Change is the Enemy of Security & Compliance

10 Network Changes You Should Be Looking For

Table of Contents

1. An Unauthorized Device Joins Your Network 4
2. Mobile Systems Join and Leave Your Network Continuously 5
3. Network Assets Disappear From Your Inventory Databases 6
4. A New Patch Is Available From a Technology Vendor 6
5. Network-Aware Applications Are Installed On Your Network 7
6. Your Users Do Not Follow Security Policy 8
7. Access Permissions Change for an Asset Important To the Business 8
8. Your Network Develops a Leak 9
9. Legacy System "Guru" Leaves the Company 10
10. You Install New Security Hardware or Software Systems 10
Summary 11

This document lists ten common changes in enterprise environments, all of which can chip away at your security and compliance in ways that you might not realize. Some are obvious; some are subtle; all can have a negative impact.

Your network is evolving through continuous changes.

New assets are joining your network. Users are installing new applications. Network services are opening and closing. File permissions are changing. An application vendor is issuing a patch. Somewhere, a hacker is coming up with new ways to access your important data. A valued IT employee is thinking about leaving the company.

The average enterprise network experiences thousands of changes per day. Many of these changes chip away at your security posture, causing your network to drift away from its most secure state. Any one of these changes could be the one that introduces a major security risk.

Unfortunately, you cannot stop time and you cannot stop change. Understanding the impact of this relentless pace of change must become part of your operational security plan or your security posture will inevitably fall prey to the forces of time. So how do you do this?

By moving away from "snapshot security" and continuously monitoring your network for changes, you can analyze the changes as they happen, logging the benign changes (for audit and compliance purposes) and fixing the high impact ones (for security purposes). Fixing a small problem is faster and easier than fixing a big one, and monitoring for and reacting to change immediately will help you find and fix problems while they are still small.

This whitepaper lists 10 ways that enterprise environments typically change and what you can do to identify, analyze and manage these changes and their associated risks on an ongoing basis.

1. An Unauthorized Device Joins Your Network

Any device attached to your network without authorization is a rogue device. Since these devices fall outside official network inventories, legacy asset management systems are unaware of their existence and traditional agent-based security tools have no way to discover them amongst the sea of thousands of legitimate assets.

A common example of a rogue device is an unapproved, unsecured wireless access point and anything that attaches to it. However, many other sources of rogue devices place corporate assets at risk, such as:

- Laptops brought in by consultants and visitors
- Home machines brought in by employees
- Employees connecting PCs or home networks to the corporate LAN via VPN

In addition, any device that lacks the controls in place to keep it updated and in compliance with security policy can reasonably be considered as rogue. Since such a device lies outside of the direct control of security administrators, you must consider it a threat.

The Risk

Rogue devices can be significant sources of problems. Since they exist beyond the review of security controls, you usually have no knowledge of their configuration, their security status, or the intent of their operators. The presence of rogue devices on a network is usually a serious violation of regulatory standards.

What should you do when an unauthorized device joins the network?

- **Discover**: Monitor your network continuously for devices joining the network so that you can detect newly-active devices immediately. Automatically scan each new asset to determine its configuration, level of vulnerability and state.
- **Analyze**: Perform a security analysis on the new asset to determine if it is compliant with security policy, rank its overall risk compared to the rest of your monitored assets, and determine its overall risk in the context of your environment.
- **Enforce**: If the asset poses a serious and imminent threat to security posture, it should be quarantined or blocked from access to the network. Less critical threats should be identified by an administrator and assigned an appropriate asset owner within the IT organization who is responsible for ensuring that the system is remediated to comply with security policy. All such asset appearances should be recorded for audit and forensics purposes.

2. Mobile Systems Join and Leave Your Network Continuously

Mobile systems such as laptops, personal digital assistants (PDAs) and smart phones present their own distinctive challenges. The same features that support easy and immediate communications at airport and coffee shop hotspots also leave these tools open to compromise.

The Risk

This risk expands exponentially every time a mobile device reconnects to your corporate network. If a laptop leaves your realm of control it could potentially network with anyone, anywhere – and possibly be compromised as a result. You have no way to know until it reconnects to the network – as a trusted device inside the network perimeter.

On top of this, it is extremely difficult to enforce a security policy when IT security has intermittent access to the target device. Mobile systems pose significant risks to security compliance initiatives.

What should you do when a mobile system joins the network?

- **Discover:** Monitor your network continuously for mobile systems joining the network. Ensure that you are able to identify devices and systems even though they may be connecting with different IP addresses and on different parts of the network.
- **Analyze:** Perform a security analysis against the new asset to determine if it is in compliance with security policy and asses its level of overall risk to the organization.
- **Enforce:** The major difference between mobile assets and rogue devices is that mobile assets are known to IT. There needs to be a process for monitoring and updating mobile assets. If the mobile asset poses a serious and imminent threat to security posture, it should be quarantined or blocked from accessing the network. Less critical threats should be identified by an administrator and assigned an appropriate asset owner within the IT organization who is responsible for ensuring the system is remediated to comply with

security policy. All such asset appearances should be recorded for audit and forensics purposes.

3. Network Assets Disappear From Your Inventory Databases

Over time, your devices may become misplaced. They remain connected to the network, but there is no record of their location. If there is no change in their function, you are unlikely to find them, even with network behavior monitors.

Assets usually become "stranded" for any number of valid reasons. Sometimes an act as simple as an agent crashing or being inadvertently removed can cause an asset to be lost. In other cases, a merger or reorganization may occur and nobody really knows what assets were there to begin with.

The stranding of assets is something that easily goes unnoticed, but it happens in most companies and usually involves 2-3% of the total network asset base. However, the industry analyst RHK, Inc. estimated in 2002 that as much as 20% to 30% of telecommunications industry network assets become stranded over time. Even a fraction of this amount represents a serious threat to network security and performance.

The Risk

Stranded assets are not actively managed or updated. They become prey to common compromises and are often the primary access method for further incursions into a network. In addition, stranded assets represent a significant violation of many regulatory standards.

What should you do to prevent network assets disappearing from inventory databases?

- **Discover:** Regularly monitor your network asset base using a combination of active and passive network discovery monitoring. Continuous monitoring is a best practice. Ensure that your network monitoring can uniquely identify systems whose IP address, system name, and location may change over time, and will find network-connected assets regardless of the software running or configuration state. Also ensure that you capture as much information as possible about asset configuration, including asset type, operating system, installed applications, patch levels, and configuration settings. You will use the detailed information to identify stranded assets.
- **Analyze:** Compare the results of your network monitoring with your inventory database. Identify unmanaged systems by finding systems that are out of compliance with policy, out of date, lack typical software packages or contain unusual software, or that have not been "touched" for longer than comparable systems.
- **Enforce:** Actively populate your inventory database using the results of network monitoring. Schedule remediation for any systems that are out of compliance and assign an owner to each affected system.

4. A New Patch Is Available From a Technology Vendor

Service packs, hot fixes and patches for operating systems and applications provide critical pathways for closing security exposures before vulnerabilities lead to attack. Just tracking the exponential growth in patches for nearly every hardware or software product deployed in a typical

enterprise environment is an overwhelming task, and actually implementing all these in-service repairs in a timely manner is all but impossible.

Poorly planned patching efforts can lead to serious service interruptions – or even rejected remediation efforts if your network security solution itself sees the patch as a threat. You need real-time insight into which systems have been upgraded to any given patch level, including clear prioritization criteria so that the most critical systems are upgraded first. Unfortunately this is exactly the information that is lacking in many enterprise environments.

The Risk

Patches are not always applied correctly, even when a patch management system says they are. Lack of patches represents significant security risk, particularly when you believe they have been applied successfully. There are a variety of factors that can disrupt a successful process—for example the endpoint security agents can treat patch files as an intrusion and prevent them from being installed, or the device was not rebooted after patching. Each security product was performing its function properly, but the overall security posture was not improved.

What should you do when a new patch becomes available?

- **Discover:** Use your vulnerability management system to identify all the systems in your network that should have the patch installed.
- **Analyze:** Configure internal security policy to require the new patch level. Use the asset configuration monitoring system to identify any non-compliant assets. Compare the list of non-compliant systems with the list of systems patched.
- **Enforce:** Use your patch process to apply the patch. Then, use your vulnerability management system to conduct a post patch verification scan to validate that patches have been applied successfully. Ensure that this system can identify operating systems, applications by version, and patch levels.

5. Network-Aware Applications Are Installed On Your Network

The software counterpart to a rogue device is an unauthorized application. Any code that executes on your network without your explicit approval and supervision has the potential to carry a malicious payload. Peer-to-peer applications, instant messaging, and guerilla Web or FTP servers grab the most attention, but any installer that comes from an untrusted source places corporate assets at risk. Hundreds or thousands of users on an enterprise network represent endless opportunities for unauthorized applications to be installed, greatly complicating your ability to remain on top of this challenge.

The Risk

Software applications themselves may inadvertently disguise malicious or unauthorized traffic. Encrypted programs such as SSH, remote control applications and desktop redirectors that route corporate email to PDAs and smart phones all create traffic that, even when legitimate, cannot be "read" by firewalls, antivirus or most intrusion detection/protection systems. If you cannot recognize these unauthorized services when they first connect to your network, you cannot stop attacks that use these tunnels until after they have penetrated the network perimeter.

What should you do when a new network-aware application appears on your network?

- **Discover:** The most important aspect of your security policy in this regard is the ability to discover new network services quickly. Continuous network monitoring with active and

passive scanning capabilities gives you the best combination of timely detection and detailed information.

- **Analyze:** When you detect a new network service, immediately analyze it for security risks using a vulnerability management system.
- **Enforce:** If the new application represents significant security risk, you should attempt to quarantine the affected device immediately by disabling its network access or altering firewall settings. You should also notify the appropriate administrator(s) immediately and attempt to rollback, patch, or otherwise remedy the security risks. Often the solution for remedying the problem of new applications is to remove the application from the network entirely and not to simply patch the application, which would have the effect of leaving your network with a secure, yet still undesirable, application on your network.

6. Your Users Do Not Follow Security Policy

Systems and devices can start out being in perfect alignment with security policy; users over time make changes that can serious implications. For example, inappropriate changing file permissions, weak passwords that do not meet the security policy represent threats that cannot be uncovered through traditional discovery processes.

The Risk

Gartner estimates that 65% of cyber-attacks come from system configuration errors – and only 35% result from software vulnerabilities.

What should you do to enforce sound security practices?

- **Discover:** Even though this is an issue with user behavior, it can be detected with a security solution that has sufficient access to user assets. A system is needed that can discover detailed asset configuration information and continuously detect changes to those configurations. Security policies, when translated to actual system configuration, often consist of hundreds of settings and objects. Your asset configuration monitoring system must be able to handle this level of detail and continuously audit your assets for compliance with internal policy. A combination of passive and active network scanning techniques can discover and log asset configurations and changes in detail.
- **Analyze:** Compare discovered asset configuration with internal security policy. Determine not only what assets are out of compliance, but to what degree, and what risk the non-compliant state poses. Continuous discovery and analysis will identify non-compliant changes as they are made.
- **Enforce:** Educate users and their managers about non-compliance. Create a culture where adherence to security policy is valued and rewarded and non-adherence is penalized. Some IT administrators may even choose to quarantine non-compliant systems or rollback unauthorized changes.

7. Access Permissions Change for an Asset Important To the Business

For very reasonable business purposes, two colleagues in accounting need to share some data files relating to an upcoming earnings report. They know their systems are networked and on the same segment. So one of the employees changes the file access permissions to allow his colleague to read and modify the necessary files. Unfortunately, so can the rest of the company.

Dozens of small, seemingly innocuous changes like this cause an asset's configuration to drift, exposing more and more sensitive data to unauthorized access. Many companies do not have the ongoing mechanisms to monitor for this kind of change except manually for an audit.

The Risk

Putting aside the issue of regulatory compliance, this example is perhaps the most effective illustration of how change is the enemy of security. Multiply this small change by thousands per day and it becomes clear how easily security can be compromised - not from one big change, but from a thousand small ones.

What should you do to prevent dangerous changes to access permissions?

- **Discover:** You must continually monitor your network for change. "Snapshot security" might identify this type of risk, but only after it has been active for a while.
- **Analyze:** Upon detecting a change, you must analyze it for security risk. This requires that you understand which assets contain valuable information.
- **Enforce:** Fix any problems you find immediately. It is easier, faster, and less costly to fix a problem when it is small and new than when it has been around for a while. In this particular example, the broad file share permissions should be detected the instant the change is made and rolled back immediately, with notification to the user making the change that such a change is dangerous, unauthorized, and non-compliant.

8. Your Network Develops a Leak

Data files are the most shared resource on your network. After all, how useful would email be without the ability to send a spreadsheet or document for someone else's comments and edits? End users know that the most straightforward means to move files from system to system is to create a shared folder on a Windows system or set up a centralized server via NFS or a network attached storage (NAS) device.

The Risk

The challenge with shared resources is that the file being shared easily passes beyond the control of the security infrastructure. A spreadsheet comes home on a laptop and is then transferred to a home PC for work over the weekend. Once there, it can easily become infected with a worm or virus prior to transport back inside the network perimeter. Anyone who then accesses that file risks introducing a full-fledged outbreak inside the corporation.

In addition, many organizations use open file shares for posting public information across the enterprise. These resources are often abused for "temporary" storage, with inadequate examination of the files' contents – including the inadvertent disclosure of confidential information. Many groupware, database or Web applications rely on file shares to distribute content or create a collaborative work environment. Any misconfiguration of user privilege risks opening this information to broad distribution, while still appearing as if the application is functioning as intended.

What should you do to prevent a network leak?

- **Discover:** Monitor your network continuously for change, where "change" involves the appearance of existing assets from new locations and changes to file permissions. You should also consider monitoring outgoing communications for sensitive data.
- **Analyze:** Establish a security policy that prohibits chained network shares that transcend your network boundaries. Prevent open file shares.
- **Enforce:** Notify users and administrators when monitoring detects unsafe chained network shares and close them immediately. Open file shares should also be closed.

9. Legacy System "Guru" Leaves the Company

Every organization has special-purpose devices, such as a plotter that requires OS/2, legacy applications running on an AS/400 or an IRIX server placed in production years ago but still perfectly functional. As the original support staff for these devices leaves the company or moves on to other responsibilities – and as technical assistance becomes unavailable from the manufacturer – the means and knowledge to secure these devices become increasingly rare.

The Risk

All these one-off systems still require adequate protection and compliance monitoring both to ensure their security and maintain compliance, so they must either be protected or identified and retired.

What should you do when a guru leaves?

- **Discover:** Monitor the affected systems continuously for suspicious activity and changes that could create risk. Commercial products to analyze these systems for change may be difficult or expensive to obtain, but you may be able to obtain useful information from standard active network scanning and passive monitoring of network traffic.

  In some cases, you may wish to identify a few critical objects to monitor for change and develop a custom check to watch those objects. For example, an older UNIX variant may have an SSH interface to it through which you can enumerate users and software packages running with two simple commands. Use a system where you could add these two custom checks into your enterprise change monitoring and you will now have controls in place to protect these from becoming stranded in the future.
- **Analyze:** Decide whether or not it still makes economic sense to continue using the legacy product, given the increasing support costs. If you decide to continue using the assets, make a small investment in change monitoring for the assets upfront so that the system will be maintained in a secure state down the road.
- **Enforce:** Assign and train personnel to secure the affected systems. You may also want to quarantine legacy systems behind internal firewalls with very strict access controls.

10. You Install New Security Hardware or Software Systems

Over the last few years, network security infrastructure has become increasingly capable and considerably easier to deploy and manage. You trust these devices implicitly once the initial configuration and hardening process is complete.

The Risk

Unfortunately, security infrastructure is just as prone to misconfiguration, inappropriate and/or outdated policy, or hardware failure as any other group of devices. Plus, the configuration of your security systems needs to keep pace with the other changes happening on your network.

What should you do when new security systems are installed?

- **Discover:** Hopefully, you are already monitoring the rest of your network continuously for change. Your monitoring should also include your security products. Any changes to firewalls, IDS/IPS systems, anti-virus systems, etc. should be noted and logged. Where security products reside on assets outside the control of IT, pay particular attention to users' tendencies to disable or weaken protections.

- **Analyze:** Your security policy should explicitly state who is permitted to alter the configuration of a security product. Unauthorized access to security systems is, of course, a significant security risk. More importantly, you also need to analyze the configuration of your security systems to ensure that they are adequately enforcing your security policy, as that policy inevitably changes. Many security products require frequent, even daily updates, to properly protect a system. You should have processes in place to identify what systems need to be updated and make sure updates are being monitored and tracked as part of your policy.
- **Enforce:** Most actions relate to configuration changes for protected assets. However, as you make security monitoring an ongoing process, be sure to include your security systems in your remediation plan. Update firewall rule sets, IDS/IPS configurations, and anti-virus settings to track the changes in your network.

Summary

nCircle Security Risk and Compliance Management Solutions

nCircle solutions enable enterprises to:

- Provide objective security risk metrics across the enterprise considering all critical factors that create risk: configurations, vulnerabilities, network topology and applications.
- Maintain a comprehensive, up-to-the-minute asset inventory with visibility into all substantive changes and whether they introduce security risk or policy deviation
- Minimize the amount of time spent preparing reports necessary to assure passing IT security audits
- Leverage existing security infrastructure, such as vulnerability assessment tools and trouble ticketing systems

nCircle solutions operate without agents and continuously monitor the network for changes to provide administrators with immediate information that allows them to effect timely remediation. nCircle gives organizations a continuous view into their networks, instead of providing periodic network "snapshots." Its ability to continuously scan assets, applications and files is made possible by its intelligent combination of active and passive scanning technologies. After understanding the baseline, its approach is change-centric, as all security risks and policy deviations start with a change. nCircle solutions offer integration with a variety of management infrastructure components (such as trouble ticketing systems and configuration management databases), providing a prioritization framework for scheduling remediation efforts, and include a real-time compliance reporting infrastructure.

Stronger Security, Continuous Compliance

With nCircle solutions, you will have the continuous network visibility you need to constantly assess your security risk and level of compliance with your policies to ensure your configurations are secure, your security risk is minimized, and to easily prepare for and pass your IT security audits.

About nCircle

nCircle is the leading provider of agentless security risk and compliance management solutions. More than 4,000 enterprises, government agencies and service providers around the world rely on nCircle's proactive security solutions to identify, measure, manage and reduce security risk and automate compliance on their networks. nCircle has won numerous awards for growth, innovation and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the USA and in London and Toronto. Additional information about nCircle is available at www.ncircle.com.

nCircle Network Security, Inc.
101 Second Street
Suite 400
San Francisco, CA 94105 USA
+1 415 625 5900
www.ncircle.com
email: info@ncircle.com

1008-02 07/08