurity.

The Technologic Shift

In 2003, according to both the U.S. Census Bureau and Forrester Research¹, there were about 500 million connected devices—that is, devices such as smartphones and laptops that can connect to the Internet and other networks—in operation worldwide. That's almost one device for every 10 people. In 2010, that number skyrocketed to 12.5 billion devices, or about two devices for every person on the planet². In just five years, those numbers are expected to grow to as many as 25 billion connected devices in operation, with a projected 50 billion connected devices by 2020. Figure 1 illustrates the immense growth expected over the next decade.

1. "Total Midyear Population for the World: 1950-2050," U.S. Census Bureau, 2010, <http://www.census.gov/ipc/www/idb/world-pop.php>; "Forrester CEO: Web services next IT storm," Forrester Research, 2003 <http://www.infoworld.com/t/platforms/forrester-ceo-web-services-next-it-storm-873>.

2. "Total Midyear Population for the World: 1950-2050," U.S. Census Bureau, 2010; Cisco, 2010 <http://www.census.gov/ipc/www/idb/worldpop.php>.

Figure 1. Projected growth of connected devices and devices per person by 2020.

These are startling numbers, but if you've charted the devices in use within many organizations, this data may not surprise you. Ten years ago, workers might have had a laptop—but it may not have even connected to the office network. They also might have had a primitive cell phone, but since it didn't do anything but make phone calls, it didn't pose much of a threat to security. Now, employees and their workplaces have laptops, smartphones, tablets, digital cameras, digital printers, wireless routers ... the list goes on.

In commercial enterprises, this adoption of new technology has been called the *consumerization* of IT. Workers have embraced new and useful devices that make their home lives more entertaining and productive, and they are petitioning their employers to let them use these devices at work as well. Thus, instead of technology innovations trickling *down* from enterprises into consumers' hands, innovations are trickling *up* from consumers.

A similar phenomenon is happening in government: the *commercialization* of government and defense IT. For instance, many of the innovations in use by the military today started out as commercial off-the-shelf (COTS) technologies. Examples include Wi-Fi, which is used in tanks to help soldiers communicate on the battlefield, and digital video cameras, which soldiers employ as reconnaissance and situational-awareness tools.

For both private and public enterprises that have integrated mobile and connected devices into their workflows, the old cybersecurity strategies cannot be applied to this new technological landscape. The older, simpler method was simply to download a patch for Microsoft Windows, the standard OS in use at most offices. Today, there isn't just one OS to protect—there are dozens. There aren't just a few endpoints—there are thousands. These endpoints and operating systems present opportunities for criminals bent on using networks to support criminal enterprises. The only logical approach to security is integrated and architectural: security must be "baked" into the network independent of the operating systems and devices in use.

The Economic Shift

Today, virtualization technology is transforming the way an organization can share storage, computing, network, and application resources and make those resources available on-demand to practically any location. A workplace, private or public, used to be defined by its physical boundaries—that is, the offices that workers went to every day. Today, work is defined not

as where we go but as what we do, since the physical boundaries have little relevance. The virtualization of an organization's operations means that people can work from anywhere they can access the Internet and log into their organization's network. This workforce is mobile, and gets the job done no matter where they are or what time it is.

However, the real driver toward the virtualized "cloud" world is the cost efficiencies involved in this new consumption model. In the cloud paradigm, the marginal cost of providing services declines with each additional user. Organizations can gain access to hosted services that otherwise might be too expensive to purchase or too difficult to implement. They also gain the agility to operate globally, beyond the limitations of geographic boundaries or cost concerns.

The shift to virtualization presents both risks and benefits from a cybersecurity perspective. When data is moving from the network to hosted service providers, to employees' smartphones, to laptops at Internet cafés, and then back to the network, how is it being protected?

At the same time, the trend toward virtualization can offer some security benefits. For instance, if data is not resident on an end device, it can be much more difficult for criminals to gain access to data than it was when they could simply steal the device. Cloud-based data offers availability in case of a business disruption, such as denial-of-service exploits targeting systems and infrastructure. Finally, virtualization presents the opportunity to implement a "moving-target" defense in which the physical and logical location of resources can be changed. With the shift to cloud services, managers should not miss the opportunity to update policies about exactly how their information assets will be protected.

To sum up: while virtualization presents valid cybersecurity concerns, it can also be a tremendous boon to forward-thinking organizations in the public sector. We must deal head-on with cloud computing's security upsides and downsides because virtualization is not going away.

The Demographic Shift

Depending on how old you are, social networking—via services like Facebook and Twitter—is either a frivolous waste of time or an essential tool for communicating with colleagues and getting work done. If you're in the former camp, it's time for a reality check: Younger members of the workforce are dead serious about using social networking at the office. These "digital natives" do not view social networks as an alien technology; they are as comfortable with them as prior generations were with the telephone.

The "millennials," as people born between the early 1980s and the late 1990s are commonly called, have brought social networking and web-based tools (not to mention consumer devices) into the workplace, and are pushing managers to consider how to balance the need for access to these tools with the need to manage security. This demographic shift is also forcing managers to confront changing attitudes about information security, since millennials are generally more comfortable sharing and sending information outside of a closed network. (They've grown up on social networking in which everything from birth dates to relationship status is freely exposed to the public. Millennials sometimes carry this same casual approach to privacy into the workplace.)

Organizations that have so far resisted this demographic shift—sometimes by putting social networking tools in the same category as online games or entertainment and banning their use at work—will find it increasingly difficult to attract the younger talent they need. The use of social networking solutions in the workplace also can result in higher productivity, faster decision-making, and more effective collaboration. Figure 2 shows how the companies surveyed in "The Connected World Report" view access to online applications in the workplace.³

3. "The Connected World Report," Cisco Systems, Inc. and Insight Express, 2010: http://newsroom.cisco.com/dlls/2010/ts_101910.html.

Figure 2. Restricted Access to Online Applications.**Q. To which of the following websites and/or applications does your company currently restrict access?****Social media use is restricted to varying degrees around the world and per company**

- » More than 2 out of 5 (44%) said they are restricted from playing online games
- » 2 of 5 (41%) said they are restricted from using Facebook at their jobs
- » 1 of 3 (35%) is restricted from using Twitter at work or with work devices
- » More than 1 in 4 (28%) workers is restricted from using Instant Messaging (IM) at work or with work devices
- » 1 in 5 (21%) is restricted from doing personal email on work devices and during work hours



There is a better, smarter alternative to banning social networks or limiting their use: Building a comprehensive policy for social media that assumes employees, wherever they are working, will use collaborative tools and share information among social networks and devices. Instead of banning the use of social networks outright, organizations should set guidelines for their use, and tell workers what is and is not appropriate to share. The goal is to create a culture of Yes around social networking, instead of a culture of No.

The Geopolitical Shift

Just as the perimeter of the organizational network has disappeared, political boundaries are fading in importance in the cybersecurity landscape. Security threats in cyberspace aren't constrained by national boundaries, particularly as more workers conduct business from wherever they can access the Internet. This makes it more important than ever for law enforcement agencies to have a policy and operational framework to work together across national borders, while respecting privacy and civil liberty laws in each country.

This globalization extends to the supply chain of IT suppliers—in both good and bad ways. The good news is that the IT industry has developed an ecosystem wherein a laptop may be made of components from around the globe, driving down costs and encouraging innovation and efficient processes. The bad news is that adequate controls to ensure the security and integrity of those products must be implemented and enforced in every link of the global supply chain.

The globalization trend adds uncertainty to the process of doing business across borders: Large economic powers are now dependent on each other, and can't afford to set rules about the supply chain based on geographic borders. So, how do we take advantage of the global economy without putting national security at risk?

Virtually every industrialized country around the world is struggling with this balancing act. More and more, governments are focusing on ways to ensure the integrity of the IT systems on which they rely. As this trend continues, both industry and government will need to adopt methodologies that work globally. The adoption of international guidelines and standards helps ensure that industry can meet the increasing need for security certifications in the public sector while continuing to maintain an appropriate pace of innovation. For example, as of 2010, 26 countries had adopted the Common Criteria Recognition Arrangement to help them ensure that the IT products they buy conform to pre-established security standards.

Bridging the Innovation Gap

*"Change in cyberspace has accelerated and shows no signs of slowing down. We will need to stay abreast of this continued pace of change if we are to remain ahead of our adversaries."*⁴

—Rob Carey, former CIO, U.S. Navy

While many organizations are taking a more proactive approach to strengthening network security—and becoming more vigilant about monitoring the ever-changing risk landscape—others continue to view security as an afterthought. Many organizations in both the public and private sector also aren't placing enough emphasis on finding ways to increase dialogue and cooperation with each other, which is essential to improving cybersecurity.

Meanwhile, online criminals are increasingly collaborating against us. Cyber crime operations are like companies in the commercial business world: They use technological innovation to their advantage to displace the competition and thrive.

To survive and protect themselves from cyber threats, organizations in the public and private sector must be just as nimble as the criminals. The first step toward increasing agility is to understand just how rapid the cyber criminals' development and deployment cycle is. Malicious technology can be deployed as soon as it is developed—cyber criminals are not delayed by long procurement cycles or the need to adhere to compliance regulations. Cyber criminals also have been early adopters of innovations such as social networking tools and are using them not only to achieve and profit from their sinister objectives, but to enhance their communications, refine and promote their areas of expertise, and speed their transactions with each other.

As reported in the *Cisco 2010 Midyear Security Report*, for example, cyber criminals around the world are using social networks as an online marketplace for stolen credit cards. And terrorists worldwide are relying on social networks as a tool for organizing and recruiting, and sharing knowledge with each other.

Government organizations and private enterprise must become better than cyber criminals at sharing information and lessons learned; being able to anticipate, mitigate, and prevent threats; and using new technologies to their advantage. Organizations also should take the time to build a working relationship with law enforcement, so that in the event of a cybersecurity incident, both sides know how to help one another.

Organizations also must ensure their networks are architected to adapt—quickly and securely—to ongoing innovation. Secure, resilient networks can form not only the foundation for effective cybersecurity, but also the cornerstone of stable society. Policies that are driven by the evolution of the network, and that promote security and innovation, also are essential.

Defining the Architecture of Trust

The four powerful forces described earlier are redefining how we must address cybersecurity. Now that simple, perimeter-based approaches are no longer sufficient, we must find new ways to provide information security based on an architectural approach for cybersecurity. We call this approach building an Architecture of Trust.

What we mean by "trust" in this context is an expectation of performance, based on high-integrity systems, that is verifiable by an objective audience. The concept of trust has gained traction in cybersecurity, since it applies equally to the people, processes, and technologies that make up any IT system.

Examples of this kind of trust exist in many different areas of IT today. For instance, Trusted Computing is based on implementing security through endpoint devices, such as a laptop or smartphone. The Trusted Internet Connection Initiative focuses on implementing security via enhanced access control. And Trusted Identity Management provides an identity management framework that supports methods such as multifactor authentication.

While each of these approaches has their place, alone they cannot provide organizations with a solution for managing cybersecurity risks. Only an architectural approach provides the framework, and the missing pieces that can meet the newest security challenges—allowing for the protection of network assets, detection of security breaches, and appropriate remediation once a breach has been detected.

4. "Departing Navy CIO Urges IT Evolution," Elizabeth Montalbano, InformationWeek, September 10, 2010, <http://www.informationweek.com/news/government/leadership/showArticle.jhtml?articleID=227400147>.

Trusted Processes, Trusted Systems, and Trusted Services

A comprehensive Architecture of Trust combines a solid technology architecture with a well-defined business architecture. The latter includes an organization's security policy and standards for IT system design. Equally important, the business architecture outlines the operational processes used to ensure the ongoing security and integrity of the network, including training, deployment, monitoring, audit, and technology refresh processes. With its trusted processes, systems and services, the Architecture of Trust, as seen in Figure 3, enables you to identify and manage risk, prevent and detect threats, and respond to and recover from malicious incidents that occur in the network.

Figure 3. The Architecture of Trust



Trusted Processes

Trusted processes form the foundational layer. They are the building blocks that allow organizations to plan, prepare, deploy, implement, and operate the products and systems that help them mitigate risk and strengthen security. Trusted processes include all the operational disciplines related to managing the network, including training, design, acquisition, deployment, and monitoring.

Trusted Systems

Trusted systems represent the middle layer in the Architecture of Trust. Trusted systems consist of the hardware and software that make up the networking, computing, and storage infrastructure. They are systems in which integrity of both the hardware and software elements and the interaction of these elements have been designed and produced with an emphasis on security, and meet globally accepted standards for integrity and security. Trust at the systems layer is established through two key elements: product assurance and supply chain integrity.

- **Product assurance** encompasses all elements in design and product development that ensure the integrity of hardware or software products. Product assurance can include good software development practices that protect against common, security-related faults such as buffer overflow exploits. It can also include processes for managing the security of any third-party code that may be incorporated into the product. In addition, trusted software must work with trusted hardware to support appropriate methods of image signing to help ensure the software running on the system has not been modified without authorization.
- **Supply chain integrity** is the other critical element in the trusted systems layer. In addition to assuring the integrity of the product, the process by which the product is manufactured (or in the case of a software product, the process by which the code is developed) must also conform to appropriate security standards. Processes put in place at each link of the supply chain, including manufacturing, assembly, and distribution, must provide protections against tampering or insertion of malicious hardware or software.

It is important to understand that the trusted systems layer in the Architecture of Trust relates not only to the integrity of individual elements such as routers or systems, but also to the infrastructure as a whole, and how it performs. This requires closely managing the configuration of network devices and implementing disciplined change management. The broader goal for organizations is to have confidence in system integrity.

Trusted Services

Trusted services comprise the top layer of the Architecture of Trust. Services in this context refer to the applications and capabilities provided by the IT system. They may be provided by the network elements themselves, by discrete devices, by providers such as Cisco, or by independent systems supplied by other parties. Examples of trusted services provided by the network include intrusion detection and prevention, Network Access Control (NAC), and Identity-Based Networking Services (IBNS). Instrumentation, diagnostics, and sensing are examples of services provided by Cisco and other suppliers that are increasingly important for organizations navigating today's cybersecurity landscape.

Differentiated trust is an important element in any architectural approach to cybersecurity. Not all information assets have equal value, and not all assets are worth protecting to the same level. The weight of an IT asset is a factor of its value, its vulnerability, and the cost of protecting it. While it is never possible to remove all risk, it is possible to manage that risk in a way that delivers the right balance between access and security. By understanding which information assets are high value, medium value, and low value, organizations can apply differentiated levels of protection that reflect varying levels of trust.

What about “Untrusted” Endpoints?

The Architecture of Trust, while rooted in the idea of system integrity, also must be inclusive of *untrusted endpoints* that may come in contact with an organization's network at any time.

In today's enterprise network environment, the integrity of every endpoint device cannot be guaranteed. Any new device connected to the network should be categorized as “untrusted” and limited to a restricted area automatically until the permissions of the device and its user can be properly determined.

In addition, some organizations may want to allow for limited access by unknown or untrusted endpoints. For example, an organization may want to provide guest network access for visitors, but constrain that access only to certain resources.

There are also many different levels of trust between the two extremes of “trusted” and “untrusted.” Therefore, within the Architecture of Trust, there must be room for some measure of “untrust” that inevitably will occur, at least temporarily, in many acceptable circumstances.

Five Steps Toward Building an Architecture of Trust

As discussed earlier, the proliferation of traditional and nontraditional endpoints—and the shift toward the connected enterprise—are demanding a change in mindset with regard to cybersecurity. The perimeter-based approach is no longer relevant because an organization's network infrastructure, and the security that supports it, has evolved into a complex ecosystem that is always changing.

In addition to embracing an architectural approach to security, there are several actions, based on some of the guidance provided by Cisco's security experts in the *Cisco 2010 Midyear Security Report*, that will help organizations better respond to current and future change and to ultimately establish an Architecture of Trust.

1. Say Goodbye to the Perimeter

Traditional network security designs were created around the concept of a secure perimeter—the “moat around the castle.” Today, both organizations and networks are becoming increasingly borderless. It's clear that a fortress approach to security is no longer adequate.

With workers collaborating and sharing vital information far beyond the walls of the workplace, every hour of every day, security limited to the network edge is bound to fail. A layered approach is the wiser course. Organizations must make certain that wherever critical data flows or resides, it is protected by intelligent technology solutions, robust policies, effective enforcement practices, and a workforce educated about security risks and their role in helping to mitigate them.

2. Get Serious About Network Management

Maintaining visibility into the critical operation parameters of the network is fundamental. IT services may be going virtual, but networks are made up of physical devices that must be configured, managed, and updated consistently. Many organizations are simply unaware of the totality of their network and the number of assets that must be managed. And there are many moving parts and areas of intermittent visibility to monitor and manage, such as mobile workers, mobile devices, web-based collaborative applications, and the cloud.

Configuration management and software version control for network devices are two areas where most organizations can make significant improvements. Organizations also should monitor vulnerability disclosures of their vendors and act accordingly to reduce their potential exposure. Securing the physical assets that make up your network—and ensuring software is up to date—are fundamental (and ongoing) steps in the process of building a robust Architecture of Trust.

3. Don't Neglect Basic Network Hygiene

Many security issues considered to be “new” problems are actually old issues that can be addressed using existing, effective practices. One word of caution, however: Organizations should start by working to solve a limited number of things and doing them well, instead of trying to solve too many things at once, only to arrive at mediocre results or unfinished projects.

Without real-time situational awareness of what is happening on your network—the “common operating picture”—you are not in a position to defend it appropriately. By taking stock of all physical assets that comprise, touch, or have the ability to connect with the network, IT teams gain better visibility into the entire network. Today's network devices provide a wealth of sensor data that provides insights into how the network is operating. Establishing a baseline of activity and performing diligent monitoring will allow IT teams to identify and correct weaknesses more easily, and remove or block users and devices that should not be connecting to the network or accessing sensitive data.

4. Build in Resilience Now

In today's dynamic environment, keeping pace with evolving security threats is not an option but a necessity. The availability of IT resources has become essential to the ongoing operations of almost every organization. A high level of system resiliency will help ensure the organization preserves its ability to "play through" a cybersecurity incident. However, it is naïve to believe that any organization is impervious to being compromised by previously undetected cyber threats. Once a breach occurs, you must be able to respond quickly to limit the scale of the incident and minimize the impact to operations, as well as put in place the appropriate safeguards.

To achieve a high level of network resilience, you must take advantage of dynamic routing protocols, redundant paths, and analysis of data collected by embedded network sensor processes. Using all these tools, you have a better chance of containing the damage done by both existing and emerging forms of cyber threats.

5. Educate Your Workforce on Security

Too often, security is considered "somebody else's job." Organizations should allow their employees to be part of the security solution by encouraging bidirectional communication about security issues. When educating users, explain the security issues the enterprise needs to address, and ask them how they can help the organization solve these problems.

The most effective training uses real-world examples to demonstrate to employees that cyber threats are genuine as well as disruptive and costly. In addition, government organizations need to shift their thinking about security from "no" to "how"—for instance, instead of banning all social networking in a bid to improve security, taking steps to protect data as it moves through these networks.

Cisco and Cybersecurity

As a leader in information security, Cisco is uniquely qualified to help develop and implement an Architecture of Trust. Cisco is not only a longtime supplier to the U.S. federal government, but also a trusted cybersecurity advisor to many government organizations around the world. Most important, Cisco is at the forefront of cybersecurity research and development.

Today's cybersecurity threats require a pervasive defense, not pockets of security or disparate overlays of technology. Cisco supports defense-in-depth and builds security into every product. Moreover, a unique set of leading practices helps ensure Cisco product integrity throughout the ordering, manufacturing, and distribution lifecycle. Customers have full assurance of the authenticity of Cisco products that they purchase through authorized channels.

Along with an advanced architecture and product integrity, Cisco can help governments achieve their cybersecurity goals. We can apply one of the industry's broadest networking and security product and solution portfolios, which can address the full range of cybersecurity deployment scenarios. Cisco offers outstanding design guidance with effective practices that include the SAFE Blueprint from Cisco for network security, plus Cisco validated designs that provide advice for how to architect, configure, deploy, and manage networks. Finally, the advanced Cisco Security Intelligence Operations (SIO) infrastructure provides the highest levels of proactive threat detection and prevention.

www.cisco.com

Conclusion

Trust, visibility, and resiliency are not new concepts, but in today's heavily connected world they are more important than ever. The forces of change, whether technologic, economic, demographic, or geopolitical, are forming a new landscape that calls for a new approach to cybersecurity: An architectural approach. Taking the initial steps to build an Architecture of Trust will help organizations of all sizes protect their information assets, detect new exploits that occur in the future, and take appropriate, corrective action to ensure the availability, integrity, and privacy of their critical IT systems.

For More Information

Visit www.cisco.com/go/security.



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.