

# Best Practices for Secure Desktop-based Information Search in the Enterprise

*February 2006*

*X1 Technologies, Inc.*



---

## Abstract

**The purpose of this paper is to urge IT management and executives to:**

- Recognize the pervasiveness and imminent entry of desktop search technology into their environments
  - Be aware of its significant benefits as well as potential threats to information security, and
  - Take proactive steps to evaluate and deploy a centrally managed enterprise desktop search solution.
-

# Contents

<b>Introduction</b>	3
<b>Desktop Search Is Changing the Way We Work</b>	3
<b>New Risks</b>	4
<i>What's the Difference Between Office Applications and DTS?</i>	4
<i>Where's the Risk?</i>	4
<i>Threat by Design</i>	4
<i>Threat by People</i>	5
<i>Not Unique to the Private Sector</i>	6
<b>Best Practices for Managing DTS in the Enterprise</b>	7
<b>Requirements for a Secure Enterprise Desktop Search Solution</b>	8
<b>Conclusion</b>	9
<b>About X1 Technologies</b>	10



# Best Practices for Secure Desktop-based Information Search in the Enterprise

## Introduction

Why are Desktop Search (DTS) tools becoming so widespread in the workplace? Knowledge workers by the millions are downloading and installing them. The opportunity for improved productivity and reduced costs is significant and the demand for DTS—from end users as well as from organizations—will not go away anytime soon. According to IDC, the market demand for technology to search unstructured enterprise data is projected to reach \$2.3 billion by 2008.<sup>1</sup> (In fact, customers of X1 Technologies are realizing direct cost savings in the hundreds of thousands of dollars and indirectly increasing revenue through improvements in areas where retrieving information faster leads to greater profits, such as sales, customer service and research & development.)

However, with change comes risk. Industry groups and analysts agree that IT management must address the potential security exposures of unregulated search tools. Despite productivity gains and cost savings, failing to proactively establish policies and lock down a standardized, centrally managed DTS solution can cost organizations exponentially more in civil and criminal liabilities.

Companies seeking to implement an enterprise-level DTS solution should use some basic criteria to evaluate proposed products, services and vendors. By following a few basic principles and evaluating vendors carefully, companies can realize the full benefits of this new technology and enhance their information security.

## Desktop Search Is Changing the Way We Work

As many as 5-10% of some companies' workforce have downloaded DTS tools and begun using them. There is a wide variety of free tools to choose from, with similar propositions: "Use this tool to search for documents and files that you know exist on your local hard drive."

Knowledge workers, typically drowning in email, files and data, have begun to adopt these light tools because they truly enable efficient work. Unlike traditional client-server models for document and workgroup management, the DTS tool delivers fast—often instant—search results that span many file types as well as thousands of stored emails. Users get faster results and spend little or no time reworking existing information.

Many companies have begun to take notice of the productivity gains realized from the use of DTS, especially in the enterprise arena. No matter the size of the firm, companies can save millions based on the combined costs savings for each employee. In fact, IDC estimates that companies, on average, spend more than \$14,000 per employee per year on information search, and waste almost \$5,300 per employee per year on searching for information they can't find.<sup>2</sup>

These numbers are based on an average employee salary of \$60,000 per year. The potential to recover this lost productivity—perhaps 25% of a knowledge worker's week—is staggering.

Gartner concurs that DTS is inevitable, stating that, for DTS, "IT organizations should deploy and train users now—they shouldn't wait," and, "Indulging [motivated end users] when possible will save time, money and training."<sup>3</sup> In short, DTS, like email, cell phones and instant messaging, is a technology whose time has come and which must now be addressed by IT.

---

1. "Worldwide Content Management Software 2004.2008 Forecast: The Myth of Enterprise Content Management," IDC #31009, March 2004.

2. Susan Feldman et al., "The Hidden Costs of Information Work," IDC, March 2005, pp. 2-5.

3. Whit Andrews et al., "Management Update: Predicts 2006: The HPW Will Influence Users' IT Choices," Gartner, December 7, 2005, pp. 3.

## New Risks

### *What's the Difference Between Office Applications and DTS?*

Considering the amazing potential benefits of DTS, companies may dismiss employee downloads in general as harmless, as long as they don't conflict with the operation of the user's machine. However, IT management needs to take the same approach to DTS as it does to any piece of software that touches corporate information, because it accesses the same applications and data as, for example, Microsoft Office or Windows Explorer.

Why the concern? Microsoft Office is a centrally managed business-oriented tool suite that honors Windows security authentication both locally and across an enterprise, while most freely downloadable DTS tools are consumer-oriented tools intended to maximize one's visibility into their computer and into any other shared locations they have access to—without the oversight of a corporate IT department.

While a typical user on a Windows O/S can be restricted from read/write access to items on their own machine or across a network, some DTS tools—by the nature of their architecture—circumvent these restrictions. Users can access virtually anything the computer touches.

As a corollary, certain DTS tools and solutions do not empower users to see all that they are authorized to see. In the case of spider-based tools, indexing capability for the network is effectively reduced to the "lowest common denominator." In a 1,000-person organization, if 500 people are restricted from read/write access to a repository, the spider will honor the restriction and will not index that repository. 500 people who normally do have read-write access to that location get no added value from the tool. Security is intact but the company misses out on productivity gains. (With certain tools, this architecture can also create new threats from accidental or deliberate misuse, which will be discussed below.)

### *Where's the Risk?*

Regulations force organizations to control access to their information, and unpoliced applications and tools can undermine controls. The Health Insurance Portability and Accountability Act (HIPAA), additional recent legislation such as the Sarbanes-Oxley Act, the Family Educational Rights and Privacy Act (FERPA) and others, clearly state that organizations—public, private, non-profit—all have a responsibility to control their data. They must know (and be able to prove) where it is, who can access it, who has accessed it and how it is being manipulated. Executives and directors, and even managers, bear liability—criminal as well as civil—for systemic lapses in security.

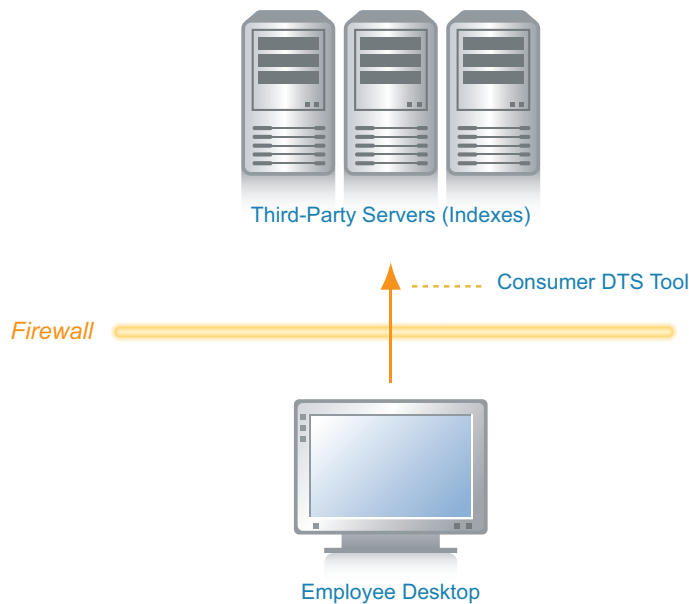
Companies have invested billions of dollars in implementing security features such as single-sign-on, firewalls, Active Directory network administration, and more, as well as correcting flaws in their security models. How could a simple, consumer-oriented tool violate what appears to be an information fortress? The two easiest methods are threats due to the fundamental design principles of a tool and threats emanating from accidental and deliberate violations of policy by end users.

### *Threat by Design*

First, certain DTS tools, by design, enable data transfer outside the corporate firewall. This raises concerns for enterprise security because it places information beyond the reach of its corporate custodian. Analysts and industry groups strongly recommend businesses do not adopt DTS tools that move information outside the enterprise and/or strip it of permissions.

Not only can some DTS tools remotely store computer contents, but they also can enable users to index and search multiple machines remotely. People who work in multiple locations with multiple computers perceive this breadth of search as very advantageous.

Major analysts question the appropriateness of granting a private company access to the contents of one's computers because this may result in significant liabilities for entities that manage sensitive data, or in essence, for practically all businesses.



**Figure 1:** Enterprise data “escapes” through the corporate firewall onto a third-party server for indexing.

Regarding the architecture of Google’s DTS tool, Google Desktop 3.0, Gartner states:

Gartner believes that [enterprise information’s] mere transport outside the enterprise will represent an unacceptable security risk to many enterprises. In addition, workers will not always reliably identify documents that must remain outside the category of shared items. Such decisions may be based on factors such as regulatory or security restrictions.<sup>4</sup>

Google itself admits risk to businesses using its latest release. In a statement to ZDNet UK, Google’s Andy Ku said, “We recognize that this is a big issue for enterprise. Yes, it’s a risk, and we understand that businesses may be concerned.”<sup>5</sup>

Considering the penalties associated with regulatory violations, exposure to lawsuits and the potential loss of customer trust and loyalty, the idea of allowing a tool that stores company content outside the company quickly loses its luster. Even at the consumer level, privacy advocates express doubt about exposing one’s hard drive to a private company.<sup>6</sup>

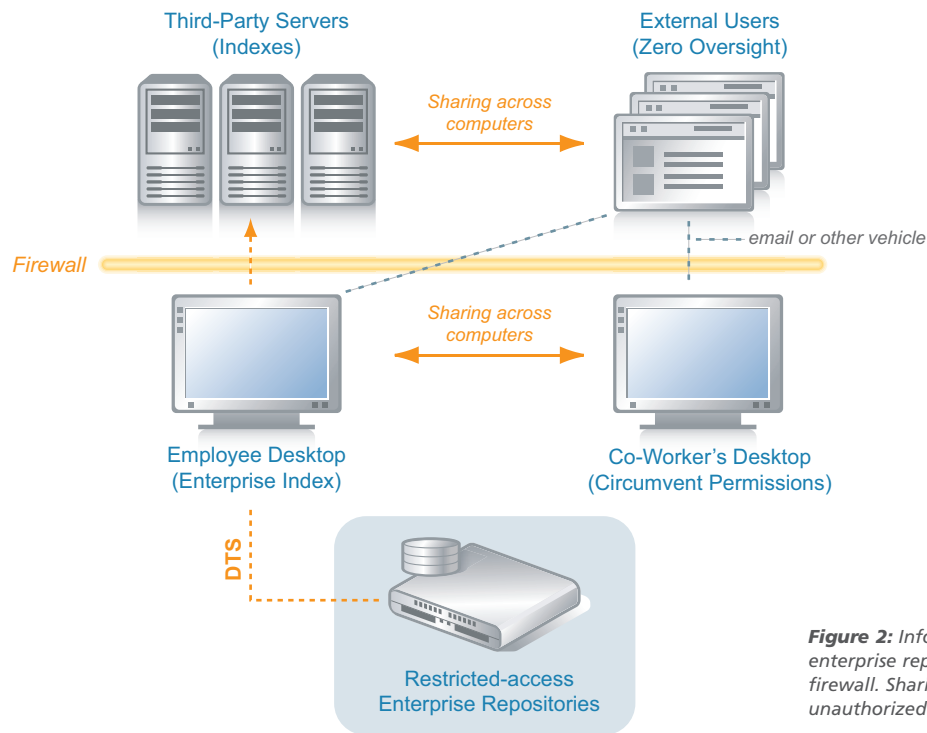
### ***Threat by People***

Information security also relies on trustworthy individuals. In practice, trustworthy people also want to be effective at their jobs. They will adopt tools that make them more effective first and worry about security later. End users do not have to have malicious intent, but simply in the course of doing their jobs, they will exercise initiative and find creative ways to simplify tasks.

4. Whit Andrews, “Manage Google’s Desktop Search Now or Lock It Out,” Gartner, February 16, 2006, pp. 2.

5. Tom Espiner, “Google admits Desktop security risk”, CNET News.com, published on ZDNet, February 20, 2006.

6. “Google Copies Your Hard Drive—Government Smiles in Anticipation”, Electronic Frontier Foundation, February 9, 2006.



**Figure 2:** Information formerly secure in enterprise repositories makes it outside the firewall. Sharing across computers enables unauthorized access and external access.

In one example, as shown in Figure 2, information that was once secure, through a “Sharing Across Computers” feature, may become exposed to unauthorized users. In the quest to work more effectively, one motivated manager decides to work from home. He uses a “Sharing Across Computers” feature to index the content on his work desktop so that he can search it from his home computer. This moves enterprise data outside the firewall.

Another motivated manager wants her direct reports to be able to access files for collaboration purposes. Her department uses a spider-based DTS tool that doesn’t give her team sufficient search functionality because it is limited to the “lowest common denominator” of security permissions. To give her team further access, she generates her own index—everything she as a manager can see—and houses that index on her own work computer, effectively creating a “user-controlled node.” Subordinates use a “Sharing Across Computers” feature to search through the same index, circumventing ACLs and violating confidentiality.

These end users, in turn, also choose to share files across computers, or attach them to emails, and the same result follows. Competitive intelligence, medical records, sensitive financial data, HR records and whatever else was once secure and controlled, escape their corporate custodians.

In just a few simple steps by well-intentioned employees, information indexed and/or stored by a poorly managed DTS tool can be exposed to the world and stripped of all permissions, opening the firm and its management to major liability. This scenario does not account for malicious use, which could far exceed the impact of “accidental” violations.

### **Not Unique to the Private Sector**

Poorly managed DTS poses risks within the public sector as well as the private. Analysts point out the extreme risk of exposure of confidential investigations, as well as the fact that some solutions cache everything the user sees, not just search results but also Web pages. This could give a hacker broad access to all systems, not just files.<sup>7</sup>

7. Aliya Sternstein, “Is desktop search secure?” Federal Computer Week, March 30, 2005. <http://www.fcw.com/article88441-03-30-05-Web>

According to Whit Andrews, research director at Gartner, once “proglers” break into a law enforcement computer system, poorly managed DTS tools could make it easier for them to reveal private information to “third parties who are not aligned with government interests.”<sup>8</sup> Andrews strongly recommends that Google’s “Search Across Computers” feature be turned off altogether. This assumes that organizations already have high confidence that they can “lock down” content from moving onto Google servers.<sup>9</sup>

## Best Practices for Managing DTS in the Enterprise

Like the disruptive technologies of email and instant messaging, DTS can add tremendous value to the knowledge worker’s day and, irrespective of regulations and policy enforcement, will inevitably creep into the environment.

Long before DTS has reached even a majority of personnel, firms will have to manage this new technology. Companies who do not proactively implement an effective DTS solution are missing out on significant productivity gains and cost savings and at the same time are relinquishing too much control to motivated employees.

There are two key principles to keep in mind when addressing DTS in the enterprise.

### **1. Know what is entering your environment (in terms of DTS installations) and know what is leaving your environment.**

Many freely available DTS tools are wonderful for consumers and small office/home office (SoHo) users. However, organizations that deal in sensitive information and are subject to regulation must be more cautious about what employees are doing with their PCs and how broadly their DTS tool can index content.

*Recommendation: Establish and communicate a policy to standardize on a DTS tool, and audit permissions to make certain that personnel have appropriate access.*

Standardize on a DTS tool that aligns with your firm’s desired degree of control over its information. In other words, if a company doesn’t want all of its data to be indexed outside the firewall by a third party, then it should expressly forbid DTS tools that use this method in any way.

### **2. Free software does not equal freedom from responsibility.**

IT management and other responsible stakeholders must not dismiss the impact of poorly managed DTS tools. IT management is 100% accountable for administration and enforcement of DTS policy. If unauthorized employees can see restricted information, or if information “escapes” from confidential folders, this can result in significant legal liability, regulatory penalties and even jail time.

*Recommendation: IT management should centrally deploy DTS to personnel and lock down desktops using an administrator’s interface.*

Organizations need to anticipate the popularity and proliferation of DTS and ensure that anything being added to desktops or the network will map to existing security systems. Gartner recently echoed this recommendation in its brief on managing Google Desktop.<sup>10</sup>

---

8. Ibid.

9. Andrews, “Manage Google’s Desktop Search Now or Lock It Out,” Gartner, pp. 2

10. Ibid.

## Requirements for a Secure Enterprise Desktop Search Solution

As stated above, DTS is on pace to rapidly penetrate the entire business computing market. This technology is proliferating so quickly, and is so easy for employees to get, that organizations have little time to waste. Gartner's Andrews says:

"Enterprises seeking a desktop search application that have not yet selected a vendor should select one as soon as possible and move employees to the supported vendor's application."<sup>11</sup>

When a firm practices the principles described above, there are several criteria for choosing an effective and secure client-server enterprise DTS solution. The following are basic objective criteria for any organization of any size.

### 1. **Standard, central deployment and control**

An effective enterprise DTS solution should have a central control interface for administration. The administrator should be able to configure the client, then deploy it to the personnel from a central location.

Ideally, users could also have access to a browser-based client so that firms have the option to eliminate deployment to individual workstations.

Administrators also need to be able to configure and customize clients after deployment. A working solution will allow changes to the interface and re-deployment of those changes.

### 2. **Integration with existing security—mapping to Active Directory ACLs**

Enterprise DTS must conform to an organization's security model. A secure solution should integrate with and automatically respect the role-based permissions and authentication process of the firm's network.

For a Windows network, enterprise DTS should map to Active Directory Access Control Lists and, when implemented, Group Policy. Failing to map to existing permissions, as in the case of spider-based solutions, will dilute or disintegrate the value-add of enterprise search and will encourage users to create their own search nodes and "get around" enterprise security.

This necessarily rules out any solution that has the potential to circumvent security or send sensitive data outside of an organization's controlled environment.

### 3. **Centralized indexing**

One of the threats discussed above derives from end users indexing sensitive enterprise data on local machines and sharing data across machines, be they company or personal computers.

Not only does local indexing of network data pose a security threat, it also consumes network bandwidth and even local processing power. An effective enterprise DTS solution will index network content and contain it where it belongs—on the network—while also federating search results with information stored locally.

This method will not only produce lower network overhead, but also deliver better search performance, reduce the threat of end users accidentally or deliberately sharing sensitive company data and enable remote users on password-enabled browser clients to search enterprise content in a unified, efficient fashion.

### 4. **Alignment of vendor's goals with your business goals**

While it may require virtually zero administration, an effective, secure enterprise DTS solution is an ongoing consideration, not just a static solution at a point in time. Your organization's needs will change over time and your vendor must evolve with you.

---

11. Ibid.

Ask these questions when evaluating your company's compatibility with an enterprise DTS vendor:

**A. What percentage of the vendor's revenue mix is services and/or hardware?**

- i. How much of the proposed solution is software (packaged code you can install and manage yourself), services (consultants from the vendor or one of their partners who must spend days or weeks configuring the software to your unique environment), and infrastructure (additional devices that you need to lease or buy and maintain)?
- ii. What is your relative comfort level with inviting consultants into your IT environment, now and in the future?

**B. What percentage of the vendor's revenue comes from activities providing effective, secure enterprise search, versus other revenue streams such as "push marketing" and targeted advertising?**

- i. Is their revenue model compatible with your information management policies and your comfort level?
- ii. Is the vendor primarily oriented toward enterprise business—geared toward making businesses more efficient—or toward consumers—geared toward extraction of market intelligence?

**C. Does the vendor's product roadmap align with your organization's IT roadmap and existing investments?**

- i. What are their plans to release future products to enhance what they have now and supplement their offering with new integrations?
- ii. What is their track record for delivering core products and enabling features to the broader market?
- iii. How much will you have to invest in additional infrastructure?

The above criteria are not exhaustive. In addition to security factors, organizations will also want to consider the power of the interface, measurable productivity gains, technical support and scalability and the extensibility of the solution, to name just a few factors.

## Conclusion

Desktop search is both inevitable and invaluable. Savvy businesses should be aware of the significant productivity gains and cost savings of a centrally managed desktop search solution. IT and senior management must also take heed that free DTS tools are being installed across the enterprise, which could open the door to liabilities and lost profits. By practicing two very basic principles, companies can take advantage of this technology and protect themselves from unnecessary risk.

- Know what is being brought into your network and what data is leaving your network
- Free software does not equal freedom from responsibility

With a proactive plan for evaluation, deployment and management of a search tool, organizations can enjoy the productivity benefits of a centrally managed enterprise desktop search solution.

## About X1 Technologies

X1 Technologies, Inc., a recognized leader in desktop search solutions, was founded in 2003 to help business users easily access and act upon information that resides anywhere on a desktop or the corporate enterprise. Companies of all sizes use X1 Technologies' solutions for their enterprise desktop search initiatives. X1 Technologies was an early leader in the desktop search space with the launch of their flagship product, X1 Desktop Search, which garnered industry awards including the "Best of 2004" and "Technical Excellence" from PC Magazine. X1 Technologies has partnered with leading companies including IBM, Yahoo! and EarthLink to power their desktop search initiatives. Headquartered in Pasadena, California, X1 Technologies is an operating company of Idealab, and is backed by U.S. Venture Partners.

For more information, visit [www.x1.com](http://www.x1.com) or call 626-229-3050.



### The X1 Platform

Employees spend as much as 25% of their work week searching, and often failing to find, critical data across the enterprise.

- The X1 Platform puts the full power of unified, actionable search into the hands of your users, enhances your information security and integrates with your critical business systems.
- X1 combines the most comprehensive search and preview abilities on the market, as-fast-as-you-type results, easy configuration and seamless integration. Organizations of all sizes, across all industries, have demonstrated significant productivity gains and reduced risk through X1's unified, actionable search.

### X1 Works Like You Do, Not the Other Way Around

The X1 desktop search model recognizes the central truth that the traditional KM and enterprise search solution does not: people work in different ways, with various organization skills. They generally seek the shortest way between Point A and Point B irrespective of the "approved" path, and all knowledge workers have too much information and not enough time to find it and make sense out of it.

### The Complete X1 Platform Consists of:

- The award-winning X1 Client—bringing desktop and enterprise search together
- The high-performance X1 Enterprise Server—the engine of the X1 enterprise solution
- X1 Content Connectors—integrating search into your critical enterprise applications
- X1 Client and Server SDKs—to tailor the X1 experience to your end users and your unique systems