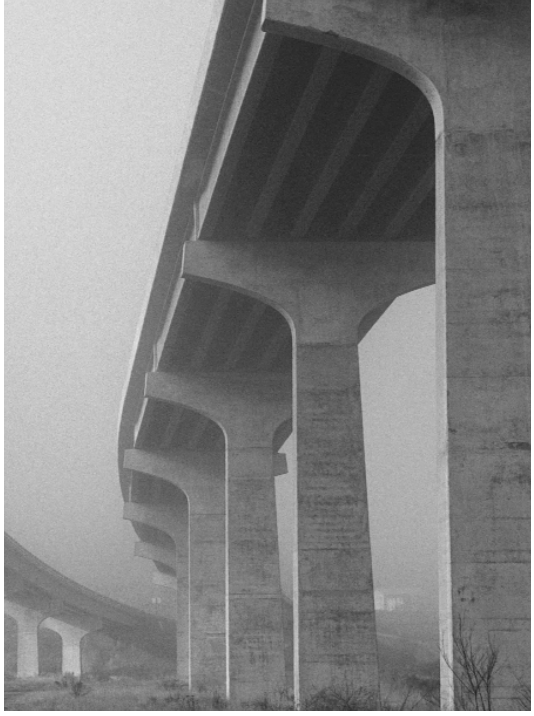
Tripwire White Paper



Data Integrity Assurance In A Layered Security Strategy

Providing The Essential Foundation For Data Security

Table of Contents

TRIPWIRE

www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, Oregon 97205 USA

WPLSSA01

Executive Summary

Much of the attention commanded by computer security issues focuses on threats from external sources. Firewalls and perimeter defense tools are deployed to deny unauthorized entry to the network. Experts look for vulnerabilities and ways to ensure that the perimeter cannot be breached. Administrators monitor network traffic for unusual activities and anomalies. It is common for users to be warned against suspicious email attachments. The assumption is that malicious intrusions and threats come from external sources. In other words, the focus is on protecting the enterprise from an outside attack.

While all of these measures are valuable and should be deployed to help protect digital assets, none of these technologies protects companies from data loss or damage that occurs from inside the network—whether it be accidental or malicious in nature. None lets you know when your best perimeter defenses and network security policies have been compromised. None are able to establish a "good," desired state of data and enable quick restoration if an undesired change occurs.

This paper will describe the elements you should consider in implementing a comprehensive security strategy and tell you why no security strategy is complete without data integrity assurance, why it is the cornerstone for safeguarding your data assets, and how it works alongside other perimeter defense products to ensure maximum protection for your enterprise.

The Layered Security Approach

A complete security strategy should be layered, which can be likened to fully securing a house. For example, you can lock your doors and windows and turn on alarms, but if you've accidentally knocked a hole in the wall or are hosting a guest who secretly causes problems once inside, locks and alarms alone won't adequately protect you.

A layered approach to security will include protecting from outside attackers, internal breaches of security and mishaps caused by both innocent and malicious people on the inside. There are several elements to a layered security strategy that assist in addressing the three elements of trusted security configuration (integrity, availability, and confidentiality). Layered security strategies typically contain all or most of the following items:

- Security Policy
- Incident Response Plan
- Host System Security
- Auditing
- Intrusion Detection Systems
- Router Security
- Firewalls
- Vulnerability Assessment

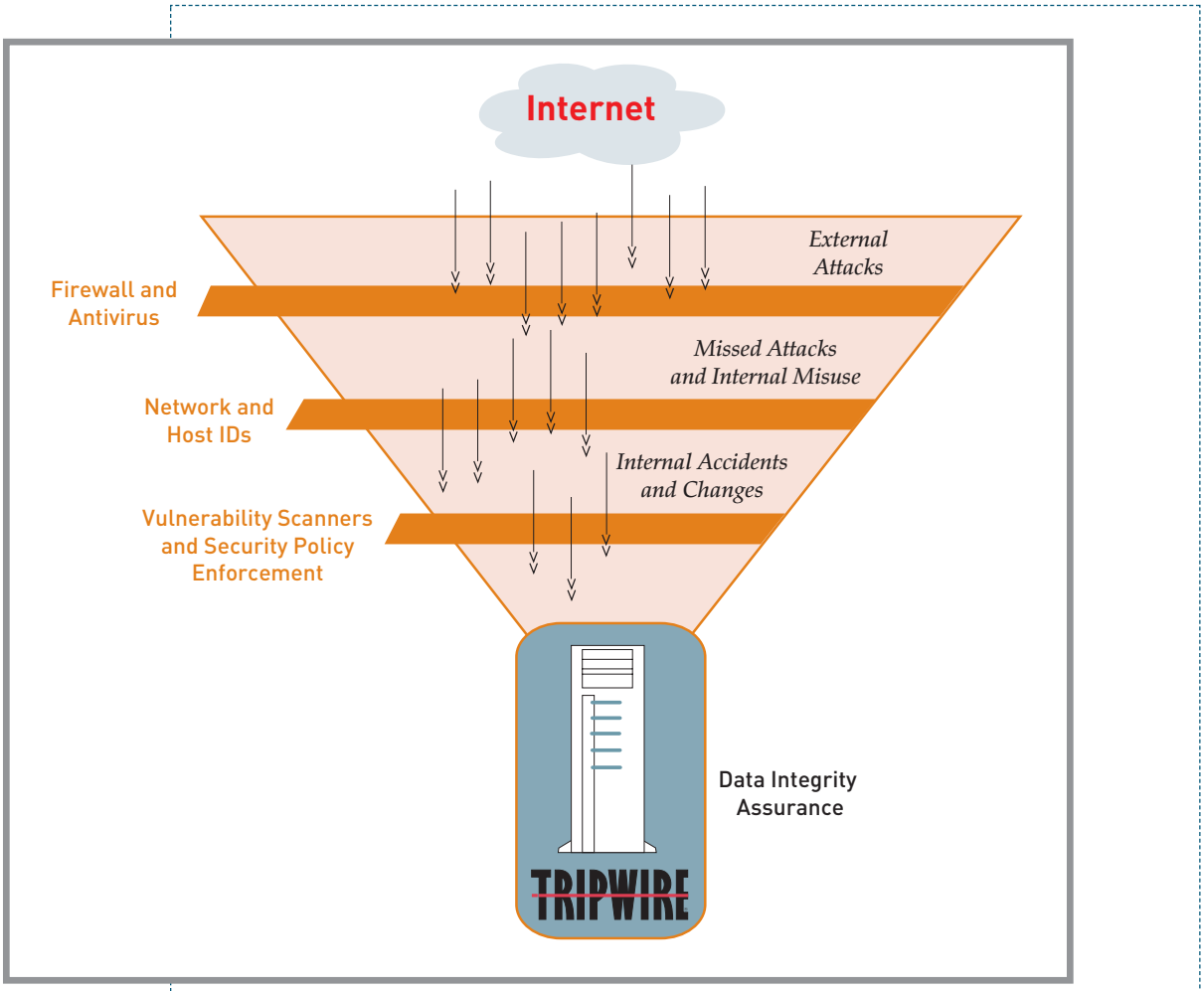


Figure 1 – This diagram illustrates that many perimeter defense tools miss many of the threats to a data system's integrity state.

Risks Inside the Perimeter

No matter what type of business you are in, computers and digital assets are an integral part of your operations. Protecting your computer systems, computer operations, and information assets against loss may be your business's most critical form of digital asset protection.

What is overlooked in many security strategies is the integrity of the "foundation" upon which the critical IT infrastructure is built. Due to the complexities of IT software, it is becoming much more difficult to know for sure what constitutes a clean start or baseline state for client, server, network devices, database management systems, and applications.

For example, one IT manager for a service provider interviewed by IDC stated that a vendor's UNIX server software contained 30,000 files per install. Even after removing files that were not required for the specific task, 16,000 files still remained. What if any of these files is altered, either by a disgruntled employee or innocently by an unaware employee?[1]

[1] IDC white paper, "Data and Network Integrity: Technology to Invoke Trust in IT", 01-104SYSTEM2930, May 2001.

Where is the Perimeter Anyway?

It's no longer easy to determine where the perimeter is in today's environment of distributed technology. VPNs, extranets, tunneling and simply the many technical possibilities of e-commerce and the Web make it virtually impossible to support a truly contained network with a clear "outside" and "inside."

That's why the original idea of a "secure" perimeter is no longer enough. The original security architects were government agencies and defense contractors who were experts in handling confidential assets. Their training led them to lean toward perimeter defenses as the cornerstone of defense. Even though baseline data integrity was recognized as one of the four pillars of conventional security, it was presumed that as long as the perimeter was secure, assets were automatically secure.The architects reasoned that IT assets didn't need to be monitored or managed for integrity, because the command and control environment gave people assurance that core data was safe.

Today, the situation is different. Any network with an Internet connection is by default an open network. One large financial institution articulated it this way, "Perimeter defense based on firewalls is still important, but more sophisticated security systems are needed because we don't even know where the perimeter is anymore."

"Integrity drift" refers to another kind of risk to data integrity that cannot be stopped at the perimeter. It describes movement away from a desired state. Integrity drift is the result of several factors, including the diversity of platforms, applications and processes operating in any typical IT organization; the complexity introduced by mergers and acquisitions; and the ongoing pressure on IT by business users to "just get it up and running quickly."

One company's information security executive related that when he came on board, his organization had 200+ machines on the Internet, each one configured differently from the rest. The machines that were created with variations also were not properly maintained. The company had a lot of operations staff focused on deployment, but there were no system administrator resources to maintain the machines.

The CIO described the feeling of his lack of control of the assets by stating that, "when I joined, it was clear that, well, the machines weren't really ours anymore." [2]

The Trusted Security Configuration

Shifting perimeters, internal threats, and integrity drift: These are all facets of security not addressed by the defenses most typically associated with computer security. The omission becomes more apparent when one revisits the goals which drive recommendations behind modern security measures:

1. **Availability** (of systems and data for intended use only)

   Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:

   - Intentional or accidental attempts to either:
     - perform unauthorized deletion of data or
     - otherwise cause a denial of service or data.
   - Attempts to use system or data for unauthorized purposes

[2] Ibid.

2. **Integrity** (of system and data)
   Integrity has two facets:
   - Data integrity—the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit, or
   - System integrity—the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation.

3. **Confidentiality (**of data and system information)
   Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

The ultimate goals of any security strategy are threefold: availability, confidentiality and integrity of the data and systems.Tripwire data integrity assurance is the cornerstone.

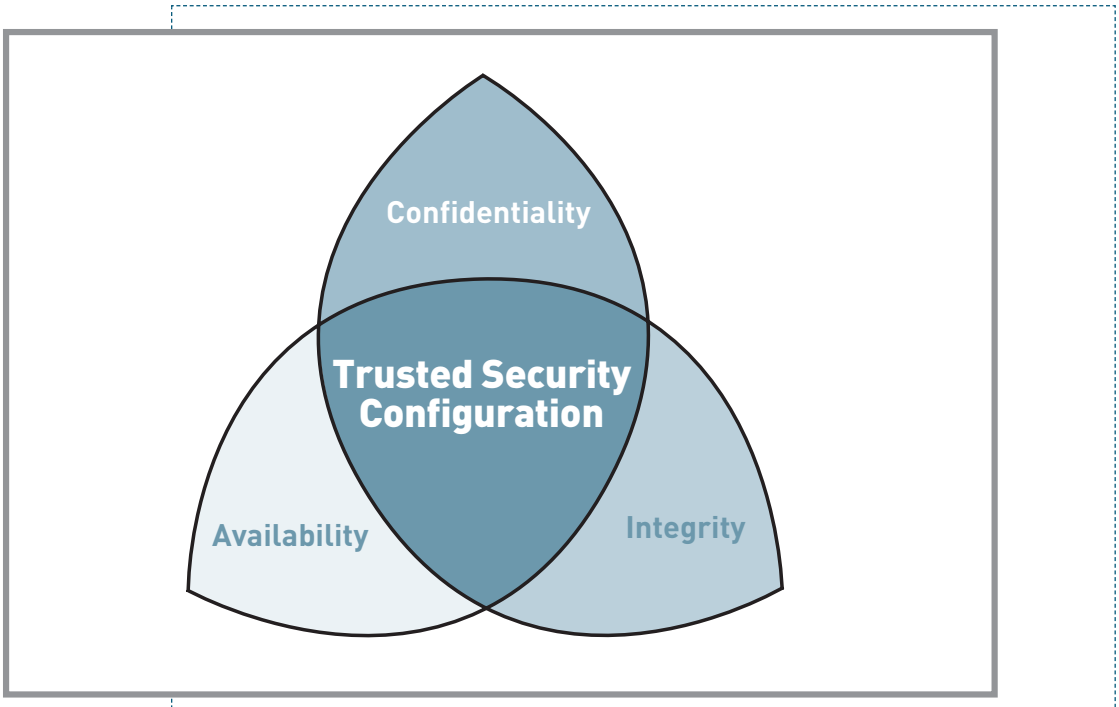


Figure 2 – Trusted Security Configuration Model

Security & Integrity Threats

Deploying a layered security solution will help protect organizations from the many security challenges that exist today. Security challenges fall into several broad categories:

- System misconfiguration
- Internal users
- External threats
- Lax security policies and processes
- Experimentation and inadvertent errors

Businesses must address each of these broad challenges to prevail. Connecting to the Internet, essentially connects the business to the public networks of the entire world, thus exposing business infrastructures to the possibility of exploitation by thousands of people in the outside, online, global community. The key points for consideration when reviewing your security standing are:

- **System Misconfiguration:** A recent analyst report indicates that more than 65% of security vulnerabilities in an organization are as a result of system misconfiguration. These include (but are not limited to) updating systems with the latest vendor-released security fixes and periodic review of risks and policies resulting from changes in services and/or service levels offered. Strong security requires operational diligence, driven by the requirements of policy and processes and a clear understanding of the underlying business risks that the organization takes when not adhering to the policies/processes.

- **Internal Users:** Threats from internal users can be classified as either malicious or inadvertent/experimentation. The former is a conscious and intentional attack on the system infrastructure to compromise services or information. Of 239 companies polled by the FBI in March 2000, 71% reported unauthorized access to systems by insiders.

  The latter is a result of well-meaning employees who can cause severe service outage or information compromise as a result of inadvertent or ill-advised actions. Indeed 'experimentation' is one of the most common reasons for system outages and has a direct bearing on system misconfiguration. It is also a result of failure to employ policy and the appropriate technology related to change control.

- **External Threats:** A lesser, but perhaps more potentially embarrassing threat to your business comes from outside; viruses, worms, denial of service, web-defacement, and hacker penetration from the Internet can lead to downtime and loss of reputation and business, especially if publicized in the popular media.

- **Security Policy:** An effective security policy will EXPLICITLY make clear the risks that a business has foreseen and how they must address them, while also setting IMPLICIT standards of practice that must be adhered to. We raise the issue of security policy here because policy ITSELF must be created first of all, and it must address the following matters of misconduct, hacking, etc.

- **Theft:** A matter often not considered is simply one of physical security. All computers (and their components) are valuable physical assets, ripe for theft. Theft leads to downtime, embarrassment, loss of business, and leakage of proprietary information.

- **Fraud:** At least two fraud-related risks impact e-commerce businesses and must be addressed: bogus payment, and liability due to theft of customer payment data, such as credit-card details.

- **Proprietary Information:** Your data is your lifeblood. Threats come from physical theft, accidental deletion or destruction (fire, flood)—or more insidiously perhaps from non-destructive copying, leaving no trace of the theft.

- **Human Error:** This is perhaps the broadest yet mildest form of threat; lack of security awareness amongst employees can lead to leakage of proprietary data through personal emails, being locked-out of network resources through loss/forgetting of passwords, and vulnerability to con-artists and "social engineering."

With data at the heart of today's business, a company's ability to compete and survive depends upon the integrity of its IT infrastructure. And that infrastructure is increasingly vulnerable to unintentional misuse and malicious attacks.

Typical and Necessary First Steps

When managers and security professionals consider implementing a security strategy, typically they implement an Intrusion Detection System (IDS) as the key first step: that's because executives and shareholders alike want to keep all the 'bad-guys' out. But who and where are the bad guys?

A complete intrusion detection system (IDS) must consist of three key components: firewalls, network intrusion detection, and data integrity assurance tools. However, while firewalls impose a barrier at the point of connection between the Internet and the protected network, and real-time network intrusion technologies are an effective second line of defense, neither address internal system misuse.

A complete enterprise security solution requires tools that can be quickly deployed and enable a security administrator to rapidly identify malicious or unwanted attacks. When combining layers of defense, these elements work together to form a resilient barrier to unauthorized intrusions and malicious attacks while complementing other security solutions such as authentication and encryption systems.

Whenever network security is compromised, whether due to a new worm attack or an intrusion from an inside source, the integrity of company data is in question. Many e-mail viruses modify or remove files from PC users' disk drives; successful attacks against Web sites deface their content; and root kits modify system executables with ones that completely cover an intruder's tracks.

These business assets are too valuable to be left open to compromise, which is where Tripwire® data integrity assurance solutions come into play.

A Unique Tripwire Advantage: Who's Guarding the Guard?

One of the primary applications of Tripwire software is to monitor the integrity of other security products such as firewalls, intrusion detection systems and anti-virus scanners. One of the first things attackers try to do is disable the security tools on the servers that they are attacking.

In some cases, a small change to a firewall might have a dramatic impact. For example, a change to the firewall configuration settings might be changed to either open up or shut down ports. If an attacker can change a firewall rule to allow them to open a port, then that would allow the attacker to gain access through the firewall to other more critical servers or targets.

Some security products have configuration files that are stored in plain text that control how the product operates and functions. It is important to monitor these files in order to detect any unauthorized changes that may allow an attacker to subvert the tool. Tripwire software can easily be configured to monitor these specific configuration files.

Other files to monitor are the binary files of security products in order to verify that no new possible malicious binary versions of the product are replaced. Tripwire for Servers uses cryptography (El Gamal) and encryption (3DES & SSL) to protect its configuration and database files to prevent any tampering. These are included in the default policy file which ships with the product—in essence, Tripwire technology helps guard Tripwire products themselves, so you are assured that they cannot be subverted without your knowledge.

Continued on next page.

How Data Integrity Assurance Fits into a Layered Security Strategy

Trust in the network begins with the certainty that you're starting from a known good state. Data integrity assurance software, such as Tripwire for Servers and Tripwire for Network Devices, establishes the baseline by taking a 'snapshot' of data in its desired state. It detects and reports changes to the baseline, whether accidental or malicious, from outside or within. By immediately detecting changes from the baseline, Tripwire software can trigger fast remediation, and avoid the necessity of having to rebuild servers or routers from scratch.

In this way Tripwire software provides the foundation for data security and ensures a safe, productive, stable IT environment. Tripwire software detects change, whether accidental or malicious, from outside or within, and is the only way you can know for certain that your data is safe and your systems remain uncompromised. Tripwire software is used for: intrusion detection, file integrity assessment, damage discovery, change/configuration management, system auditing, and policy compliance.

A Unique Tripwire Advantage: Who's Guarding the Guard?

Continued

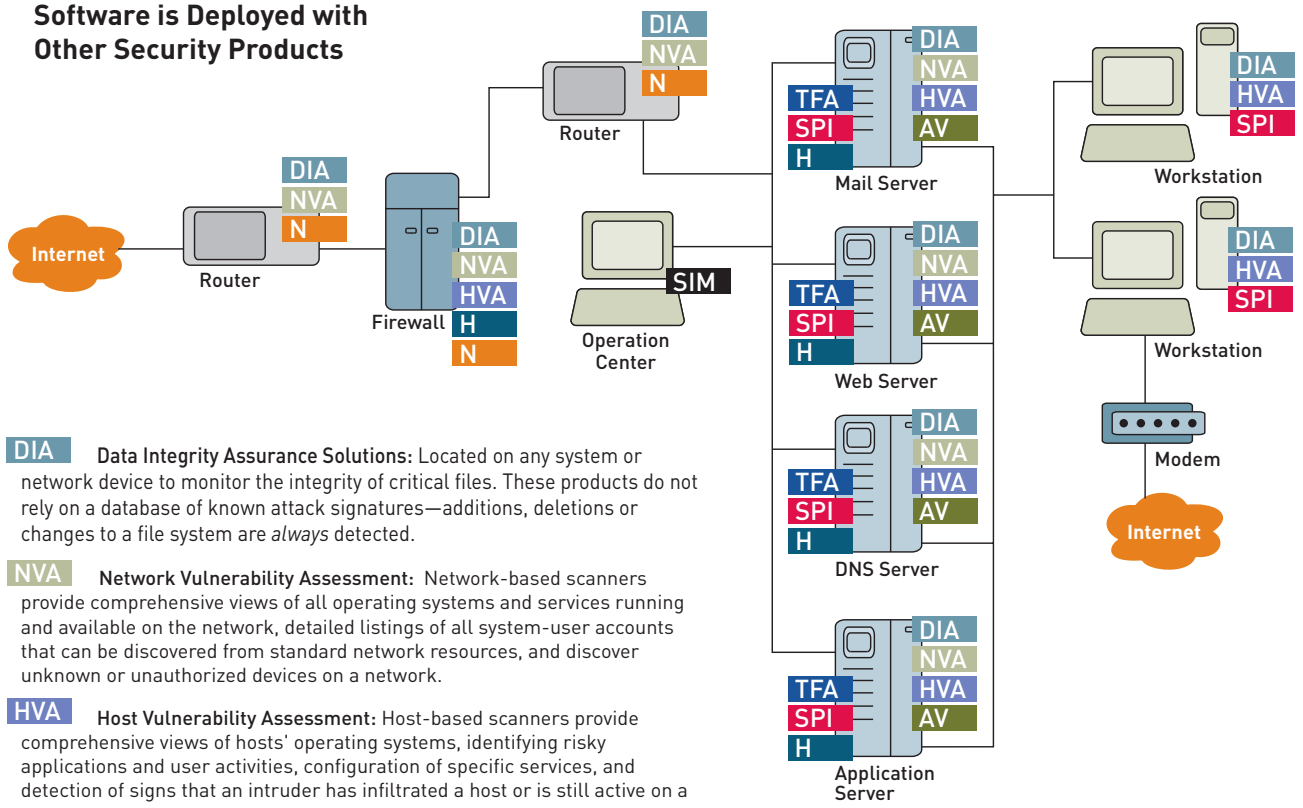
Unlike firewalls, the Tripwire approach is not focused on the prevention of unauthorized access. Instead, it monitors data at rest and identifies data changes, and then alerts the system manager to unauthorized changes or internal or external intrusions. This is an extremely important security function as many intentional and unintentional unauthorized changes on data at rest take place from within an organization, or inside a firewall.

There are many types of security tools that do many different jobs, but it is important that these applications are also being monitored to allow for immediate notification and remediation of events that could potentially allow for an attacker to penetrate your network infrastructure. Tripwire software is used in many cases to complete a well-rounded security policy complementing other security tools that may lack integrity verification functionality. In fact, determining the integrity of a system is one of the key components of having a solid security foundation.

How Tripwire Complements Other Security Technologies

There are many data security technologies that a company can deploy that accomplish different goals. Many of these technologies complete specific security objectives and functions and play a key role in building a layered security strategy.

How Data Integrity Assurance Software is Deployed with Other Security Products



DIA **Data Integrity Assurance Solutions:** Located on any system or network device to monitor the integrity of critical files. These products do not rely on a database of known attack signatures—additions, deletions or changes to a file system are *always* detected.

NVA **Network Vulnerability Assessment:** Network-based scanners provide comprehensive views of all operating systems and services running and available on the network, detailed listings of all system-user accounts that can be discovered from standard network resources, and discover unknown or unauthorized devices on a network.

HVA **Host Vulnerability Assessment:** Host-based scanners provide comprehensive views of hosts' operating systems, identifying risky applications and user activities, configuration of specific services, and detection of signs that an intruder has infiltrated a host or is still active on a system.

AV **Anti-Virus Scanners:** Provide the ability to block viruses from getting to servers or workstations. These products should be deployed to prevent virus attacks from deleting and changing files. Many AV products use a signature database to scan against to detect viruses. Often time new viruses will not be in the database until it can be updated, which leaves a system vulnerable.

TFA **Two Factor Authentication:** Provides the ability to verify that someone who is trying to access a system is actually authorized to access the system. The most common form of authentication is the use of logon passwords, the weakness of which is that passwords can often be forgotten, stolen or accidentally revealed. Often times passwords will be combined with tokens to provide two-factor authentication.

SIM **Security Information Management:** Enables users to consolidate security reports and information from many different security products to correlate and provide actionable data.

SPI **Security Policy Implementation:** Enables security mangers to automate each step of the security policy from a central console. These tools enforce awareness and assess employee understanding of security policies

H **Host-Based Intrusion Detection Systems:** Monitor system or application logs for evidence of attack, based on a database of attack signatures.

N **Network-Based Intrusion Detection Systems:** Examine network packets for suspicious patterns, based on a database of attack signatures.

Figure 3 – This network diagram illustrates where Tripwire software should be deployed along with other security products to build a layered security defense

Firewalls/VPNs

A firewall is a system or group of systems that enforces an access control policy between two networks. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Usually, a firewall's purpose is to keep intruders out of your network while still letting you get your job done.

Tripwire software data integrity assurance complements these firewalls as part of a layered security strategy:

- Tripwire software will detect intruders from both within and from the outside where most damaged is caused.
- Firewalls can't protect against attacks that don't go through the firewall.
- Tripwire software can operate on many types of servers monitoring all changes.
- Tripwire software can be used to monitor and detect changes to firewall configuration changes as well as exploitable operating systems.
- Firewalls are deployed to detect and protect from known vulnerabilities.
- Tripwire software will detect changes based on both known and unknown vulnerabilities.

Virtual private networks (VPNs) allow remote employees, partners and customers to securely access a corporate network by establishing an authenticated, secure connection. These solutions certainly must be deployed as part of a layered security strategy. Other security products, such as data integrity assurance, will augment VPN security by verifying system and data integrity and changes that would be made by authorized individuals who have an authorized and secure VPN connection.

Antivirus

Antivirus companies have made virus protection the best known defense against network invasion. Certainly, no layered security strategy is complete without it. However, virus protection software works primarily by looking for known virus signatures, coming from the outside in. That's why virus definitions must continually be updated—the software won't find what it hasn't been told to look for. Nor does it bother to report file changes not associated with virus signatures.

Tripwire software is complementary to antivirus solutions because if a virus goes undetected from an antivirus solution, Tripwire software can be used to assist in system or file recovery. For example, many worm viruses change or delete Windows Registry values that would be nearly impossible to detect if a user didn't know which entry changed. But with Tripwire for Servers, a user can quickly detect exactly which registry entry was changed or deleted and replace only those files that were affected.

Authentication

Authentication is the process of determining whether something or someone is who or what it has declared it is. The most common form of authentication is the use of logon passwords, the weakness of which is that passwords can often be forgotten, stolen or accidentally revealed. Often times passwords will be combined with tokens to provide two-factor authentication. Users who need access must identify both elements (token and password) in order to be authenticated.

Tripwire software is complementary to all forms of authentication because it can identify any changes to a machine if the authentication method has been compromised. For example, suppose an attacker has obtained both the token and password from a person who legitimately has the right to access a machine and gets access to a machine or server to plant a backdoor (software that allows a hacker to continue to have access to a machine without being detected). After the attacker has planted the backdoor, he returns the token to the person he had stolen it from. At this point, no one knows that this attacker has had access to the server, but later the attacker comes back to compromise and steal critical company files.

Tripwire software would provide two things here. First, it would identify that additional files (backdoors) have been installed on the server in a hidden directory. The administrator can quickly delete this file(s) which will not allow the attacker back into the system. Secondly, Tripwire software will identify the company files that were tampered with, so that measures can be made to recover or restore those files. No authentication product can provide this ability to recover from a breach.

Intrusion Detection Systems (IDS)

There are two primary kinds of intrusion detection systems:

- **Host based –** Software that monitors a system or application log files. It responds with an alarm or a countermeasure when a user attempts to gain access to unauthorized data, files or services.
- **Network based –** Monitors network traffic and responds with an alarm when it identifies a traffic pattern as either a scanning attempt or a denial of service or other attack.

Intrusion detection, again, is a vital facet of layered security. However, it will not tell you how data has been compromised, what's changed on your system, or what your data baseline was before the attack. Moreover, IDSes do not look for internal threats, either malicious or due to employee error. Only data integrity assurance software monitors data itself for change, whether initiated internally or externally, regardless of the cause or motive.

Firewalls, intrusion detection and anti-virus scanning systems are all quite effective against identified attacks. Such 'tried and true' techniques continue to be employed by hackers simply because so many companies have failed to implement these basic defenses. Of course, the industry's best and brightest hackers are constantly coming up with new and innovative ways to penetrate network resources. And when they do, the vendors who supply firewall, IDS and anti-virus technologies upgrade their solutions. But what happens if your network is one of the first to experience a new form of attack? Or what if there is a defense against an attack, but you haven't yet patched it into your network? How can you protect yourself against what we cannot predict?

Vulnerability Assessment Scanners

These tools check the settings on systems to determine whether they are consistent with corporate security policies and if they identify "holes" or vulnerabilities that attackers could exploit. Many products simulate the behavior of attackers to learn which of as many as 600 possible weaknesses possibly present on a system could get attacked.

Security Information Management

These products provide a very useful function. They centrally manage security data from other security products to provide analysis and correlation of attack patterns across a network. They enable users to interpret the vast amount of security data from multiple products into usable and actionable data that can be responded to. A security product is only of value if the user can use and understand the information that other security products provide. SIMs try to assimilate information to make it easier for users to understand. These products are a component of a layered security solution because they can provide a higher level view of a company.

Digital Video Surveillance

One often neglected part of a layered security solution is digital video surveillance that physically watches servers, network devices or data centers. Integrating digital video surveillance security with data security measures provides a well rounded approach at protecting a company's critical IT infrastructure. Some video surveillance solutions can send images electronically over a wired or wireless network to centralize all computer security monitoring.

Putting It All Together: Benefits of Data Integrity Assurance

Tripwire software for servers, firewalls, routers, and switches helps companies build a foundation of security by providing them a way to quickly detect accidental or malicious changes to data and quickly recover to a desired good state. In combination with other security technologies, Tripwire software provides companies the assurance that their digital assets are being monitored and protected.

Tripwire software provides the following benefits when deployed to detect data integrity changes:

- **Establishes a Foundation for Data Security –** Tripwire takes a snapshot of data in its known, good state, providing companies with a good starting point to monitor against. This snapshot allows companies to verify that changes exist from the last known, good snapshot. This integrity assurance provides a critical component in establishing and maintaining data security.
- **Lowers Costs –** Using Tripwire software will help lower costs associated with troubleshooting, downtime or change management. Instead of wasting precious time looking for individual files that have been tampered with or attempting to troubleshoot a system error, you can use Tripwire software to quickly detect the change and allow you to get back to business. Time spent discovering the source of system problems is reduced from hours—sometimes days—to just minutes, freeing up valuable IT resources for more proactive, productive activities.
- **Maximizes System Uptime –** Tripwire software enables companies to maximize their investments in IT by eliminating risk and uncertainty, while maximizing system uptime. Tripwire software pinpoints the exact location and nature of change to enable quick restoration of systems to a desired, good state. This reduces down time and maximizes uptime.
- **Increased Control and Stability –** By verifying system integrity and limiting integrity drift users gain more control over systems by knowing unequivocally whether a system has drifted from a known good state.

Summary

There are many security practices that companies should implement in order to develop and deploy a layered security solution that prevents, detects and responds to security incidents. Developing a robust layered security strategy requires companies to consider complementary solutions that can address attacks and breaches from the outside and the inside. In today's environment, organizations connected to the Internet must be more vigilant than ever. Networks are scanned for vulnerabilities many times a day. Viruses and worms abound. And the threat of cyber terrorism looms. It takes a comprehensive well thought-out strategy to protect against all of these problems.

By utilizing Tripwire software companies will not only mitigate security threats, but also create a more stable IT environment. By detecting unauthorized changes, companies can proactively increase the effectiveness of their change control and configuration management. Computer security is in many ways similar to physical security in that no single technology serves all needs—rather, a layered defense is proven to deliver the best results.

Tripwire software provides the fundamental security layer that provides a high degree of confidence in the integrity of data assets and system infrastructure. This foundation provides the means to detect and understand changes to systems and data over time, and better enforce the security and availability of those assets. As a result, companies and their customers are able to maintain trust in their network and IT infrastructure.

TRIPWIRE

www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, Oregon 97205 USA