

# Pervasive Trust—Enabling A Mobile Workforce Through Identity-Based Access

## What You Will Learn

Government IT leaders must support an inexorable move to a mobile and nimble workforce without diminishing the security established in traditional work environments. To both allow and accelerate this transition, this paper explains the powerful role of pervasive and automated policy and security controls based on identity and context. Where today's traditional technology-limited solutions hold back mobile access, new support allows identity- and context-free organizations to move forward. Today's network technologies can make user and device access decisions based on understanding "who, what, when, where, and how". By weaving reliable, dynamic controls throughout the network infrastructure, government IT leaders can facilitate telework and other forms of mobile access while preserving security and compliance.

## Introduction

As the government addresses costs and moves to a more fluid and distributed workforce, government IT infrastructure is on a one-way commute to the borderless network. The new government workforce has many permutations—employees, contractors, part-timers—and any of them might be teleworkers. This user base fluctuates in its roles, its network access requirements, and the devices it expects to be able to use. Controls based on identity and context should be woven throughout the network to make this process more automated, and thus more reliable and transparent to end users.

## The Transition to Telework

An important factor accelerating the change in access models is the 2010 Telework Enhancement Act. This act serves political desires to prevent disruption during pandemics and other disasters, to cut carbon emissions, and to compete successfully for new workers who expect flexible work styles.

"The [2010 Telework Enhancement] Act does not mandate telework or promote telework for its own sake. It asks agencies to step up efforts to implement telework to help:

- Ensure continuity of operations
- Reduce management costs
- Improve our employees' ability to balance their work and life commitments."<sup>1</sup>

<sup>1</sup> [2010 OPM Telework Report](#), February 2011

### Employees Want Flexibility—Is IT Ready?

Sixty-one percent of employees globally don't believe they need to be physically "in the office" to be productive, with 40 percent of Americans believing they need to be "in the office," while 25 percent responded "sometimes," and 35 percent "no."

—[Cisco Connected World Report](#), October 2010

### The President Wants Flexibility—Is IT Ready?

"It's about attracting and retaining top talent in the federal workforce and empowering them to do their jobs, and judging their success by the results that they get—not by how many meetings they attend, or how much face-time they log..."

—President Barack Obama, White House Forum on Workplace Flexibility, March 2010 (according to the [2010 OPM Telework Report](#))

### Regulations Insist Employees Have Flexibility—Is IT Ready?

"Under the [2010 Telework Enhancement Act](#), agencies were given 180 days from the law's enactment—until June 7—to establish a policy on working outside the office, identify eligible employees and inform them of the option. The law also requires agencies to name an official to manage telework programs, and incorporate the policy into plans for continuing essential services during natural disasters or other emergencies."

—One Hundred Eleventh Congress of the United States of America

---

Although cost savings make telework appealing—and more than 40 percent of agencies polled in the U.S. Office of Personnel Management 2010 Telework Report claimed cost savings benefits from telework—telework offers other benefits as well.<sup>2</sup> In the Fall 2010 Cisco® Connected Survey, almost half of U.S. employees with remote access said they work up to an extra hour as a result, and more than a quarter of those polled said they work an extra 2 to 3 hours.<sup>3</sup> They may work longer—and they may also work for lower salaries. More than half of the employees surveyed would accept a lower-paying job with more flexibility than a higher-paying job without flexibility. These results demonstrate that telework is a win-win for both the government and its employees.

Finally, the government must continue to win new workers with the latest knowledge and technical skills. Agencies compete for these scarce talents with the private sector, where 44 percent of employees in the United States and 57 percent of employees worldwide are able to connect seamlessly to their corporate networks from remote locations.<sup>4</sup> Remote and mobile access is now a requirement for modern work styles.

It is clear that more direct government employees will be using “telework” as a way to remain productive. At the same time, the uneasy budget climate is forcing reductions in the overall number of these workers. However, unless projects are actually eliminated or rescope, these workforce reductions and early retirements often have the side effect of increases in numbers of contractors and temporary workers.<sup>5</sup> The net number of users does not really decline; instead, the requirement for flexible and remote access actually increases.

As we inspect this less traditional workforce, we see workers carrying mobile computers of all sizes. The Cisco Connected Survey showed 59 percent of workers expected to use home computers to perform their jobs. In addition, 45 percent of employees were following the “consumerization of IT” trend by using personal devices—laptops and smartphones—to access corporate applications.<sup>6</sup> This personal-device access may be from home, but it may also be from a traditional office, or a conference room at an agency campus, or the local coffee shop. Wherever they log in, this “consumerized” workforce uses devices IT did not provide and cannot fully control.

### Making Telework Work

The US Government Office of Personnel Management’s OPM 2010 Telework study listed several barriers to adoption of telework. Security comes in fourth behind office coverage, organizational culture, and management resistance.<sup>7</sup> As shown in Figure 1, although all of these factors are important, security is the primary barrier IT can address.

---

<sup>2</sup> [2010 OPM Telework Report](#), February 2011

<sup>3</sup> [Cisco Connected World Report](#), October 2010

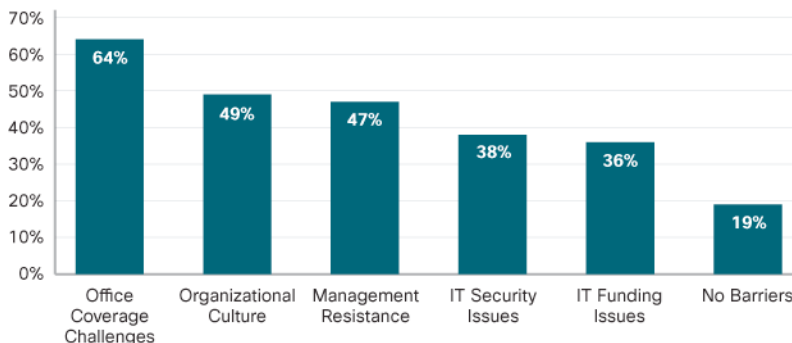
<sup>4</sup> [Cisco Connected World Report](#), October 2010

<sup>5</sup> [Lawmakers criticize growth of federal workforce](#), Elizabeth Newell, June 4, 2010

<sup>6</sup> [Cisco Connected World Report](#), October 2010

<sup>7</sup> [2010 OPM Telework Report](#), February 2011

**Figure 1.** Barriers to telework implementation



The government is in good company. Security is also the number one challenge facing mainstream enterprise IT as it supports a mobile and distributed workforce, according to the Cisco Connected Survey (57 percent worldwide, 45 percent United States).

### What Are the Security Risks of Telework?

Within the realm of security, data protection is a primary concern of both government and commercial organizations—especially under the specter of WikiLeaks. However, remote access is not the sole concern. Leaks can happen within the traditional office. More than 30 percent of U.S. IT decision makers think that data leaks are as likely inside as outside of the office.<sup>8</sup>

#### THE WEAKEST LINK

Automated policy enforcement is crucial for security. The Cisco Connected Survey showed employees are a weak link in the security chain:

- Forty-one percent of U.S. employees think "security is the IT department's problem, not mine".
- Eleven percent never think about security threats when accessing corporate information from outside the office.
- Of those employees who admit to breaking IT policies, two of every five (41 percent) say it is because they need restricted programs and applications to get their job done.
- Worldwide, 58% have allowed others to use their company-issued computer without supervision.

Complicating data protection, users cannot always be trusted to do the right thing. Users are often rushed, sloppy, unaware, or unmotivated to comply. In the Cisco Connected Survey, IT decision makers listed three primary reasons why employees ignore policy:

- Lack of concern about risk
- Confidence that IT will protect them if something goes wrong
- Poor understanding of the security implications of their actions

Cybercriminals count on this unsafe and irresponsible behavior. Social engineering—getting users to install software, hand out passwords, and ignore “common sense” or “required” maintenance—has become a central tactic in cybercrime today.

The reality is that IT has to work around the workforce in order to enable that workforce. Although it is critical that today's tech-friendly, consumerized workforce be able to perform its job where, when, and how it needs to, it is also crucial to maintain the assurance—the confidentiality, integrity, and availability—that governance bodies, employees, and the public expect.

<sup>8</sup> [Cisco Connected World Report](#), October 2010

---

## Different Rules for Different Roles

Different type of users merit different degrees of access to government networks and data. Clearly, **unapproved** users—guests, visitors, and cyber terrorists—must be rigorously controlled with tight security, especially around use of personal devices (smartphones, laptops, Apple iPads, and USB devices) and wireless access points.

With increasing mobility and device choice, **approved** users require additional supervision. When they use approved and managed devices, such as government-owned laptops and personal computers, access controls are fairly straightforward. These endpoints can be tested for compliance with malware (DAT file) levels and operating system patches before allowing access. Any noncompliant systems can be quarantined or remediated.

Antimalware protections can be placed on the endpoint, but also positioned within the network to limit exposure to these risks.

Approved users with laptops introduce new risks. When a laptop is connected to the network from home or a public wireless access point, there are few controls filtering out malware. When approved users visit risky or compromised sites, data-stealing malware can infect their systems and be carried into the office. Increasingly, targeted phishing attacks plant malware on government-oriented sites, specifically to lure privileged government users.

When approved users use **unapproved** computers, the risks mount. If they use personally owned laptops, home PCs, or smartphones, IT has limited control over endpoint software and its maintenance. However, IT can dictate the terms of access and control how data can be used on the endpoint. This sort of control is increasingly essential as organizations contemplate rolling out BYOD (Bring Your Own Device) policies for their workforce.

Often, approved users try to introduce “computer-like” Internet-enabled devices to the network. These devices include personal printers, cameras, badge readers, and the ever-expanding range of USB devices. Uncontrolled devices like these can carry malware into the office and home networks—malware that can transmit out data and infect other systems. Protections throughout the network are critical to block inappropriate network access and proliferation of malicious software.

In addition to being the source of innocent policy violations and data exposure, approved users also often deliberately misuse their privileges, a common trait of insider theft and fraud cases, including conscious violations like WikiLeaks. Extra care and control must be taken to recognize inappropriate and anomalous activity, actions that are outside the approved scope of an individual’s role (identity) and the normal parameters of that person’s activities (context).

Perhaps the most complicated user community is the temporary, or transitory, workforce, which includes approved but less-trusted users such as contractors and guests visiting from other agencies or regions. These users require more attention before, during, and after access.

- Do you grant broad access or limited access?
- Can you control their access (where they travel on the network, what they do) when they are attached?
- Can you define appropriate time windows?
- Do you remember to delete their access rights when they leave the building or the contract ends?
- Can you document activities in case of violations while they were online?

## Using Identity and Context to Manage Access: Pervasive Trust

To seize the telework opportunity and comply with mandates to reform the workforce, IT must find ways to maintain security and compliance while opening up the network. It must find a satisfactory compromise between enabling productivity—what users want—and enabling confidentiality, integrity, and availability—the security that enables the IT team’s mission to provide services. This new balance requires change, but not upheaval. One analogy is a shift from centralized physical office controls (guards, locks, and badges), and physical network controls (such as firewalls and intrusion prevention systems) to a pervasive model where virtual controls enforce policies ubiquitously and automatically throughout the network: from device to data center.

The most efficient way to enable this model is to build a secure access infrastructure in as you update and reinvent network and data systems.

The design focus should be to enable role-appropriate data and application access by using identity- and context-aware technologies that weigh lightly on the user and ensure compliance with policy. Success will be a system that: Makes it easy for users to comply with policy (foster acceptable use) while using a range of IP-enabled devices, wired and wireless networks, and virtualized and cloud-based services:

Stronger security based on identity is a good idea, and it is what the experts recommend:

“Information Assurance Officers/Network Security Officers will ensure either MAC security (with profiling) or 802.1X port authentication is used on all network access ports.”

—Defense Information Systems Agency  
“[Access Control in Support of Information Systems Security Technical Implementation Guide](#)” (December 2008)

- Supports more types of transient users: guests, contractors, full-time employees, and telecommuters
- Makes it easy for IT to manage and report compliance against mandates in the U.S. Federal Information Security Management Act (FISMA), U.S. Defense Information Systems Agency's (DISA) Security Technical Implementation Guide (STIG), and U.S. Homeland Security Presidential Directives (HSPD-12)
- Helps IT be resilient to changing requirements, user demands, and technologies
- Maintains service and network availability and data integrity

## Network Access Control Is Just the Beginning

Most organizations have some form of simple security for network access. We are proposing something much stronger than one-time authentication based on the device, after which a user typically gains broad access controlled primarily by network segmentation (VLANs). Much more robust, this new pervasive trust infrastructure does more than grant initial network access; it enforces appropriate policies automatically as the user and the device move within your network and touch networked assets, such as data stores and printers.

## The Device and Beyond

This sort of pervasive trust requires the application of identity and context. It looks beyond the device accessing the network—laptop, smartphone, or printer—to the role of the user (identity) and the time, place, and risk of access (context). The network queries for user specifics, such as:

- Who is the user?
- What device is in use?
- What resources are being requested?
- Where is the device located?
- When is the access?
- Is the device compliant with policies?
- If not, can it be quarantined and made compliant (remediated) or should it be blocked altogether?

When access is approved for that individual and device, policies can automatically control what the user can do while connected to the network:

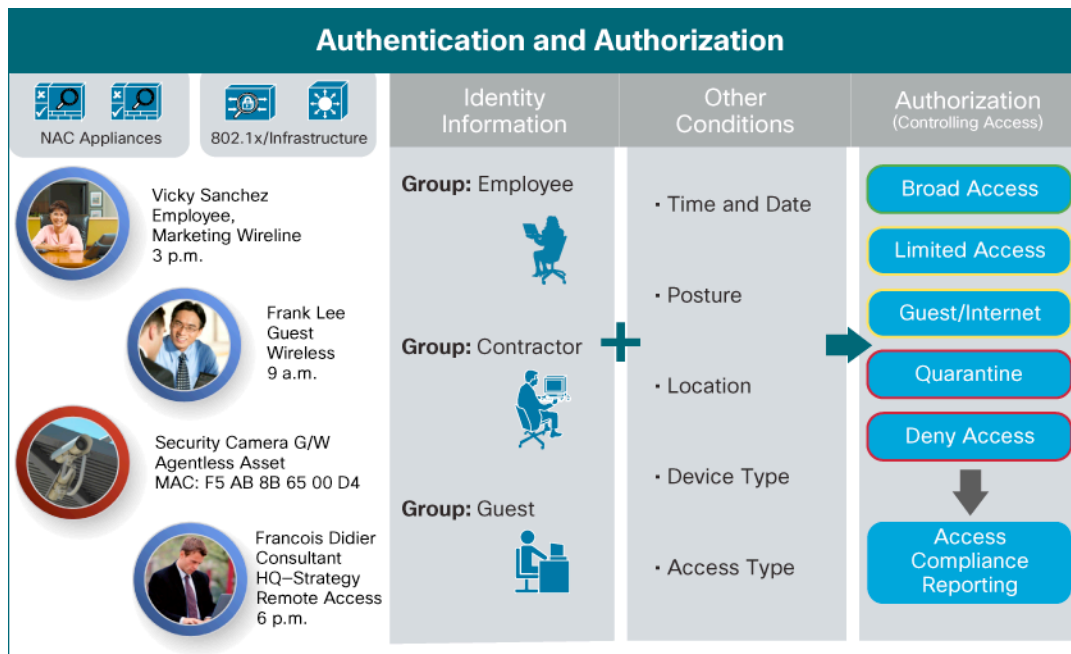
- What buildings, networks, and network segments can the device plug into?
- Is the resource request consistent with the role?
- What networked resources (applications, fileshares, printers, and data sources) can it access?
- What resources are explicitly blocked (data stores housing sensitive data)?
- Based on the role or the individual, what service level (priority) is network traffic given?

While each user is connected, the system can track identity and location as it monitors activity. Both in real time and afterward, the system can report user and device actions to provide evidence of compliance or assist with tuning of policies. This visibility provides details that might include:

- What is the user doing?
- When was the user active?
- What policies were in force?

This complete access lifecycle of control, visibility, and accountability enables a high degree of confidence in the organization's security and compliance, as shown in figure 2. With this confidence, you can now permit the types of services and connections that the modern workforce is clamoring for, from telework to social media, from cross-organization collaboration to the use of personally owned devices.

**Figure 2.** Complete access lifecycle



## Detailed Solution Requirements

The identity- and context-based model places new requirements on government IT infrastructure—requirements that can be met with technology available today. One of the most essential enhancements to the network is a robust policy-based infrastructure. This infrastructure enforces network access rules dynamically, matching enforcement to the role of the user and organizational, regulatory, and security policies. It relies on a sophisticated policy language that can be expressed in terms of who, what, where, when, and how.

## Policy-Based Enforcement That Is Pervasive and Persistent

Unlike physical technology-oriented requirements (linked to operating systems, protocols, or ports, for example), these policies should reflect abstract business-level concepts and organizational needs.

Organizational policies might encompass the websites users can visit, prohibiting adult content and gaming sites to every user while permitting social media to select organizational units. Or, requirements for data-handling controls, such as privacy legislation (state laws), healthcare legislation (HIPAA and HiTech), and the Payment Card Industry Data Security Standard (PCI DSS), might require encryption of sensitive data in motion and at rest.

The network access control point is the first line of defense in this infrastructure. It uses these policies to interrogate the device and user and determine how much, if any, network and resource access to provide. Rules can flex and be updated dynamically, and explicit and fine-grained rules can be applied based on the **identity** of the user (role and group), **profile** of the device, and **compliance** of the device in use, as well as the time and place of the access request. For example, a laptop might need to have the approved operating system patches, antivirus updates, and registry settings in order to gain access using campus wireless networks. Noncompliant devices could be quarantined or forced to remediate before being allowed access.

Because these policies are linked to the user, group, and role, policies can be differentiated for employees, contractors, and guests. This initial enforcement point can offer different degrees of access based on all of these factors, explaining why it is considered dynamic access versus the “all-or-nothing” static controls of older environments.

## Multiple Enforcement Actions in One Process

Depending on the mode of access, the enforcement point can integrate multiple aspects of policy enforcement to make access as simple and painless as possible for the user. For example, a single transaction might handle several different “handshakes”, enabling a remote user with:

- VPN
- Encryption
- Authentication of the device and user to both wired and wireless networks
- Validation of endpoint compliance

### IDENTITY-BASED ACCESS ENFORCES POLICIES

#### Who are you?

802.1X or other authentication methods authenticate the user.

#### What device are you using?

Validate managed and unknown devices to determine compliance.

#### Where can you go?

Based on authentication, the user is placed in the correct workgroup or VLAN.

#### What service level do you receive?

Per-user access can explicitly restrict or allow access to specific resources on the network, or apply specific quality-of-service (QoS) priority on the network.

#### What are you doing?

Using the identity and location of the user, tracking, compliance, and accounting can be better managed.

---

The experience is like single sign-on for applications, but the implementation enforces several different policies and controls in one step.

### Pervasive Control of Traffic

In addition, it attaches “tags” to the traffic of the device. These tags characterize the user’s privileges, or entitlements, and travel with the traffic, allowing other automated enforcement points within the network to allow or block access to network resources without the user’s reauthenticating. The user gains appropriate, controlled access to resources such as printers, file servers, databases, or applications in a shared data center.

These other enforcement points may sit at trust boundaries between networks, connect network segments in a campus, patrol the “perimeter” of the network sitting between home users and the agency campus, or hand off third-generation (3G) wireless network traffic to the local, wireless LAN.

### Persistent Application of Access and Resource Policies

Policies and privileges persist after admission to the network, remaining in effect at the initial enforcement point as well as if the device moves to another location or access mode (such as from wireless to wired networks). This persistence and pervasive coverage helps prevent users from getting access that exceeds their rights or privileges. For example, a guest might be allowed wireless access only to the public Internet and a specific printer, while being denied access to any other resources. In fact, the public Internet access could be restricted to sites that are approved; avoiding the chance that someone walking by the user might be exposed to inappropriate content (a situation that could lead to a lawsuit).

One justification for this attention to access privileges is the increase in a type of attack called “spoofing”, in which a malicious user pretends to be another user (or system) with higher access privileges, perhaps rights to get into a restricted file server. Detection and control of spoofing behavior has become more difficult as more IP-enabled devices are used in the network, such as digital cameras, badge readers, printers, and even network gear. Most of these devices do not require authentication and require little maintenance, except that they have vulnerable operating systems that routinely go unpatched. A knowledgeable attacker uses these weaknesses to penetrate the network, and escalates privileges to extract sensitive data, plant malware, or disrupt availability of resources (perhaps appearing as a denial-of-service attack). However, if a device has a specific identity: “printer”, and there is a policy: “printers can receive but not send network traffic”, an attacker has no way in and cannot escalate or explore.

### Data Confidentiality and Integrity

So far, we have covered access to the network and its resources. Now, let’s look at the data that traverses the network. Data confidentiality (leaks) and integrity (corruption or changes to data in transit) are central to security and regulatory compliance. To limit the potential for sensitive data to be mishandled or stolen, in transit or by compromised hosts and malware, best practice is to use encryption and content inspection.

Ideally, encryption should secure the entire data path, from device to data center and back again. However, encryption has become problematic with today’s dynamic, web-centric applications. Encryption at the application level requires significant compute resources, and many applications operate at capacity or in virtualized environments where these encryption resources are just not available. Further, the bulk of network traffic does not need to be encrypted, so blanket encryption slows operations needlessly. It is much more efficient and practical to enforce encryption within the network based on the data and its sensitivity, and the identity and context of its use.

---

Encryption helps with more than accidental data leaks. By placing encryption within the network, enforced according to policy, IT can also better protect sensitive data traffic from attacks launched by malicious or disgruntled insiders, spoofed devices, or compromised PCs that provide insider access. Encryption helps counter man-in-the-middle eavesdropping attacks and sniffing of packets by making the traffic impenetrable.

A further protection for data is to insert extra content inspection at critical network control points and trust boundaries. Essentially, content inspections such as those in data-loss prevention and web gateways, firewalls, and intrusion prevention systems already protect traffic within the network—as well as at the perimeter—against malware and attacks. By using the same enforcement point to scan traffic and apply multiple operations—authentication, encryption, and malware inspection—these extra operations can be handled expeditiously, without delaying traffic. Further, these controls can be linked to other network policies to support identity- and application-oriented preferences around quality of service (QoS) and traffic shaping. High-priority users and their traffic can take precedence—with appropriate security.

### Policy Development, Manageability, and Compliance

Clearly, having crisp policies is critical. In the past, however, establishing, maintaining, and demonstrating compliance with policies was painful. Each regulation, IT control, product, and protection has had its own effect on policies, occasionally resulting in conflicts that can be difficult to resolve. Reporting has meant cross-correlation of details, usually with lots of hunting for missing data and mistakes. However, this ugly picture gets much more attractive when identity is used as a pervasive, consistent way to enforce policies and entitlements across access, resources, and services.

For instance, identity-aware infrastructure can be natively integrated with existing user directories. This approach has the benefit of enabling one authoritative source for identity and role information. It thus eliminates network segmentation performed through switch-level implementation and maintenance of access control lists (ACLs) and VLANs. Instead of the typical add, move, and change overhead, when users change roles or leave the organization, policies can be efficiently, dynamically updated to suit the new role or block access. When Susan moves from administration to accounting, her access rights can change in seconds. When a contract ends, all access privileges for that contractor's team can be terminated in one transaction.

For the policies themselves, a centralized policy environment allows coordinated policy creation, distribution, auditing, and management of policies based on business terms (identity, role, and applications) rather than IT terms, such as network segment, IP or MAC address, port, or protocol. Because the user community and business demands typically change faster than the underlying technology, security policies in business terms are better able to keep up with business operations.

When it comes to monitoring and auditing for compliance, a unified environment offers real-time situational awareness of “who, what, when, where, and how”. Imagine you were concerned about the activities of a guest. Administrators can view what is happening in real time, look back in time if necessary to investigate problems, and use access details for troubleshooting and incident resolution. For instance, at any given time a session database can list active sessions and the policies being applied to each session and user. By pulling these details into a single data environment, the organization streamlines audit and compliance reporting for FISMA, DISA STIG, and HSPD-12.

When this policy environment is applied to telework and mobile access, some important compliance advantages emerge. Teleworkers, contractors, and guests can be “sponsored”, where their access rights are provisioned through a user-friendly web portal, and then monitored and reported throughout the lifecycle of their access.

---

Enforcement events such as quarantine and remediation are documented. A window of use might be an afternoon, a month, or a year. This data can be archived as long as regulations and policies require.

## Conclusion

As the network perimeter evaporates, IT must rethink network security infrastructure. When people enter your building or access your network, what do you want to let them do? How can you provide the flexibility they want with the security and compliance your responsibilities mandate?

The solution we recommend is to enrich network access policy enforcement to reflect identity and context and integrate enforcement throughout the network—not simply at the edge of the network and the data center. With this pervasive trust model, wherever access happens, whatever device is used, wherever traffic travels, security and compliance policies will remain in force.

Identity- and context-based policies can offer powerful improvements to the way governments manage network access and the kind of access IT can provide. An identity-based access system keeps interlopers and malicious software out, and allows government employees, contractors, and guests to perform their roles where and how they need to, using a range of devices, without breaking the security rules, the network, or the IT budget. IT can consolidate and enhance the services users can access, taking advantage of cloud and virtualized options and delivering resilient, highly available services.

By tying together context-based access control policies, identities, and enforcement across systems, it becomes easier—and much more efficient—to monitor, audit, and report user and endpoint compliance. A unified view also provides visibility into usage, behavior, and trends, so your security updates and plans can keep up with organizational requirements.

The mobile, teleworking, collaboration-directed, and gadget-toting workforce will not wait, and efficiency pressures and regulations make action imperative. The ideas discussed in this paper are concrete, and they build on network, identity, and security infrastructure the government already has in place today. Best of all, they already have traction delivering value in both the commercial and government sectors today, so government IT leaders can get started immediately.

## A Solution for Success

Cisco TrustSec® technology helps organizations secure access to their networks and networked resources with context-based access control, identity-aware networking, and data integrity and confidentiality services. This secure network fabric enforces policies on all devices that attempt to access the network, improving compliance, monitoring endpoint health, strengthening security, and increasing operational efficiency.

Cisco TrustSec solutions include user authentication and authorization, posture assessment, device profiling, guest access, data integrity and confidentiality, centralized policy with distributed enforcement, and collaborative monitoring, troubleshooting, and reporting. The technology can be deployed as an appliance-based overlay solution or as a network-integrated 802.1X solution designed to extend access enforcement throughout the network.

With Cisco TrustSec technology, the Cisco Catalyst® switch authenticates users and devices, requests policies based on the role and context of the user and device, and applies and enforces those policies associated with the authenticated devices. An identity tag, or “metafile”, which includes a policy marker for that device, can then actually be inserted into the header of every data packet, and then the entire data stream can be encrypted to ensure data confidentiality. Cisco TrustSec-enabled devices are then able to decrypt the data packets, read the

---

policy tags, enforce the policy, and then re-encrypt and send the traffic through—and it all happens at wire speed. The result is consistent policy enforcement and visibility into device behavior throughout the entire networked environment.

For centralized policy and identity management, the Cisco Identity Services Engine (ISE) provisions and delivers cross-domain application and network access services. It allows IT to create a centralized access and control policy for all users and devices, and then distributes those policies to ensure consistent enforcement the agency campus to the regional office. To incorporate context, the ISE gathers information from users, devices, infrastructure, and network services, allowing Cisco ISE to act as the “single source of truth” for contextually rich identity attributes, including connection status, user and device identity, location, time, and endpoint health. ISE combines that contextual information with user and device information sources, such as Active Directories, to determine the appropriate access policy for that user and/or device. ISE then dynamically distribute this access policy to TrustSec-enabled Cisco devices, or other strategically placed ISE appliances, for network-wide enforcement. Automation eliminates labor-intensive tasks and simplifies the delivery of new services, including access to cloud-based services and guest access management. Offering system wide visibility, ISE dashboards show IT who and what is on the network, including their access status, while correlated logs, customized queries, and integrated diagnostics assist with discovery and troubleshooting.

Each network product consumes the policies it needs, eliminating rules managed per switch, router, or firewall. Multiple policies—authentication, authorization, and accounting (AAA), posture, and profiling—can be applied in a single step at each access point, helping ensure compliance without latency. And Cisco change management features mean that access policies can be automatically updated and pushed to all enforcement points should any of the access conditions change, such as the device travels outside the network.

The Cisco TrustSec solution offers more than technologies; it includes guided workflows, monitoring dashboards, sample reports, and professional services designed to help organizations move quickly from best practice to successful implementation. Cisco professional services help organizations with Cisco TrustSec lifecycle management to simplify deployments, strengthen security, improve productivity, and lower operating costs. Cisco TrustSec technology is a foundational component of the Cisco SecureX security strategy, enabling the secure and transparent delivery of agile business services to anyone, anywhere, anytime. Cisco TrustSec capabilities continue to be developed to take full advantage of this common network-based model of a policy enforcement framework based on identity and context as network services and applications continue to evolve.

### For More Information

To learn more about Cisco TrustSec and other Cisco pervasive trust capabilities and solutions, visit:

- [www.cisco.com/go/securex](http://www.cisco.com/go/securex)
- [www.cisco.com/go/trustsec](http://www.cisco.com/go/trustsec)
- [www.cisco.com/go/security](http://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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Printed in USA

C11-681297-00 07/11