- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Bit9

Windows XP End-of-Life Handbook for Upgrade Latecomers

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Introduction

Windows XP end of life is April 8, 2014. Do you have Windows XP systems but can't upgrade to Windows 7 or Windows 8, or can't afford to pay Microsoft for out-of-band support? If so, read this eBook to learn how you can continue to use Windows XP after end of life and still keep your systems compliant and secure.

The Facts about Windows XP

- April 8, 2014, is the end-of-life date for Windows XP and Microsoft Office 2003.
- There will be NO MORE security updates and critical patches available after April 8 unless you pay Microsoft for extended or premier support.
- **The estimated cost of premier support per endpoint system is:**
  - $200 per PC for the first year
  - $400 per PC for the second year
  - $1,000 per PC for the third year.
- **Premier support provides:**
  - Critical patches only
  - Important patches are available at an additional price. Historically, Microsoft labeled many patches as 'important' that, in our opinion, should have been labeled as 'critical'
  - No support for moderate-or low-priority security updates.
- For other widely distributed Windows-based POS systems, such as Windows Embedded POSReady 2009 or POSReady 7, you will continue to get updates/patches until these products reach their end-of-support dates, which are April 2014 and April 2016, respectively.   Both of these products are based on Windows XP system components. Any updates for these products will not be installable on any version of XP, Pro or standard (FES or desktop) image.
- AV solution software will be ineffective in covering XP systems after EOL. Many AV products will not be supported and won't have the necessary signature updates.   AV vendors have announced that they will not support XP or only continue support for 6-12 months.
- Many legacy applications built on XP will no longer be supported after end of life.

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

What Organizations are Affected?

Originally launched in 2001, Windows XP is Microsoft's most widely implemented operating system. Without XP support, organizations across a multitude of industry segments will be vulnerable to malware attacks after April 8, 2014. If your organization is driven by compliance requirements, such as SOX, HIPAA, PCI, NERC, Gramm-Leach-Bliley, etc., you will have even greater challenges. In addition to security concerns, your organization will also be noncompliant without updates and support.

The nature of your business can make for even greater complexity. For example, if you are a large retailer, you may have many distributed systems that are not powerful enough to run Windows 7 or Windows 8, and their POS equivalents. This means you cannot upgrade the operating system without a hardware upgrade and possibly an upgrade to the legacy applications running on the XP systems.

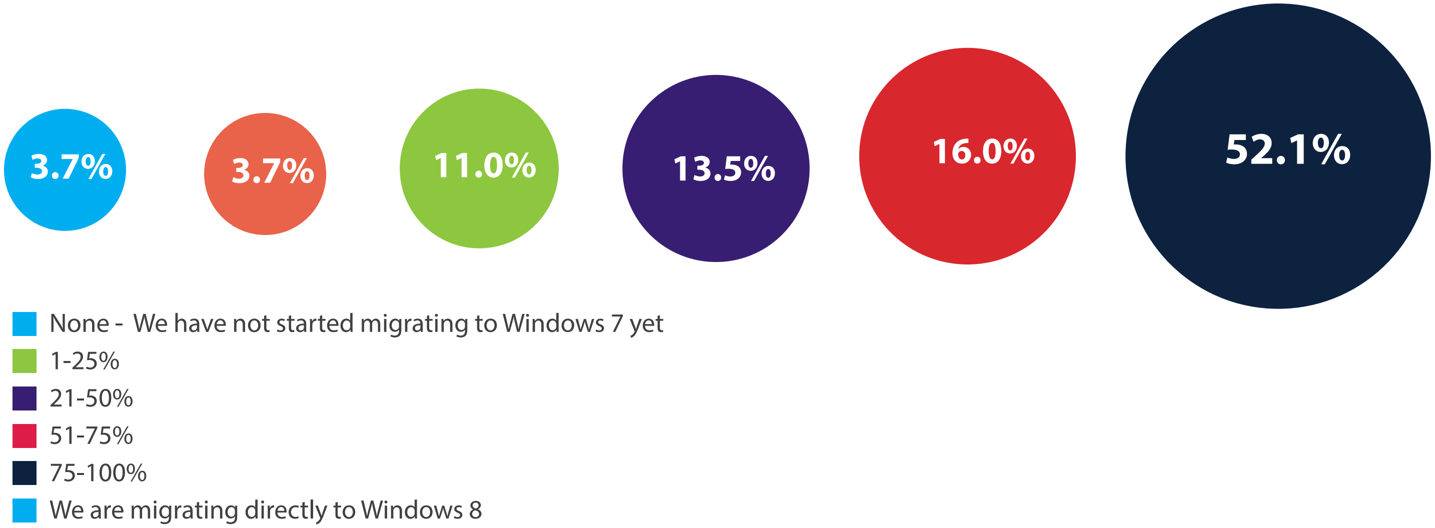
If you are a healthcare provider or payer, you are subject to both HIPAA and PCI requirements. More than likely, you have terminals similar to the retail POS systems that are running older versions of Windows. In addition, you need to ensure the confidentiality of electronic patient health information and audit proof that patient information is safe and secure.

The Status of and Barriers to Upgrading

According to the Application Usage Management Survey conducted by IDC Research and Flexera Software in September 2013, almost a third of organizations – 28 percent – haven't yet migrated 50 percent of their application estates to Windows 7, and only 3.7 percent of respondents plan on migrating directly to Windows 8. Gartner estimates that more than 15 percent of midsize and large enterprises will still have Windows XP running on at least 10 percent of their PCs after Microsoft's support ends. If you are only now starting a Windows XP migration, it is unlikely that you will finish before support stops in April 2014. According to Gartner, it can take six to 12 months to complete an OS migration.

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

What percentage of your application estate have you migrated to Windows 7?



Source: Application Usage Management Survey, September 2013

There are several reasons why your organization may not be able to upgrade to Windows 7 or Windows 8.

- You need new hardware to support the new operating system, a scenario we discussed previously.
- Your organization's mission-critical applications are not compatible with Windows 7 or 8.
- You are unsure whether to migrate to Windows 7 or Windows 8.
- You don't have the budget for the migration.
- Your organization's IT team doesn't have the resources to execute a migration and maintain day-to-day operations.

In some cases, Windows 7 and Windows 8 may not run on your existing fleet, which means that in order to upgrade, you must upgrade your hardware as well. Microsoft's Windows 7 Upgrade Advisor is a good source to learn whether Windows 7 will run on your current PCs. If it doesn't, and if you have a large fleet, this option can be too expensive for you to consider in the short term.

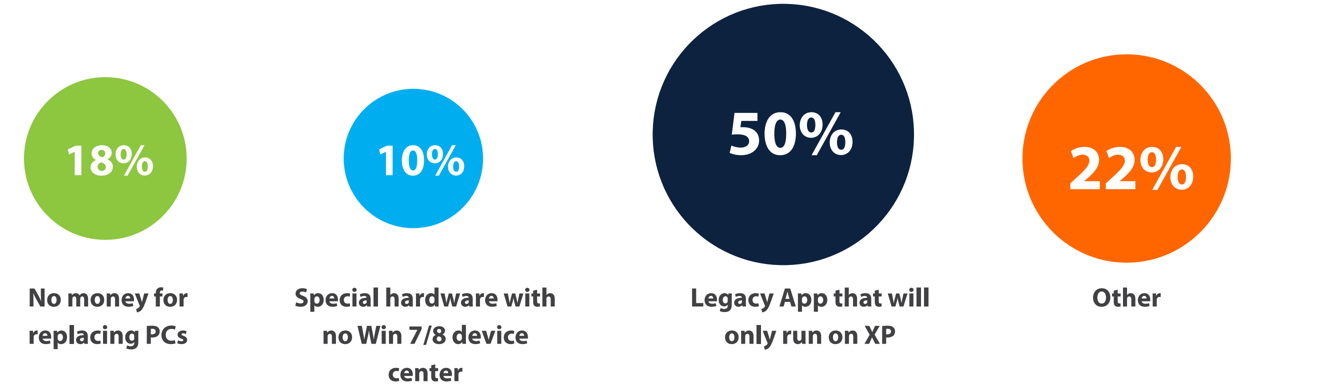
- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Another barrier you may encounter is application compatibility. If you have 32-bit legacy applications running on XP, these applications won't run on, or are not an easy upgrade to, a 64-bit operating system. And, unfortunately, developers of XP-certified legacy applications may not have the budget or the motivation to certify their software on newer operating systems.

Microsoft has produced a list of programs that have trouble running on Windows 7 or Windows 8. Microsoft also has a program that will analyze your application and come back with a compatibility report, but there are concerns with exactly how accurate the application checker is.

On October 30, 2013, Ultimate Windows Security and Bit9 polled more than 250 individuals across a multitude of industry segments to determine the challenges they are experiencing with regard to upgrading. Fifty percent of those polled indicated they had legacy applications that would only run on XP while 18 percent claimed they had no budget to replace XP machines.

What's your hold back on upgrading XP?



You may also have a challenge dealing with third-party applications from vendors such as Oracle, Adobe, etc., who, like Microsoft, are encouraging that you upgrade. It is also unclear whether third-party antivirus and scanning software – software that may be part of your current security stack - will be supported. Some of these vendors have stated that they will not support Windows XP after April. Others have indicated that they will support XP for a maximum of 12 months past the deadline.

The bottom line is that Windows XP's end of life will affect all applications that run on your XP systems and these may be bigger targets for attack than the Windows operating system is itself.

Introduction
The Facts about Windows XP
What Organizations are Affected?
The Status of and Barriers to Upgrading
The Consequences
Compensating Controls
Network Isolation
Virtualization
Positive Security
Why Positive Security
The Advantages of Bit9 as a Compensating Control
The Benefits of Bit9 as a Compensating Control
About Bit9

The Consequences

Unpatched XP systems will lead to "zero-day forever scenarios" – that is, there will be no patches for zero-day attacks so new vulnerabilities will never be remediated. And since Windows XP lacks the memory protection features found in later Windows operating systems, the lack of support can make your situation worse.

Without updates and patches, you may be cited for noncompliance and/or failure to pass assessment and regulatory audits. Here is Microsoft's official position on this topic: "Unsupported and unpatched environments are vulnerable to security risks. This may result in an officially recognized control failure by an internal or external audit body, leading to suspension of certifications, and/or public notification of the organization's inability to maintain its systems and customer information." This statement is absolutely true.

Once you have an operating system that can't be patched and new malware is discovered, your organization will definitely be out of compliance and the effects can be devastating:

Breach and data compromise: Malware authors can get access to highly confidential information such as your consumers' credit card / financial data or patient information.

Financial penalties: Your organization can be fined for failure to pass compliance audits or for being in a noncompliant state (i.e., requirement 6.1 of PCI).

Loss of privileges: Your organization can realize loss of use of major credit cards and access to business-critical data you need to conduct business.

Damage to your corporate brand: This is often the most devastating consequence and can be difficult to remediate. Your organization's public image can suffer from a breach or failure to operate in a compliant state.

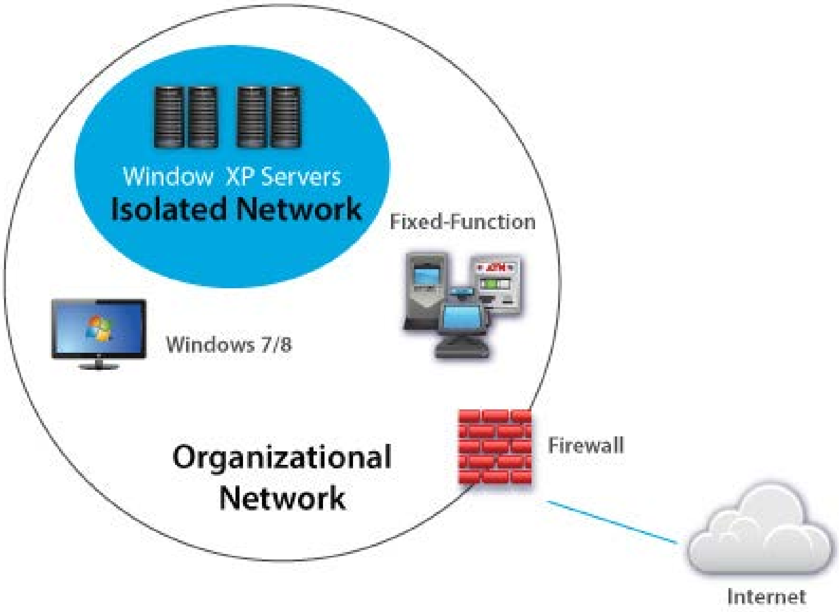
- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Compensating Controls

If you are late in addressing a solution to XP end of life, there are three compensating controls that you can consider to keep your XP systems secure after end of life; **network isolation, virtualization and positive security software.**

Network Isolation

With network isolation, you isolate XP servers so that these machines cannot access your central services. An XP machine will interact with other systems on the isolated network, but cannot interact with any machine outside of the isolated network. With network isolation, you will protect your XP systems from malware attacks but this will only work in cases where your XP applications don't need internet access and/or access to other systems outside the isolated network. Legacy applications, in particular, typically need access to either the Internet or other server applications that you cannot contain on the isolated network. As a result, this compensating control can only be used under very strict circumstances.



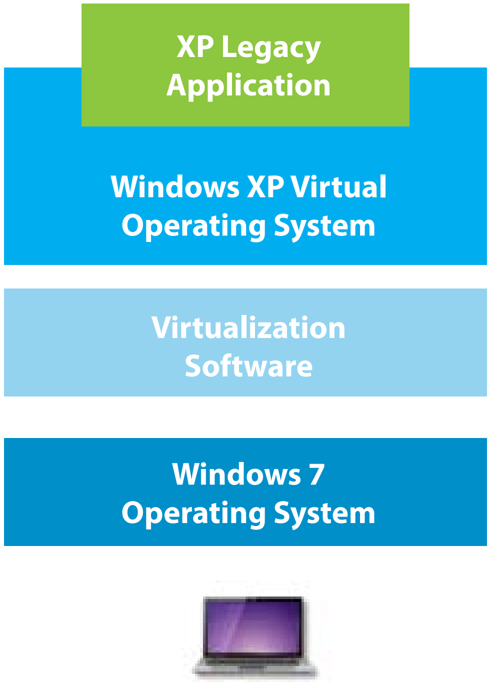
- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Virtualization

Another compensating control is virtualization. The most rudimentary option is virtual desktop infrastructure (VDI) where you host Windows XP (and the XP legacy application) on a PC running Windows 7 or Windows 8.

In this scenario, XP is running on your main desktop but the user's access to the Internet, Microsoft Office, etc. – all of those activities that make you vulnerable to zero-day attacks - are now being accessed via the Windows 7 desktop. As long as the legacy application doesn't require access to the Internet or other applications across the enterprise, this option may work. Also, bear in mind that you are now managing two desktops so you have the additional administrative, training and operational costs to consider. And in many cases, it will cost you just as much to port the XP operating system and legacy applications over to the VDI environment as it will to upgrade the system.

From a security and compliance perspective, there is risk with a virtualization scenario, whether it is a desktop, server or network scenario. You have to be sure to unify the two operating systems and close the security window to the XP system. Also, there is 'virtualization aware' malware that can get through to the XP system. Lastly, if your compliance and internal auditors are not tech-savvy, they may not be convinced that the XP system is safe from attack without audit proof, regardless of the security you have in place.

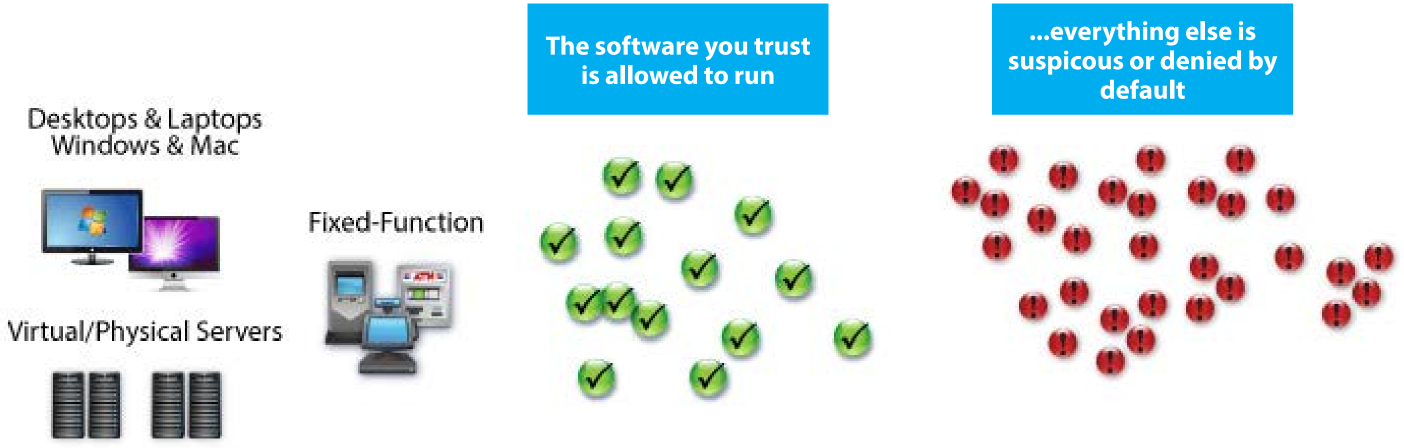

XP Legacy Application
Windows XP Virtual Operating System
Virtualization Software
Windows 7 Operating System

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Positive Security

Positive security is a security model based on known, 'good' applications and focuses on what you want to have happen on your systems. Every rule added to a positive security model increases what is known and allowed. This means that positive security software won't let applications run that are not trusted. While positive security software is designed to secure all your systems, you can also use positive security software to harden out-of-date systems, such as XP, so anything that is not known will not run, preventing zero-day exploits and targeted attacks. Positive security is also often referred to as whitelisting, trust-based security, proactive security or advanced security.

At the other end of the spectrum of security solutions is negative security. Negative security is based on a set of bad applications that you know are out there, and denies access to an application because it was previously identified as bad. Negative security is also referred to as reactive security. Examples of negative security are antivirus (AV) software and host-based intrusion prevention systems (HIPS).



The software you trust is allowed to run

...everything else is suspicous or denied by default

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Why Positive Security

From a compliance perspective, negative security cannot keep your outdated XP systems compliant because negative security only stops known malware and exploits. An example: after XP end of life when Microsoft releases new patches for the newer Windows operating systems, we expect malware authors to reverse-engineer those updates, identify the vulnerabilities and test Windows XP to see if it shares those same weaknesses. If so, malware authors will develop exploit code – new, unknown malware – targeting XP. A negative security solution will not stop this exploit, not only placing you out of compliance but threatening the security of all of your systems.

Laws and organizations such as the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST), and the SANS Top 20 recognize that positive solutions are a best practice for closing the threat window to lock down and protect POS systems, kiosks, servers and endpoints. They endorse positive security technology such as application control and whitelisting, and recommend that companies replace their negative solutions with positive ones.

A positive security model does more than secure your XP systems after EOL. For every operating system, end of life is as certain as death and taxes.

> *By implementing a positive, proactive security model, you are putting in place a fix to stay compliant with XP. More importantly, you will also stay compliant in any end-of-life situation and get protection from zero-day and malware attacks for ALL of your servers and endpoints.*

With positive security, your organization is 'killing two birds with one stone': lowering the cost of compliance and security and getting 100 percent coverage.

You stay **secure** with a positive security model by putting a trust policy in place that controls all of your servers and endpoints and identifies the critical events that are important to your business. In this way, you can detect and stop malware and immediately respond to alerts and incidents.

You stay **compliant** with a positive security model because once in place, you know at any given time what is running on every in-scope system across your organization. You can determine, on a real-time basis, if you have any vulnerabilities and whether any in-scope systems have fallen out of scope. You have all the parameters set up that matter to your business as per the trust policy. In this way, you maintain complete control and stay focused only on the activities that are important to your business.

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

Negative security uses extensive scans to collect data, all of which you must analyze in order to identify what changes are important to your business. The result: these platforms do not provide evidence of real threats that are relevant to your business on a real-time basis AND the scans drain system performance.

If you need to keep your XP system and applications past end of life in April 2014, and you can't afford to upgrade your hardware, or your XP applications won't run on a newer operating system, positive security is your safest, fastest, most cost-effective option for protecting your XP systems.

The Advantages of Bit9 as a Compensating Control

Bit9 offers an advanced positive security solution that your organization can deploy as a compensating security control in lieu of regular patching and updates that are no longer available from Microsoft. Bit9 extends the security window and protects your XP endpoints from breach and data compromise past the end-of-life date. With Bit9, your XP systems will remain compliant because the solution provides:

- **Complete visibility** into everything that is happening on every in-scope server and endpoint so you can measure compliance and risk.
- Automated, **real-time detection** of zero-day and advanced threats.
- A change history and **full audit trail of all server and endpoint activity** including real-time compliance risk measurement and reporting of your in-scope systems, including those which are no longer supported. This reporting provides the actionable intelligence to monitor compliance, identify any unexpected activity or event, and proactively improve the security posture.
- **Prevention to stop advanced threats** and other forms of malware from executing, including targeted, customized attacks that are unique to your organization.
- **Integration across the existing security infrastructure** to understand enterprise-wide compliance risk and exposure.

- Introduction
- The Facts about Windows XP
- What Organizations are Affected?
- The Status of and Barriers to Upgrading
- The Consequences
- Compensating Controls
  - Network Isolation
  - Virtualization
  - Positive Security
- Why Positive Security
- The Advantages of Bit9 as a Compensating Control
- The Benefits of Bit9 as a Compensating Control
- About Bit9

The Benefits of Bit9 as a Compensating Control

- Most important, get your XP systems into a compliant state **BEFORE THE APRIL 8, 2014 deadline** and eliminate financial penalties and brand damage associated with failed audits, data breaches, or noncompliance.
- **Consolidate your enterprise security stack and eliminate the need for and costs** associated with other security software. Bit9 is all you need to get visibility, detection and protection for all servers and endpoints across the enterprise.
- **Lower the cost of obtaining compliance data** because Bit9 uses an up-front trust policy to control change and filter data, allowing you to focus only on those events that are relevant to your business.
- **Eliminate the high costs of XP extended support contracts and hardware upgrades.** Bit9 is an affordable, more cost-effective solution when compared to the costs associated with Microsoft's out-of-band support and/or replacing your fleet of PCs.

Bit9

Bit9 is the leader in advanced threat protection for endpoints and servers based on real-time visibility and prevention. Bit9 is the only solution that continuously monitors and records all activity on endpoints and servers and stops cyber threats that evade traditional defenses. Bit9's real-time sensor and recorder and cloud-based services provide actionable intelligence within days of implementation, and Bit9's real-time enforcement engine delivers the most reliable form of prevention. This combination gives organizations immediate visibility into everything running on their endpoints and servers; signature-less detection and prevention of advanced threats; and a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents. Security teams use Bit9's real-time integration with FireEye and Palo Alto Networks to accelerate incident response and ensure all files arriving on endpoints and servers are safe. Bit9 has stopped the most advanced attacks, including Flame, Gauss, and the malware responsible for the RSA breach. 1,000 organizations worldwide – from 25 Fortune 100 companies to small businesses – use Bit9 to increase security, reduce operational costs and improve compliance.

201312