White Paper

2001 — The Quest for Understanding Security Management

Group: Product Marketing
Revision: 1.6

BINDVIEW™
Integrity. IT Matters.™

BindView Corporation, 5151 San Felipe, Suite 2100, Houston, Texas 77056 USA ▪ Phone: 800-749-8439, 713-561-4000 ▪ Fax: 713-561-1000 ▪ World Wide Web: http://www.bindview.com ▪ Email: info@bindview.com ▪ If calling from outside North America, please call: +1-713-561-4000 ▪

Table of Contents

It Is All C-O-N-N-E-C-T-E-D

Beginning a white paper about understanding security management with a children's song may seem out of place, but this lyric goes a long way toward helping readers gain a clear understanding of the subject. Remember the song?

The head bone connected to the neck bone
The neck bone connected to the back bone
The back bone connected to the thigh bone...

The connected world is here. Everything is tied together. And like the human body, most everything in the business world is not only connected, one system to another, but also interdependent. This has brought new levels of responsibility to corporate IT departments, as they work to ensure that business-critical computing systems stay connected and that all the mutually dependent relationships between platforms, directories, networks, and applications function without any impediments to security, reliability, integrity or consistency.

The concerns that used to keep system administrators and IT managers awake at night now keep line-of-business managers, corporate executives, and board members awake at night. The often-spoken wish of IT personnel — that executives should "feel their pain" — has been granted. And as the old saying goes: "Be careful what you wish for because you might just get it."

Strong Concerns About Information Management

This is a major reason that IT departments now have the visibility they do — IT is key to business performance. Everyone inside the business, as well as customers, partners and suppliers, are depending on IT to provide a trouble-free computing experience that satisfies each of their very different needs — and these needs almost always involve some type of information transfer or access. The wants of the individual, though, must be balanced against the larger desires of the business as a whole, thus the need of a rigorous business process —a process where people follow policies.

Since information is the life-blood of business, it has become more valuable than an organization's physical possessions. Information has become a new currency and just like money, the people responsible for its use must be prudent in the way they manage this most valuable asset . They also have to keep it safe and secure because there is a wide range of people who may not treat this corporate data in a way that benefits the larger needs of the business.

A very important aspect of information management is determining who has access to the different kinds of information in an organization and how those permissions are kept up to date. As external and internal users achieve different levels of status they gain or lose access to certain information stores and lines of communication (e.g., an e-mail distribution list). A business with 10,000 internal users, hundreds of business partners, and hundreds-of-thousands of customers has a big job on their hands managing this information flow. This has become a growing, significant area of concern for corporations.

BindView RMS™ — bv-Control™ and bv-Admin™ — can completely automate this entire oversight and updating process.

---

[1] *This is easily demonstrated in the valuation of companies that trade information but have few hard assets. Many enjoy superior valuations over companies with a large base of tangible assets (e.g., heavy industry, consumer goods, retailing), even when their earnings trail behind those of the asset-rich companies.*

Business Issues — Time is Money

For any large enterprise to thrive in today's competitive environment, there has to be more automation and flexibility in how the IT department responds to challenges. One reason for this is the accelerating shortage of qualified, available IT personnel. Increasing dependence on IT resources means an increasing demand for IT workers, but continuing to add people becomes harder to justify (and afford). Effective ways to extend IT resources and automate large portions of the enterprise infrastructure are needed.

An additional factor adding to the strain on IT resources is that today everyone is connected to the system. This means more users and higher system demands. As many businesses are finding, this is causing a rising tide of calls into the corporate Help Desk. Simple problems, such as not being able to print, not being able to logon to the network, or forgetting a password, have strained IT resources to the breaking point. In a ripple effect, the very people who are demanding that the Help Desk solve their problems suffer a corresponding lack of productivity in these overload conditions.

Another drain on business productivity is the routine, repetitive tasks that the IT department is required to perform. Updating basic user or customer information can mean accessing 10 different databases. It is understandable why so much data that should be identical from one place to another, is not.

These issues, and many more like them, ultimately affect business in a very fundamental way. Throwing more resources at problems like these may not be the answer. The solution is really about articulating a process and establishing a culture of discipline that will ultimately have a positive effect on business performance.

Forget the Headlines — Security Begins at Home

September 14, 1998 — *The New York Times* is hacked and has to take its site down.

October 27, 2000 — *Microsoft Hacked! Code Stolen?* shouts the headline of the interactive edition of the Wall Street Journal.

December 22, 2000 — Egghead.com's stock price falls 16% after alerting credit card companies and 3.5 million customers that their financial information may have been accessed.

These are just a few of the headlines that have fanned the flames of fear of a "hack attack" — a very real possibility and one every company should take seriously. Beyond these external threats are the threats that don't make the headlines. Threats from within are where companies are most vulnerable.

A *New York Times* article about threats from within companies stated, "More than 87% of the corporate, financial, government, and university information security managers polled said disgruntled employees were the most likely cause of data security incidents." A computer security specialist at PricewaterhouseCoopers agreed, saying, "Break-ins by outsiders are bad from a PR standpoint . . . but in terms of damage and dollars, it's the insiders that pose the biggest threat."

NOTE: In the box to the right, the term "previous assessments" does not connect. The statement, now isolated in the "box," cannot point to something previously stated. It stands alone—so can "previous assessments" be explained? Maybe "…respondents agreed that insiders pose the biggest threats."

Survey Says...

The "2000 Information Security Survey" compiled by *Information Security* magazine showed that the 1,897 respondents agreed that the threat to security is mainly from within. Startling, though, was the fact that insider security breaches almost doubled in comparison to the 1999 survey. Of the respondents, 58% said that insiders had abused computer access controls and 41% said that insiders had electronically destroyed or distributed confidential company information.

In a very high profile case of an inside security breach, an angry worker at Omega Engineering planted a "bomb" on his company's computing system when he learned he was going to be fired. The bomb erased all of the company's contracts, as well as the proprietary software used by the company's manufacturing tools. Omega's estimated loss was $12 million *plus* its competitive position in the marketplace.

From these reports, it is easy to see why the need for security integrity across the corporation is greater than ever. Businesses need to be able to not only locate security problems but take corrective actions as well. This capability should be tied into a systematic process that simplifies and automates system administration, while simultaneously leveraging a company's infrastructure investments.

The Three A's — Assessment, Auditing, Administration

IT administrators face a conundrum. On one hand, they are responsible for controlling and securing the IT environment. On the other hand, they need to reduce the amount of time they spend on the mundane, repetitive "housekeeping" chores they must perform to achieve that security. This is the "IT challenge." It is a challenge that BindView bv-Control software and an understanding of the three A's can help IT personnel meet.

From an IT standpoint, implementing the three A's should not interfere with the day-to-day performance of a company's computing infrastructure. From a business standpoint, it should not cripple the productivity of the people depending on the system. And the process should be ongoing so that the evolving needs of the enterprise are met.

A powerful benefit of the BindView solution is that it provides administrators a methodology to assess, audit, and administer their environment as a comprehensive solution for security management. This is vital in a world where business runs 24x7. Today's IT department cannot afford to divert its resources from critical business processes to perform an assessment or analysis of who has access to what or perform a port scan across the organization's Internet devices. bv-Control allows the system to run normally while these critical tasks are executed.

The three A's should be tied to policy-based management. This brings consistency to the computing enterprise, boosts reliability, and reduces complexity.

Assessment — How do I know what I have?

Assessment describes a policy of addressing security vulnerabilities: the leaks and breaches that occur inside an organization. Security vulnerabilities may be the result of a merger where people are laid off and possibly disgruntled. A business may be growing at a phenomenal rate and need to hire people as contractors. In either case, non-core employees have access to critical information and could present a security problem.

During the assessment process, a continuous analysis of internal and external threats is performed. A large part of assessment relates to policy compliance — determining who has access to the system, what level of permissions they've been granted, and who, if anyone, is violating the corporate policies that have been established within the environment.

Auditing — How do I know its impact on the business?

If assessment describes security vulnerabilities, audit describes the performance of online or ongoing activity monitoring as well as offline audit trail analysis. Policy validation is a process of ensuring that the right policies are established and applied across an organization. An IT environment is audited to ensure compliance with these policies.

---

[2] *Another challenge is battling the "myth" that deploying a firewall or VPN ends all security issues. This is hardly true. In fact, the more security pieces put in place the more complexities in the system. Now there are many more points of entry into the network. Business managers and IT directors need to understand that regardless of the security infrastructure that has been or will be deployed, it needs to be managed too. BindView is the only company delivering this type of management capability.*

Administration — How do I fix it?

Gartner Group states that 80% of all IT issues stem from people and process issues and have nothing to do with technology. To minimize the downtime attributable to people and processes, appropriate administration processes need to be enforced to ensure that the right people do the right task at the right time in the right order. So administration is really about policy definition and enforcement.

Configure, Evaluate, Administer

Another example of the use of the three A's is in configuration management and policy application. Before updating its systems, the IT department has to know that the update they are applying is compatible with the hardware and software in its environment. If it isn't, and there is a version conflict or a .dll conflict (a.k.a. ".dll hell") or a hardware conflict, the administrator needs to know it prior to making the update, since this would put the system at risk. In general, introduction of any third-party software can create security risks.

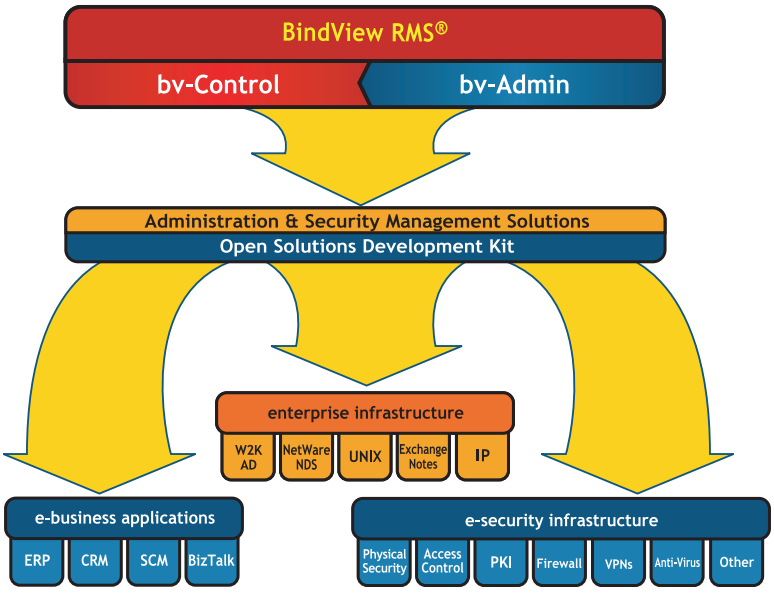
Once the administrator understands what the environment configuration is, auditing and assessment can be used to understand what the impact of the update will be. With proper administration, policies can be defined and enforced.

Snapshot Summary

Assessment is about policy compliance. Auditing is about policy validation. Administration is about policy enforcement.

Policy enforcement relates primarily to business issues. For example, a company establishes a policy that all e-mail older than 90 days will be deleted. Whether the business is compliant is an assessment issue. Whether people under the authority of the policy are actually deleting their e-mail is a validation issue.

The value of the bv-Control solution lies in its ability to perform all three A's — assess, audit, and administer. Existing products are only capable of performing one or two of these processes but not all three. Separate tools are necessary, and even if these tools work well, they cannot provide a consolidated view of the impact an action will have on the IT environment and the business it serves.



The BindView RMS solution spans the enterprise, delivering unparalleled security management from one integrated, easy-to-install and easy-to-use solution.

No Security, No Business

Simply put, if a business does not operate in a secure manner, other companies will not do business with it. Company information is a valuable commodity and, as a result, any information transaction between business partners must be done in a secure environment. If not, valuable information could be pirated and given or sold

to a competitor. The idea of "no security, no business" is real and hammers home the necessity and urgency to understand and undertake proactive security management and ensure environmental integrity.

The BindView bv-Control solution proves its worth in helping companies tackle security issues. The first step in pinpointing security problems or threats is usually through the creation of simple queries. For example, show all users violating the corporate e-mail retention policy, or show all users who have inappropriate access to financial information. Next, administrators enforce the right corporate policy and produce a report showing that the systems or the users are in compliance with the corporate policy — all with one click of the mouse.

Ensuring enterprise integrity is not only a key to survival but also a way to thrive in the new economy. The way this is done is to go beyond query-based analysis with real-time policy enforcement on changes that are happening in the system. For example, a business has 159 Microsoft® Exchange servers. An assessment determines that there is a vulnerability that needs to be fixed. An exception report of all the Exchange systems is run and it is determined that 99 Exchange servers are affected. With one click a change is applied to just the 99 Exchange servers that needed it.

Getting Granular — Additional Business Benefits

As mentioned earlier, security management goes beyond the IT department. It is a board-level issue. If the company is not secure, if it cannot scale its business, if it cannot grow its business because IT has become a disabling entity within the organization, then the business is in trouble.

Security Analysis

With its scalable, distributed analysis and query architecture, bv-Control software provides the in-depth security analysis, trending and baselining capabilities a business needs for success. It spans platforms, networks, directories, and applications across the enterprise and is capable of providing answers to questions such as:

- Why are there so many logon attempts from South Africa?
- Why is the event log filling up in Japan?
- Why are there so many changes to the servers or additions to administrative groups in Boston?

Additionally, bv-Control consolidates all of this information and presents it in a single console.

True Ease of Use and Deployment — Delivering on the Promise

The terms "ease of use" and "ease of deployment" often cause seasoned IT professionals to raise a skeptical eyebrow. Rest assured, bv-Control delivers on the promise. Use of bv-Control for security management leverages an organization's existing infrastructure with no intrusive impact on the environment.

- Servers are not brought down for analysis.
- Business processes are not interrupted.
- Users experience no degradation of service.

The entire suite can be installed, deployed and used to conduct global enterprise security management from one central location within one day. This single-point rollout reduces deployment time from months to hours. When system security is at stake, the sooner you know your vulnerabilities and take corrective actions, the better.

Comprehensive Reporting

The reports available in a security management solution are important to any administrator. bv-Control software comes with over 800 out-of-the-box reports with over 1,200 fields of information available for reporting. This information gives administrators a view of their environment they may have never had before. Administrators can use these reports, a function of assessment and auditing, to perform automated actions for policy enforcement.

Productivity Boost

Administrators benefit from using bv-Control software with enhanced productivity through the automation of routine tasks. Additionally, the solution helps to ensure policy compliance from users who access the computing infrastructure.

Consistency and Reliability

Since policies can be enforced, consistency increases across the enterprise. With a consistent system in place, reliability increases.

Efficient Resource Management

Effective system utilization is another benefit of bv-Control. When system administrators know what is in their environment and have a clear understanding of the security impact, they can establish policies to maintain control over that environment and manage their resources more efficiently. For example, when an e-mail storage policy is established, resource hogs cannot store hundreds of megs of MP3 files, .jpg files and video clips on the system.

Planning for Disaster

Disaster recovery planning is a troublesome yet necessary activity for IT administrators. If disaster ever strikes, the lack of such a plan becomes a very critical issue. With bv-Control software, administrators enjoy complete and up-to-date network documentation at their fingertips. In the event of system failure, administrators have full documentation about their prior environment. The system can be brought back online quickly and with the full assurance that the underlying structure will be intact and responsive.

In-Depth Analysis — Additional Productivity Gains

bv-Control software offers an in-depth analysis of situations that other solutions cannot offer. For example, administrators can run a query asking, “How did user X gain access to financial files F and Q?” Previously there was no speedy way to answer that question. Perhaps user X entered through a group the administrator did not know existed. Maybe user X was embedded in five different groups and gained access through inheritance.

There is certainly no immediate way an administrator can work through the system manually and come up with the answers. bv-Control though, can put an immense amount of productivity power in the hands of the administrator and swiftly identify the underlying reasons for such a security breach.

Action Based on Knowledge

When an administrator can see the pathway users take to gain access to restricted areas, whether intended or unintended, they gain knowledge. This knowledge is powerful because of the assurance of system integrity it

provides. The sweet reward is that the administrator can now take quick action. A policy is established to deny the intruder or everyone in the intruder's group access to sensitive information. With one mouse click the administrator can clean up errant permissions and keep the environment policy-compliant.

RapidFire Updates

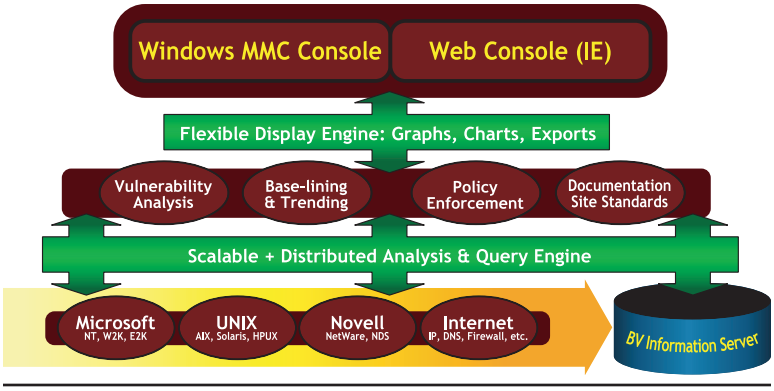
The RapidFire Updates™ and ActiveAdmin® capabilities in bv-Control regularly provide network administrators with updated security solutions as soon as new security problems are discovered. These capabilities promote continuous network integrity by allowing administrators to automatically take action to enforce new security policies.

Cross-Platform Functionality

Easing the day-to-day grind of security management, bv-Control provides true cross-platform functionality from a single console, enabling interoperability from a centralized location. This helps network administrators to focus on multiple platforms and securely integrate all network resources.

bv-Control is the only complete security and configuration management solution designed to protect complex and distributed enterprises. It provides in-depth security and administrative analysis, ensuring the integrity, security and performance of mission-critical systems enterprise-wide. Whatever the environment, BindView has an answer for protection against system vulnerabilities:

- bv-Control™ for Windows® 2000 and Windows NT®
- bv-Control for NetWare® and NDS®
- bv-Control for UNIX®
- bv-Control for Microsoft® Exchange
- bv-Control for Active Directory™
- bv-Control for Internet Security
- bv-Control for SAP® Systems
- bv-Control for OS/400
- bv-Control for Desktops



The bv-Control architecture is scalable, flexible and customizable. It is also open and based on the latest industry standard Windows and Web technologies. Users will enjoy enterprise-wide analysis in a variety of formats, easy to use "out-of-the-box" reports, historical data storage, baselining, and support for any platform with a module snap-in.

Baselining

Baselining technology helps to ensure efficient security policy management. Network administrators can take a snapshot of their network and create a baseline image of their security configurations. They can then efficiently and easily audit, compare, and repair any unauthorized changes.

Network Hardening

Network hardening through a comprehensive audit boosts the level of enterprise security. bv-Control allows administrators to report on hidden or invisible objects within a directory and allows users to harden their networks by challenging password strengths.

Stay Sharp with RAZOR

RAZOR is a worldwide team of cutting-edge security researchers sponsored by BindView. They are dedicated to advancing the state of the art in securing networks and computers. RAZOR develops the art by identifying new security holes and disclosing these results publicly, so that all may benefit from the team's research (http://razor.bindview.com).

It's Up to You

It is no surprise security is a paramount issue in today's enterprise. Security threats come from everywhere, but more than ever they are coming from a totally innocent person, usually an employee, who starts a process that can devastate an enterprise's computing infrastructure.

How can an IT staff cope with security threats that are frequent and pervasive? The answer to that question used to involve multiple point products stitched together in a loose security framework.

With the BindView RMS solution led by bv-Control, the enterprise gains a level of security and security management unavailable from any other solution.

It is imperative that a systematic process of continuous assessment, auditing, and administration be used to ensure a business's integrity. A successful business must provide the highest level of security management possible to its computing systems. BindView solutions can help businesses find and close security holes for nonstop protection against ongoing security threats.

Award Winning

bv-Control software received Priority One certification from the System Administration, Networking and Security (SANS) Institute (www.sans.org). Because of its ability to detect all the security vulnerabilities identified in the SANS Priority One list of security threats, bv-Control became the first commercial software product to receive the highest level certifications from the SANS Institute.