

WHITE PAPER

Phoenix
TrustConnector™

The Trusted-Connection Landscape

The Importance of Device Identity in the World of Trusted Connections



Introduction

In spite of firewalls, intrusion detection, and user authentication, today's information systems are being rapidly and successfully attacked. Computer networks continue to grow at a rapid pace. Organizations must upgrade their defenses to prevent attackers and malicious processes from connecting to and accessing their systems. Ensuring that each connection is a "trusted connection" is the best improvement an organization can make. This can be done by certifying both the user's device as well as the connecting user.

Trusting Your PC Connection can be Risky Business

Do you want to connect with the PC that's knocking on your door? Chances are you don't. In addition to ongoing virus threats, according to Information Week, a whopping 80 percent of PCs have at least one instance of unwanted software in the form of spyware, adware or Trojans. Many of these insidious infections are capable of propagating themselves to your systems and, unfortunately, they are getting better at it.

The following is a sampling of the serious security risks that may be relevant to your particular PC connection:

- Is the connecting PC properly configured to ensure a relatively secure connection?
- Is the connecting PC running a personal firewall?
- Were the latest security patches applied?
- Could your network be used to distribute illegal or pirated material or launch inappropriate gambling, gaming, or other services?
- Can the PC requesting a connection be trusted to safeguard your sensitive data?
- Will you face a shareholder lawsuit if that PC or laptop is stolen and confidential information appears on the Internet or in the hands of a competitor?
- Is that connecting device a company owned PC that has been configured to properly safeguard the data, or is the user on their own, un-secure personal laptop or Internet kiosk machine?

Is the user of that PC really who he or she claims it is? The most damaging computer crimes occur when an attacker steals, deduces, or otherwise obtains user IDs and passwords for privileged accounts. Armed with a privileged ID, attackers are welcomed into the system and can do just about anything they please. Unfortunately, it's relatively easy for a sophisticated attacker to obtain a significant number of IDs and passwords. The small percentage of the systems protected by strong user authentication are not immune, particularly from inside attacks where insiders can share one-time pass codes or digital keys with accomplices who then access the system.

Facing real and growing risks, it's imperative that organizations upgrade the trust level of their computing connections. Connections must become trusted connections. A trusted connection occurs when the devices or applications involved know and certify the ownership, user, and configuration of the connecting device. If any of these elements are missing, a trusted connection cannot be established. Ideally, every connection should be a trusted connection, but where high-value data access is vital, a trusted connection is critical. VPN and wireless network access are important candidates for the added security of a

The Trusted-Connection Landscape

trusted connection because they provide access to the entire network. Further, any access to financial systems, company trade secrets, customer or personnel records, and all regulated data (health, personal-private, insider information, and so forth.) should always mandate a trusted connection.

While untrusted connections may occur and may be necessary in some instances, such access should be limited to resources that don't include sensitive data. Connection with an unknown user or unknown device should generally be restricted to data that is in the public domain.

Which Characteristics Comprise a Trusted Connection?

There are a number of characteristics that together comprise a trusted connection. The user's identity must be obtained and authenticated; the user's relationship to the organization must be established as well as the required level of monitoring of the user's activities.

On the device side, the device identity, device relationship, and device configuration (including antivirus, anti-spyware, security patch level, and personal firewall state) need to be certified. The device's ability to automatically encrypt and control access to stored data is also important for many organizations and uses. Finally, there should also be monitoring of the device's activities to assure compliance with access limits and privileges.

These various user and device characteristics determine the trust level of a connection. Like the support blocks of a pillar, they collectively create a trusted environment. However if any of the blocks are missing, the trust level will collapse. Determining these characteristics, the process of certifying devices and their users to establish trusted connections, involves a number of products and technologies. Various identity and authentication mechanisms, role-based policy or authorization systems, personal firewall, anti virus, anti spy-ware, and several other systems or technologies may be used separately or in combination.

Device Identity is Essential

As user identity and user relationship characteristics are essential in determining the level of trust, device identity and device relationship is also vital. Establishing the relationship of a device is critical because it allows an organization to easily determine whether or not a connecting device should be trusted. For example, if an organization configures all company laptops with antivirus and other security packages it deems necessary, the organization can decide if a connection with a company laptop is relatively safe without a full-security assessment, or if any valuable company resources should even be allocated in bringing the device's configuration up to date. Unknown machines can be denied access, or restricted to low-risk usages. This level of added security is significant and can be deployed today without integrating a number of disparate security packages.

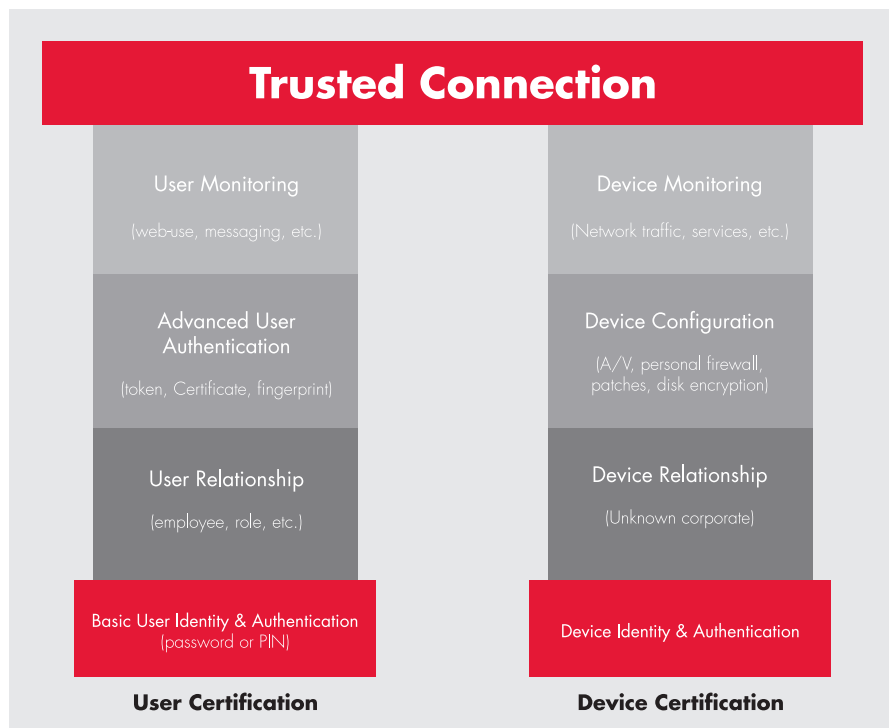
Currently, and for the next few years, determining device identity, coupled with user identity is the simplest and most effective way to determine if a connection should be trusted. If networks and high-value applications would add the ability to verify that the connecting device is owned by the organization, or at least known to the organization, at least 80 percent of the most damaging attacks would be prevented. Consider the case where an attacker supported by organized crime obtains a valid user ID and password to a financial system or highly sensitive database. If the target networks only allow trusted connections, the attack would be easily thwarted because the attacker's PC would be an unknown device and would thus deny access. If such protection is not implemented, an attack of this type will always succeed.

The Trusted-Connection Landscape

Trusted Connections Require Two Pillars

As stated above, a trusted connection requires establishing the trust level using two critical pillars. The user must be certified, including their identity, role, and monitoring level. The user's device must be certified. This entails establishing its identity and relationship to the organization, determining whether the device is associated with an authorized user, knowing the device's security configuration so that the device won't spread contamination to the network, and realizing that data downloaded to the device will be protected from corruption or theft, both in transit and as it resides on the device. The device's role and the level of trust for the connection will also establish the level of monitoring needed for the device. Both user and device examinations are critical. If either are lacking, the trust level of the connection can't be established and will be called into question. The comprehensive trust level of the connection depends on these two important and vital pillars.

The various technologies work in concert to establish the characteristics necessary to qualify as a trusted connection. Phoenix TrustConnector (explained later) provides the important device identity characteristic which is the foundation of device certification. Other products and technologies also provide important functions that contribute to the overall connection status.



Establishing a trusted connection rests on the two pillars of user and device certification. Basic User authentication and device authentication are the foundations for each column.

The Trusted-Connection Landscape

Trusted Device Characteristics			
Trusted Characteristics	Purpose	Technologies	Vendors
Device Identity	Gives unique device identifier to networks or applications that request it	Microsoft CSP, CAPI, hardware binding	Phoenix
Device Authentication	Validates the authenticity of device identifiers	X.509, RADIUS	Microsoft, Entrust, and other certificate-based systems
Device Relationship	Determines device ownership	LDAP	Microsoft Active Directory or other LDAP suppliers
Device Configuration	Verifies protection for viruses, spyware, and Internet intrusion. Patch and configuration management	NAC, NAP, and other proprietary methods	Trend, Symantec, McAfee, Cisco, Shavlik, others
Device Monitoring	Monitors devices to ensure network traffic is appropriate and to ensure device is operating correctly	Firewalls, intrusion detection	Cisco, Checkpoint, ISS
Trusted User Characteristics			
Trusted Characteristics	Purpose	Technologies	Vendors
Basic User Identity and Authentication	Client system gives user IDs and passwords or PINs to networks or applications where it is authenticated.	Usually fixed password or PIN delivered via EAP or similar and authenticated by LDAP or other methods	Microsoft and others. Built into most networks and applications
User Relationship	Determines if user is employee, contractor, business partner, or customer and their privilege level. Unknown users are identified as such.	LDAP and proprietary systems	Microsoft Active Directory, iPolicy, CA, OpenNetwork
Advanced User Identity	Client system provides something users have in their possession, or something users are to networks or applications where it is authenticated.	Fingerprints, digital certificates, token cards, smart cards, X509, RADIUS	Microsoft, RSA, Secure Computing, Identix, Entrust, Vasco, ActivCard and others
User Monitoring	Monitor user behavior	Web filtering, central reporting	Cisco, Checkpoint, ISS, Websense, SurfControl, 8e6 Technologies, Reconnex, and others.

The Trusted-Connection Landscape

Integration Not Required

An organization is likely to use products from different companies to establish the trust characteristics. Even in rare situations where an organization can obtain most of their products from one vendor, the integration is typically lacking. Establishing the identity of a PC allows an organization to know if the PC is likely to have the security systems in place, even without any integration. In the future, enough of the various security mechanisms on the connecting device will report their presence and status in such a way as to be useful to most organizations. Although there are emerging endpoint security products and management initiatives headed in this direction, currently these are proprietary and address only some of the needed characteristics. Cisco NAC, Microsoft NAP, and the Trusted Computing Group's TNC are examples of companies who offer these initiatives.

TrustConnector Provides Device Identity

TrustConnector, from Phoenix Technologies, is client software that runs on Microsoft Windows based PCs. It gives a PC the ability to securely identify itself when it connects to networks or applications. Using TrustConnector, an organization can easily determine if a PC requesting access to a network or application is owned by the organization and should therefore be trusted to make the connection. PCs that can't be identified as being owned by the organization can be refused, or restricted to low-risk areas.

TrustConnector works by creating a unique device key for each PC. The key is created and stored by using the strongest available cryptographic service on the device, which could be the PC's hardware or core system software (BIOS), or if neither is present, a software-based cryptographic module provided by TrustConnector. This binds the key to the PC. The device key, and all keys protected by the device key, cannot be moved, stolen or copied, and assures a unique device identity for every device protected by TrustConnector.

Specifically, TrustConnector uses the device key to protect the private key in a standard X.509 digital certificate, which can be used to authenticate the PC to any certificate-based network or application. For example, Microsoft's certificate-based authentication system, included in Server 2000 or Server 2003, can be enabled to automatically and transparently authenticate a PC's device certificate whenever the PC connects to the network.

TrustConnector can be used to identify the PC when connecting via VPNs, wireless access points, all network connections, or to any application that supports certificate based authentication. TrustConnector can be transparently deployed to all PCs in the network.

TrustConnector Offers the Best Secure Solution

TrustConnector is the only viable solution for securely identifying PCs. Although MAC and IP addresses can be used to identify a PC, both are susceptible to spoofing and not generally secure enough to warrant their implementation. Furthermore, deploying a device identification system using MACs or IP addresses would need to be home grown because there are no off-the-shelf packages available.

Emerging trusted platform module (TPM) based systems are a way to provide device identification TPM hardware is an excellent place to store device keys. As TPM compliant systems become more readily available during the next several years, they will be a perfect compliment for TrustConnector because they provide an additional option for securely storing device keys. TrustConnector is already supporting this feature and can currently store device keys in TPM hardware if it is present on the PC.

The Trusted-Connection Landscape

TrustConnector Benefits

By implementing TrustConnector today, organizations can significantly enhance their IT security by taking full advantage of the following benefits:

- Identifies company owned or authorized PCs attempting to access high value networks and data and grant them a trusted connection. Restrict unknown PCs to low risk networks and data.
- Protects entire networks, or specific applications such as financial systems, employee or customer personal and private data.
- Secures specific access methods, such as VPN or wireless access. All access, including local LAN connections can be protected.
- Protects high value departmental systems from access by employees in other departments.
- Prevents attackers from accessing protected systems even if they have obtained valid IDs and passwords. This capability thwarts entire categories of computer crime.
- Stops ex-employees from accessing your system from their homes or new workplace.
- Prevents insiders from giving outside accomplices the ability to login.

TrustConnector does not require tight integration with other security packages and can be implemented. TrustConnector is the best solution for organizations desiring to significantly upgrade IT security.

Summary

In the past the inability to easily establish trust with connecting devices, and dependency on connecting with unknown devices, has generated serious problems that are undermining today's critical information systems.

A significant number, if not most information system attacks that cause substantial damage are successful because in spite of improved authentication systems, attackers obtain IDs and passwords of authorized individuals. However, most of the penetrated systems have a relatively small number of authorized users who access the system from a small number of authorized PCs. The easiest, most cost-effective solution to prevent computer attacks is to verify that connecting devices belong to those with the proper authorization. This simple security measure will prevent the majority of the most damaging types of computer attacks, even in those cases where the attacker obtains logon credentials for authorized individuals.

Determining the identity and ownership of a PC before granting a connection is also the best way to determine if the device is properly configured, up to date with security patches, and is protected against firewalls and intrusion. In the future, this might be accomplished through tight integration with a number of security packages working together to report their presence and status. Today, and for the next several years, the best approach is to validate that the PC is a company-authorized device, and rely on company policy to mandate that all company PCs are properly secured and protected.

TrustConnector, from Phoenix Technologies, makes it easy to deploy device identity and achieve trusted connections.

The Trusted-Connection Landscape

Appendix

This appendix provides more information regarding the various products and technologies available to establish trusted connections. Both strengths and weaknesses of various technologies and solutions are noted.

User Certification

User inspection entails a number of examinations and checks centering on the user's identity, relationship to the organization, and the users' actions while connected.

Basic User Identification

Technologies that provide a claimed identity of a user. These can generally be divided into three areas: 1) Something the user knows such as a password or PIN; 2) Something the user possesses such as a smart-card, token, private key for a digital certificate, or a registered device; 3) Something the user actually is such as a fingerprint, voiceprint, or facial template. Note that identification differs from authentication in the sense that identification technologies present data that claims to identify a person whereas authentication is the process that validates the claim.

Note that user identification and authentication are generally divided into two areas. Basic user authentication is based on something the user knows such as a password or PIN. It is suitable to deploy to the masses and is the foundation of the user inspection pillar. Advanced or Strong user authentication adds an additional factor such as a biometric measurement or something the user possesses. Advanced authentication is expensive to deploy and is only suitable for a small percentage of organizations or users (in 2004, around seven percent of logins utilize advanced authentication).

- Hardware token systems such as reader-less token cards, USB tokens, and smart cards. Technologies include a variety of encryption systems including private key systems such as DES, Triple DES, and AES. Public encryption systems (PKI) are also utilized. Leading vendors include RSA, Secure Computing Corporation, Aladdin, ActivCard, SafeNet, SCM Microsystems, and Vasco.
- Software token systems emulate hardware tokens as described above. However, the secret keys and processing are software based and not protected by special-security hardware. Many hardware token vendors also offer a software version.
- Biometric systems such as fingerprint, voiceprint, and facial recognition. Leading vendors include Identix, Bioscrypt, Cogent Systems, Cross Match, Sagem Morpho, Visiage, and others.

Basic User Authentication

Technologies that validate a claimed identity. These include authentication systems and servers using technologies like RADIUS, EAP, PKI, and so forth. Basic authentication is built into all successful products including Microsoft Registry and Active Directory.

User Relationship Enforcement

Technologies and processes that establish a user's relationship to an organization, and determine and enforce the rights and privileges that are associated with that relationship. For example, a user that is unknown to an organization will have fewer access rights than the head of IT. Customers, business partners, employees, and managers may have different access privileges. Access rights can be refined by what department(s) a user may belong to, or by time of day, or other criteria. LDAP directory management systems, policy creation systems, and policy enforcement systems play a part in establishing user relationships and enforcing the associated rights and privileges. Although there have been a few vendors and products that specialize in policy establishment and enforcement for multiple applications (iPolicy, for example), LDAP directories such as Microsoft Active Directory have been the only products in this area getting any traction.

The Trusted-Connection Landscape

User Activity Monitoring, Logging, and Policing

This area includes technologies and systems that monitor, log, or police user activities. This is usually done by a device on the network as opposed to PC based technologies. User activity monitoring, logging, and policing technologies include:

- Resource Usage Logs such as general network logins and access, application usage, or transaction auditing and monitoring. 8e6 Technologies, e-Security, Guidance Software, Niksun, and other vendors offer solutions in this area.
- Web Filtering to discourage or prevent users from accessing illegal, offensive, or inappropriate web sites. Products in this area include SurfControl, Websense, and SmartFilter/Web-Washer/N2H2 from Secure Computing Corp.
- Message Filtering to discourage or prevent users from transmitting illegal, offensive, inappropriate, or company confidential material via e-mail, instant message, or by other means. Product vendors include Reconnex, Actimize, Aladdin, IP Locks, MessageGate, NetIQ, Vontu, and others.
- Regulatory Compliance systems that specifically monitor, log, and police user behavior as it relates to legislative regulations such as Sarbanes Oxley, HIPPA, Graham Leach Bliley, or others. These technologies are related to and perform some aspects of message filtering but are specific to regulatory compliance. Products that specialize in regulatory compliance include Reconnex, Actimize, Documentum, and others.

Device Certification

Device inspection includes those technologies and processes that examine a user's PC, handheld, or other device to understand the device's relationship to the organization and user, and to ensure that it is safe to connect with. In the past, device inspection has largely been ignored, but recent attacks and trends make it clear that device inspection is becoming as important as user inspection. Device inspection includes a number of technologies that ensure the device itself can be trusted. The technologies cover the gamut of positively identifying and authenticating a device attempting connection, which is the foundation of the device inspection pillar, making sure the device will not spread viruses or contamination, examining the device's ability to safeguard downloaded data from theft or corruption, and verifying that the device has the latest security patches and is properly configured.

Device inspection technologies and processes include the following:

Device Identity

It's critical to understand the relationship of a device to an organization. Knowing the identity of a device is the foundation of the device certification pillar. A device may have the latest patches, be virus free and running an accepted personal firewall, but if it is owned by a hacker you don't want it to connect to your network. Attackers have matured. They now comprise sophisticated crime rings targeting specific companies and organizations. They are skilled at stealing or guessing IDs and passwords of authorized users, sometimes even when advanced authentication is used. Verifying that the connecting device is owned or controlled by the organization will prevent a host of attacks from occurring, even if stolen authorized IDs and passwords are being used.

The following technologies may be used to establish Device Identity:

IP or MAC Addresses associated with a device can help establish device identity in low-risk situations; however because both are subject to impersonation and spoofing their use is not suitable for organizations with anything substantial at risk. Many products that attempt to identify devices today use one of these two methods. These may include patch management systems, personal or distributed firewalls, software and licensing distribution systems, and others.

The Trusted-Connection Landscape

Software-based device keys are identifiers stored on hard disks or within volatile storage of some sort. While stronger than device identity based on IP or MAC addresses, software-based device keys are subject to being read, copied, or stolen making them particularly vulnerable to insider attacks. They also suffer from extra maintenance to repair or replace device keys if unintentionally removed or corrupted. Products that typically use software-based keys for device identity include remote-access products like VPNs. Some of the endpoint security products using device-resident agents may also use software-based device identifiers.

Hardware-based device keys are identifiers that are protected by hardware. The hardware makes it extremely difficult if not impossible for an attacking user or process to learn or steal the device keys. This is the strongest solution for providing device identity. The following methods are used to deliver hardware based device keys:

- **TPM compliant-security chips:** This emerging technology uses specialized hardware that safeguards device identifiers (keys) within secure silicon. All processing that requires the use of the device keys is done within the protected chip and is not available to outside processes. Although this is a strong solution, it is not practical for most organizations because it requires replacing the users PCs with new, specially configured ones. This solution may become feasible in the future if TPM chips become standard offerings.
- **Secure NICs:** Over the past few years 3Com and other startup vendors have produced a series of secure network interface cards. These products replace existing NICs with a NIC that includes security chips capable of securely hosting device IDs. This solution is also a strong solution, but again, not feasible for most organizations because it requires the replacement of a user's NIC card which is time consuming and expensive.
- **Hardware fingerprint systems:** When device identification is requested, an agent running on the device scans the hardware configuration and through various methods establishes a unique hardware fingerprint used to identify the device. Although not as strong a solution as secure NICs or TPM solutions, hardware fingerprint-based solutions are significantly stronger than software-based device identification systems. Furthermore, hardware fingerprint systems don't require the installation of additional hardware and are thus suitable for mass deployment to today's installed base of computers. For most organizations, the added security and deploy ability of this approach makes it the best overall single device-identity solution available today. This is one of the methods Phoenix TrustConnector can use.
- **Secure core system software:** For X86-based systems, an upgrade to a secure version of core system software (BIOS) allows device keys to be stored in an area of system memory that is protected by the X86 system hardware. Neither the OS nor applications running under the OS can directly access the protected device keys. Security related processing such as device identity is done entirely within core system software and the keys are never available to other processes. This is a strong solution and because it works with existing X86 architecture, additional hardware is not required. It does however require an upgrade to secure core system hardware. Phoenix Technologies offers the secure core system software and when present, TrustConnector can utilize this method to safeguard the device keys.
- **Combination systems:** These solutions support multiples of the above technologies, allowing a company to role out a solution with their existing base of computers, yet take advantage of new hardware in the future as it becomes more feasible and cost effective. Phoenix TrustConnector is the only known device identity product that has the capability. It's a hardware fingerprint system that can use either secure core system software or TPM hardware if present.

The Trusted-Connection Landscape

Device Authentication

This is the process that takes a claimed device identity and authenticates it. Some point products such as VPNs, patch management systems, and others use proprietary methods to authenticate the identity of a device. The better solutions use standards-based systems such as PKI, RADIUS, or EAP.

Together, device identity and device authentication make up the foundation of the device-identity pillar upon which trusted connections rest. If, for example, a connecting device is known to belong to the company, and that it has anti virus, patch management, hard disk encryption, and a personal firewall in place, the trust level of the device is high, even without an inspection of each of the various security components. Moreover, if the device is completely unknown to the company, questions should be raised even if the device is virus free, and so forth.

Device Configuration

This can include checking the device for current, approved anti-virus and anti-spyware systems, or a personal firewall. It may also check to ensure that data on the device is free from infection. Is the device up to date with security patches? Is the device configured properly so default user IDs and passwords are changed and unused ports are closed? Is the device able to recover from an operating system failure and re-establish the O/S and user data?

There are a number of endpoint security vendors such as Sygate, Zone Labs/Checkpoint, Endforce, Senforce, InfoExpress, Secure Elements, Safend and others that provide various levels of device state of health inspections. Whereas TrustConnector identifies the device itself ("Can I see your driver's license please?"), these products focus on the device's health ("Can you operate safely on our data highway?")

Additionally, to establish a truly trusted connection, it is necessary to validate that the connecting device has security features that will automatically encrypt downloaded data when stored on the device itself, and that it will require user authentication to access that data. Vendors such as PointSec Mobile Technologies, Mobile Armor, and a few others provide products that safeguard data residing on endpoint devices. When used in conjunction with a device identification system such as TrustConnector, organizations can establish that the connecting device is known, and configured with such protection.

To learn more about the entire line of Phoenix TrustedCore products for core system security visit us at www.phoenix.com

Secure from the Start

Phoenix Technologies develops a complete product suite of Core System Software, tools and applications to deliver trusted, seamless computing to digital devices for an Internet-connected world. Phoenix Technologies helped launch the PC industry over 25 years ago. Today we are extending our leadership and knowledge at the core of machines, beyond the PC to a wide range of platforms and devices.

Phoenix Technologies Ltd.

915 Murphy Ranch Road
Milpitas, CA 95035
408.570.1000 main
408.570.1001 fax

800.446.9202 North America sales
781-BUY PTEC Outside North America sales

