



Three Must-Have Capabilities for Managing Enterprise Desktop Environments

Today, more than ever, businesses rely on a dependable desktop and laptop environment to drive revenues and growth. However, this very same computing environment is increasingly working against organizations. Security breaches and wayward downloads disrupt operations and have a direct impact on compliance and the bottom line. As a result, IT organizations are completely rethinking how they manage the population of PCs on which their businesses have become so dependent.

Only recently have technical breakthroughs in large-scale information collection and analysis made any new approach feasible. This whitepaper discusses three capabilities made possible by these breakthroughs—visibility, knowledge, and control. Taken together, these principles represent the most fundamental components that every IT organization must employ to realize a winning desktop management strategy.

Table of Contents



Introduction	1
Changing Desktop Environments	1
The Thinning Perimeter	1
Current Solutions Aren't Working	2
Direct Business Impact	2
The Visibility-Knowledge-Control Paradigm	2
Visibility: An Intelligent View of the Total Environment ..	3
Knowledge: A Deep Understanding of the Details	3
Control: Simple Policy Enforcement Set By You	3
Bit9 Parity	4
Examples: Gaining Visibility, Knowledge, and Control with Bit9 Parity	4
Conclusion	5
About Bit9, Inc.	5

Introduction

Today, more than ever, businesses rely on a dependable computing environment to drive revenue and growth. Desktops and laptops have become central tools for mission-critical operations, placing the PC user at the heart of successful enterprises. However, this very same computing environment, open to the Internet and all the mysterious software it contains, is increasingly working against organizations. Security breaches and wayward downloads disrupt operations and have a direct impact on compliance and the bottom line.

This situation has forced IT organizations to rethink how they manage their desktops and laptops on which their businesses rely. Ideally, IT groups want to automatically block all disruptive and unwanted software without getting in the way of end users' business requirements, but in the past this had been unattainable. Only recently, with technical breakthroughs in large-scale information collection and analysis, can this goal finally be achieved.

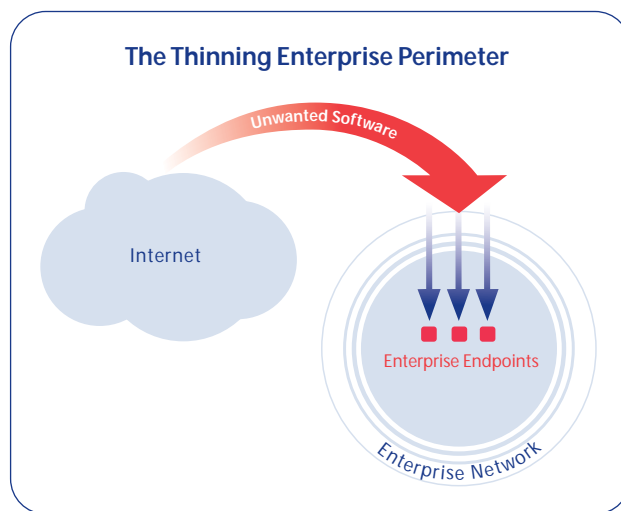
This whitepaper will discuss the three must-have capabilities for managing today's multifaceted enterprise PC environments: Visibility, Knowledge, and Control. These principles apply equally well across a range of initiatives—from reducing the IT support burden, to instituting stronger application control policies, to adhering to compliance regulations. Taken together, they represent the most fundamental components of a winning desktop management process.

Changing Desktop Environments

The power of the Internet has unleashed great business potential from corporate PCs. At the same time, however, it has also changed the nature of desktop management. The increase in connectivity has corresponded to a decrease in IT's ability to ensure the integrity of internal endpoints.

The Thinning Perimeter

Any IT professional who manages desktops and laptops recognizes that the line between internal endpoints and external networks is becoming fuzzier. Mobile laptops regularly connect to foreign access points, and USB drives have enabled the easy transport of new software directly onto PCs. Meanwhile, web-savvy end users are finding and installing a swarm of applications such as instant messaging, file sharing, desktop search, and games—none of which have been analyzed for compatibility, performance impact, or security characteristics. These factors, compounded by the growing pool of sophisticated spyware and malware, scream for more efficient management of desktop security and application control.



Current Solutions Aren't Working

Many existing tools have strained to fill this gap, but none have succeeded because the problem has developed in such a way that it requires an entirely new approach to resolve it. Thus, products with roots in traditional endpoint security or desktop management are simply not the right fit:

- ❑ Current security tools require IT administrators to master elaborate security technologies just to establish basic defenses. This complexity increases the likelihood of misconfigurations or outright misuse, actually wiping away the desired security benefits.
- ❑ On the other hand, desktop management is a major commitment that is heavy in process and hard to enforce. Typically, only a limited portion of applications come under the management of these traditional tools. Supporting any other software through these mechanisms is simply too expensive.

Clearly, these existing strategies do not scale to solve the realities of today's endpoint management problems.

Direct Business Impact

As a direct result of these failures, business suffers in several ways:

- Weaker security and greater risk to business operations
- Unenforced usage policies leading to legal, license, and risk exposure
- Easily corrupted desktops adding to the interruption of business and the cost of support
- An overly strained IT organization

So what is the right approach to address these problems? The answer lies in next-generation technologies that implement the principles of visibility, knowledge, and control.

The Visibility-Knowledge-Control Paradigm

It doesn't take much to recognize that the problems described above have their roots in a lack of actionable information. IT simply hasn't had the ability to see across their entire environment and understand what it was looking at. Without that information, it is impossible to create and enforce suitable policies that improve security, reduce risk, and ensure the integrity of business operations.

To effectively manage dynamic desktop environments, IT organizations must implement tools and processes to enable three critical capabilities with the following properties:

The Visibility-Knowledge-Control Checklist

Visibility	Knowledge	Control
<input type="checkbox"/> Prioritized <input type="checkbox"/> Filtered <input type="checkbox"/> Accurate <input type="checkbox"/> Real-time <input type="checkbox"/> Detailed	<input type="checkbox"/> Contextual <input type="checkbox"/> Relational <input type="checkbox"/> Up-to-date <input type="checkbox"/> Community-oriented	<input type="checkbox"/> Policy-driven <input type="checkbox"/> Clear <input type="checkbox"/> Fast & easy <input type="checkbox"/> Bulletproof

Visibility: An Intelligent View of the Total Environment

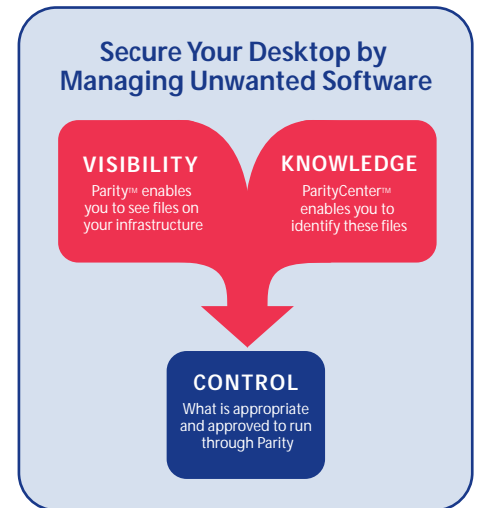
IT has long suffered from a lack of visibility into what software is installed on enterprise desktops—much less when new software arrives from unknown sources. Heavyweight application inventory, deployment, and support systems have helped IT get a handle on a portion of this landscape, but this solution remains substantially incomplete due to the volume of software being installed directly by end users.

True visibility into the environment—now a core requirement of IT—goes far beyond simple installation inventories. Centralized, real-time visibility of new and possibly unknown software as it appears on a desktop infrastructure enables IT to quickly identify and diagnose problems before they have business impact. As a result, IT can focus its scarce resources on just the portions of the environment most in need of its attention.

Knowledge: A Deep Understanding of the Details

It is surprising to realize how limited IT professionals are in their ability to find contextual and associative information about the thousands of software components running on the desktops they are trying to manage. Searching for file names in an Internet search engine is not just inefficient—it is also completely unreliable because the same file name can refer to hundreds of different files and therefore is unsafe to use as a basis for action.

True knowledge of the environment means having information sources upon which you can rely as you are trying to understand what you are seeing in the environment. Often, simply verifying which vendor manufactured a particular file can be enough to determine the appropriate policy for that file. By gaining a full understanding of what all these components are, who made them, how they were deployed, and understanding what other users across the world know about them, IT professionals can make better decisions and greatly reduce the opportunity for error and damage.



Control: Simple Policy Enforcement Set By You

Once you can see across your environment and understand the nature of that picture, the next obvious step is to enforce clear and effective policies to achieve the results you seek. Historically, the lack of visibility and knowledge made it impossible to monitor and enforce sensible policies to ensure a secure and stable desktop environment.

True control relies on a high degree of visibility and knowledge. Accurate information enables stakeholders across IT, risk management, and business operations to set the best policies, but it is clear and effective control that lets you enforce those policies. By regaining control over user desktop systems, individual business owners can implement operational policies to stop business disruptions, assure compliance, and secure their infrastructure. As a result, they can implement the rules and strategies that are most aligned with their business goals.

Bit9 Parity

Bit9 is the first company to offer a complete solution that provides IT professionals with total visibility, knowledge, and control over new, unknown software in enterprise endpoint environments.

Bit9 Parity™ is an endpoint management and security system that provides network-wide discovery, tracking, and control of application software. Based on Bit9's breakthrough Automatic Graylist™ technology, IT administrators using Parity can focus on new and unknown software being introduced into the environment, no matter how it arrives. As a result, what was previously an uncontrollable class of software can be brought under simple, reliable, and efficient management.

Bit9 ParityCenter™ is a web-based service that integrates with Parity software to provide knowledge and context for identifying new, unknown applications that arrive on corporate desktops. ParityCenter gives you access to the most comprehensive knowledgebase of commercial application software and published executables available today. Simply click on a file from within the Parity console to discover who manufactured it, how it was distributed, what names it goes by, and more. With 4 terabytes of information collected directly from authoritative government and commercial sources, ParityCenter has indexed more than 250 million files and is still growing. No other source is as rich or as accurate for researching executable files.

Gaining Visibility, Knowledge, and Control with Bit9 Parity

Example 1: Call Center Disruption

Situation	<ul style="list-style-type: none"> A Trojan virus is making its way through the email system disguised as an email attachment. The Director of Call Center Operations is worried about his agents opening the email and corrupting their machines, as system downtime directly impacts revenue. Fortunately, Bit9 Parity is running across the entire call center environment preventing agents from running any unknown executable.
Visibility	<ul style="list-style-type: none"> Parity identifies the machines where the Trojan is located, and even who tried to run it.
Knowledge	<ul style="list-style-type: none"> Other users have reported in ParityCenter that this file is suspected to be malicious. The hash-based lookup confirms it has never been released as part of a legitimate commercial application.
Control	<ul style="list-style-type: none"> Parity has blocked this unknown piece of software from running, and IT has placed it on the permanent ban list so it will never be allowed to run.
Result	<ul style="list-style-type: none"> Without any prior intervention from IT, this Trojan was incapable of doing any damage to call center operations, even if users had attempted to launch it.

Gaining Visibility, Knowledge, and Control with Bit9 Parity

Example 2: Enforcing Usage Policies

Situation	<ul style="list-style-type: none"> One Monday afternoon, IT receives an alert that a new piece of software has suddenly appeared on nearly 10% of managed workstations—an inherently suspicious event. Fortunately, Bit9 Parity has been deployed across the environment.
Visibility	<ul style="list-style-type: none"> IT pulls up a real-time report in Parity to see where and when these new files appeared.
Knowledge	<ul style="list-style-type: none"> IT uses ParityCenter's hash-based search to identify the file as a component of a new media player that had just been released. This specific media player is known to conflict with business applications and as a result, typically generates a high number of support calls.
Control	<ul style="list-style-type: none"> With the click of a button, IT bans the media player from executing throughout the environment.
Result	<ul style="list-style-type: none"> The unapproved media player is banned from running, and the corporate usage policy is enforced. IT eliminates what could have been an expensive and nagging support problem.

Conclusion

IT organizations are demanding the next generation of endpoint management and security software so they can regain control over their complex and distributed endpoint environments. Built upon a strong set of founding principles—visibility, knowledge, and control—these tools are revolutionizing a process that was quickly becoming outdated. Bit9 is at the forefront of this transformation, enabling IT to implement strategies that will succeed against tomorrow's challenges.

About Bit9, Inc.

Bit9 is the first company to solve the problem of unwanted software at the endpoint. As the only solution to detect and stop spyware, malware, and non-business applications, Bit9 gives IT professionals unprecedented, network-wide visibility and control in real time. Bit9 provides the earliest and best possible protection against known and unknown intrusions, including zero-day attacks. Founded in 2002 and headquartered in Cambridge, Massachusetts, Bit9 is a privately held company.

For more information, contact Bit9:

Ten Canal Park, Suite 201

Cambridge, MA 02141

Tel: 617.393.7400

Fax: 617.393.7499

www.bit9.com

