



## **Symantec LiveState™ — A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations**

Enabling Client Resilience  
by Helping to Ensure That  
Devices Are Secure, Available,  
and Compliant with Corporate  
Standards



# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## Contents

<b>Executive summary</b> .....	3
<b>Symantec’s Information Integrity initiative</b> .....	4
<b>The case for convergence</b> .....	5
<b>The infrastructure lifecycle</b> .....	7
Healthy business operations .....	7
Planned disruptive operations .....	7
Unplanned disruptive operations .....	8
The need for rapid recovery from disruption .....	9
Seamless management infrastructure .....	10
<b>Converged management architectural considerations</b> .....	11
Normal state operations .....	12
Transition to a disrupted state .....	13
Recovery from disrupted operations .....	14
<b>The Symantec LiveState architecture</b> .....	16
Systems “state management” .....	16
Single unified platform .....	17
Symantec LiveState management objects .....	19
Symantec LiveState image snapshots .....	19
Symantec LiveState installation packages .....	19

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## Contents (cont'd)

<b>Symantec LiveState family of information availability solutions</b> . . . . .	<b>20</b>
LiveState process flow . . . . .	21
Symantec LiveState Designer . . . . .	22
Symantec LiveState Delivery . . . . .	22
Symantec LiveState Patch Manager . . . . .	23
Symantec Discovery . . . . .	23
Symantec LiveState Recovery . . . . .	23
Remote control . . . . .	24
<b>Sample scenario: Preventing exploits and recovering rapidly</b> . . . . .	<b>24</b>
<b>Symantec LiveState and Symantec's enterprise management strategy</b> . . . . .	<b>25</b>

## Disclaimer

This paper is available to Symantec customers, prospective customers, and partners for the purpose of describing Symantec's strategic vision and direction in the area of systems and storage management. This document is best used by IT professionals as a guide to understanding and evaluating Symantec's overall direction for its LiveState architecture and family of solutions. While this document describes Symantec's best view of its direction, this document in no way constitutes a commitment to provide specific product or services. The enclosed architectural, product, and services plans and capabilities are subject to change. Capabilities will be provided to customers, when and if available, in a general release.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## **Executive summary**

The exponential increase in security threats—combined with the increased dependence of businesses on their IT infrastructures—puts organizations at significant risk, including financial and legal or regulatory risks as well as risks related to their reputations with both customers and investors.

In addition to costly disruptions caused by “unplanned” events such as security attacks, many organizations also face the potential of costly business disruptions due to “planned” IT initiatives such as enterprise-wide OS migrations and the deployment of new applications and platforms.

Organizations’ inability to successfully respond to these threats and business disruptions is due in large part to both the intended and unintended barriers that often exist between their systems, storage, and security management infrastructures—as well as between their IT personnel and processes. To successfully combat these challenges requires a dramatic shift in how businesses look at managing their enterprise infrastructures.

In order to respond to today’s elevated threat environment, to protect mission-critical IT infrastructure, and to rapidly recover from disrupted IT operations, organizations need to “de-silo” their storage and systems management processes and infrastructures, and further integrate them with their security management infrastructure and processes.

Symantec’s innovative LiveState family of information availability solutions helps organizations remove the technical and operational boundaries that have historically existed between storage, systems, and security management. The Symantec LiveState family is based on world-class storage and systems management technologies and a single unified platform for automated configuration management, including image/package design, asset discovery, provisioning and software delivery, patch management, and system recovery. Built upon an open and modular architecture, Symantec LiveState products can work on their own—with tools and processes you already have—or can be combined into a more comprehensive solution.

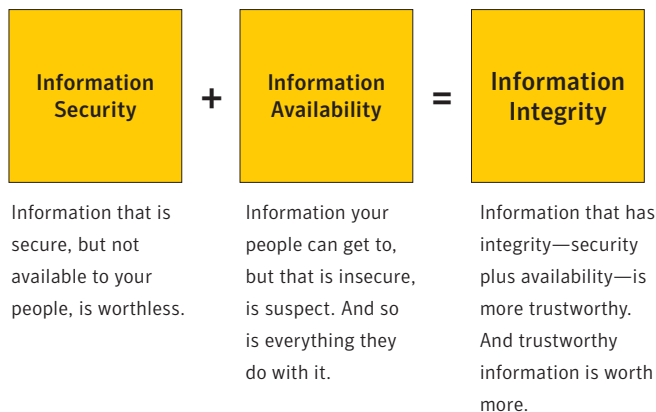
The Symantec LiveState architecture has been designed to include specific integration interfaces to Symantec’s industry-leading solutions for enterprise security management. In addition, security configuration templates are provided for deploying and configuring Symantec’s market-leading client security solutions. This innovative combination of Symantec solutions promotes a significantly more manageable, and therefore more secure, enterprise infrastructure.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

This new enterprise management approach enables businesses to establish healthy, normal operating states as well as effectively manage, minimize, and recover from disruptions to their operations. Organizations can now manage and protect the state of their business operations with greater ease, efficiency, and effectiveness, and without hiring additional IT personnel.

Symantec LiveState solutions help ensure *Client Resilience* by enabling organizations to keep their critical systems secure, available, and compliant with corporate standards—from acquisition to disposal—providing a better, smarter, and more efficient way to combat attacks, eliminate vulnerabilities, and respond to and recover from disruptive events in less time, with less effort, and with greater success.

### Symantec's Information Integrity™ initiative



**Figure 1. Information is your most valuable corporate asset. When it flows freely and securely, it can change the nature of your company.**

Information is the engine of your business, and you need to ensure that it is always secure and always available throughout your enterprise. Symantec's approach to information management is designed to simultaneously provide both world-class security and world-class systems and storage management of your networked resources. We call the result Information Integrity. It is a revolutionary approach to information management designed to help keep your business up, running, and growing, no matter what happens.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

Organizations of all sizes have found it challenging to simultaneously maximize both information security and availability due to the diverse requirements that they face each day, including fragmentation. In even mid-sized enterprises, you need to support multiple devices, operating systems, applications, and networks—all while providing everything from intrusion prevention, antispymware, policy compliance, and virus protection to patch management; OS and application rollouts; license monitoring; and systems and data recovery.

Faced with this fragmented array of needs, companies have built equally fragmented solutions with products from multiple independent vendors—creating a new set of challenges. Critical systems and security tools aren't always interoperable. IT operations and security functions often overlap or have conflicting priorities. Problems can require dozens of vendors to fix. The result is higher costs, slower response times, and an inability to achieve your business objectives.

Information Integrity can dramatically improve productivity and efficiency throughout your enterprise. It augments your current security and IT operations environments and enables them to work efficiently in concert.

When information is readily available and trustworthy, you can keep operating costs down, increase customer satisfaction, and accelerate revenue and profit growth. More importantly, your organization can more easily achieve regulatory compliance, build a more resilient IT infrastructure, enable and empower a mobile workforce, and successfully pursue new business and technology initiatives.

In short, Information Integrity can help you realize the full potential of your business, enabling you to achieve maximum value from your most important asset.

### **The case for convergence**

Companies face significant challenges managing their IT environments and ensuring the ongoing availability of business services. Disruptions to business services can be caused by a number of events, including operator error, power failures, poorly configured systems, and cyberattacks that exploit software vulnerabilities. Building an environment that is completely disruption-resistant is impossible given the complexity of the IT environment and changing threat landscape: increasing vulnerabilities, sophisticated attacks, and exploits that are published before companies can complete patch testing and deployments.

The vulnerability management window is shrinking. For the past four or five years, there has been a consistent increase in the number of new vulnerabilities reported, growing from 10 per week in 1999 to an average of 53 per week in 2004.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

According to the Symantec Internet Security Threat Report<sup>1</sup>, 80 percent of these vulnerabilities were remotely exploitable and 70 percent were easy to exploit.

Additionally, the average time between the public disclosure of a vulnerability and the release of an associated exploit is now 5.8 days. This has shrunk from the previous reporting period, when the average was 7 days. The Blaster worm leveled networks just 27 days after the vulnerability was publicly disclosed.

The exponential rise and cost of malicious computer attacks has made security a top agenda item within nearly every boardroom and IT oversight committee. While more attention is being paid to securing the enterprise, the desired results still fall short of expectations and need. Some might argue that the problem lies in the fact that while the frequency and intensity of threats has increased significantly, the staffing resources that most IT departments have to combat the rising threat has increased little in the past few years. However, throwing a significantly greater number of IT personnel into the fight is more than just costly; it's not the right answer.

To stay ahead of the security threat curve, organizations need to find a better, smarter, more efficient way to combat attacks, eliminate vulnerabilities, and respond to any event that disrupts the normal course of business. Security threats aren't the only events responsible for disrupting business operations; natural disasters, terrorist threats, power outages, hardware and software failures, and even simple human error all threaten to disrupt normal IT operations.

Most IT departments accept that routine updates to software operating environments are a necessary part of managing the enterprise even though such procedures are prime culprits for disrupting normal business activities. Also, most IT professionals agree that the protection of data assets forms the foundation for recovering from any disruptive event. But even though systems management, storage management, and security management all play significant roles in preventing and recovering from business disruptions, they are all too often treated as isolated silos of responsibility and operation. They typically operate in an autonomous manner with manually controlled policies employed at the points of integration.

If the IT environment could be locked down to a specific configuration with minimal change, then this lack of integration would not be so significant. However, expecting configurations to remain static is not realistic in today's increasingly dynamic business and IT environment. The ever-changing dynamics of today's enterprise call for a corresponding change in the scope and definition of how the IT environment is managed.

## Changing Threat Landscape

*Patch time is short:*

- W32 Blaster Worm: 26 days from vulnerability announcement to exploit. Vulnerability announced on July 16, 2003. Blaster worm discovered on August 11, 2003.
- W32 Sasser Worm: 17 days from vulnerability announcement to exploit. Vulnerability announced on April 13, 2004. Sasser discovered April 30, 2004.
- W32 Witty Worm: 30–40 hours from vulnerability announcement to exploit. Vulnerability announced on March 18, 2004. Witty worm discovered on March 19, 2004.

*Fast-moving threats:*

- Klez H: 4,516 submissions per day. Peaked in 2 weeks.
- BadTrans: 3,709 submissions per day. Peaked in 7 days.
- Bugbear B: 4,812 submissions per day. Peaked in 2 days.
- SoBig F: 1,800 submissions per day. Peaked in 1 day.

<sup>1</sup>Symantec Internet Security Threat Report VII, Trends for July 1, 2004 – December 31, 2004

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

Organizations need to eliminate the barriers between the disciplines of systems management, storage management, and security management to create an IT environment that fosters a healthy, normal state of operations. They need a way to bring these isolated silos together into one holistic infrastructure that enables organizations to stay well ahead of the security threat curve, as well as combat and recover from the onslaught of both planned and unplanned events that can potentially disrupt and harm business operations. To help organizations achieve this goal, Symantec created the LiveState family of information availability solutions.

### **The infrastructure lifecycle**

#### **Healthy business operations**

The harsh reality of today's dynamic and uncertain business world is that even when an organization is operating under normal conditions, an honest scrutiny typically reveals that the normal state of its IT environment should actually be considered an unhealthy state. Many "normal" or routine business operations—such as the deployment of new business applications or OS platforms—can be just as disruptive and costly to a business' health as malicious attacks on the infrastructure.

Whether they're malicious attacks, system failures, or normal provisioning activities, events occur during the life of an organization that disrupt business operations. It doesn't matter whether the event was planned or unexpected—every minute of disruption costs money and potentially puts the business at risk. Across the board, businesses recognize the need to minimize and eliminate their exposure to and recover quickly from these disruptions. The key to eliminating or significantly minimizing the effects of these disruptions is for organizations to take a holistic approach to systems, storage, and security management in a way that creates a normal, healthy state of business that addresses:

- Planned disruptive operations
- Unplanned disruptive operations
- Rapid recovery from disruption

#### **Planned disruptive operations**

During the normal state of IT operations, servers, desktops, laptops, and mobile devices must be constantly updated and configured to insure that the environment is available and secure. Whether it's a hardware refresh, new OS deployment, or just a service pack update—such as

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

Windows® XP SP2—the normal state of the enterprise changes on a regular basis. Although these changes in configuration can be planned, they can also be very disruptive and costly to the business.

As a case in point, the challenge of migrating and building systems at the rate of arrival of new operating systems has become so difficult that some CIOs see provisioning as a career-threatening event. The process involves determining exactly what is on every machine in the enterprise, setting the standards for a new operating environment, preparing that environment for deployment, and then finally deploying the change. The whole process takes significant manual activity and expertise. It can be so difficult that many organizations have still not migrated to Windows XP even though it provides significant reliability, security, and performance benefits to the enterprise.

Provisioning is traditionally a normal state management task but one that takes significant effort and is generally disruptive to the enterprise. Improvements in the automation of the provisioning task decrease these disruptions, while fostering a healthier normal state.

### **Unplanned disruptive operations**

Unplanned disruptions are characterized by a sudden threat to or interruption in the operational environment and an unplanned, unscheduled need to respond in order to restore normal operations.

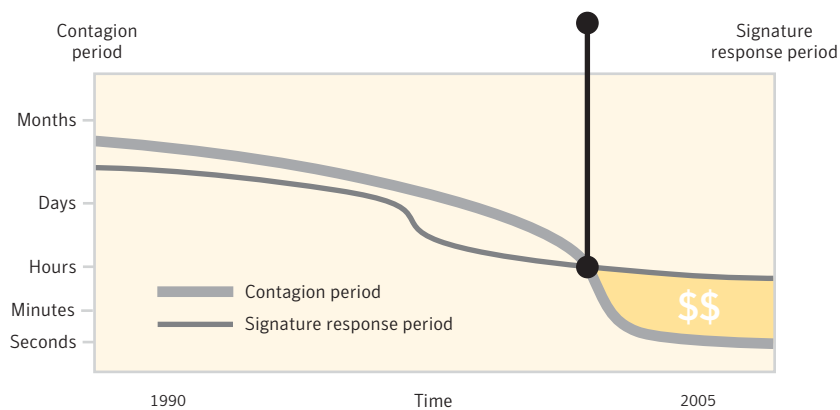
A classic example of unplanned disruptive operations is the announcement or discovery of an emerging security vulnerability, such as a worm or other blended threat. Of course, security vulnerabilities are not the only causes of unplanned disruptions; other operational disruptions can be caused by natural disasters, power outages, hardware or software failures, or even human error. But in all instances, the urgent business requirement to recover to normal operations is the same.

The IT infrastructure is constantly under attack by intrusions that exploit weaknesses in the operating software of the enterprise. Exploit prevention activities, such as patching vulnerabilities, protecting critical data, and configuring security defenses, drive dynamic change processes that can be disruptive to the normal operating state of the business and IT environment. As disruptive as these prevention activities can be, more severe damage can occur if vulnerabilities are not eliminated faster than they can be exploited. As a result, the urgent nature of these prevention processes does not allow for advanced planning.

In the area of exploit prevention activities, patch remediation is a key pain point for CIOs. The ability to completely patch and configure machines securely (e.g., close open ports, shut down unnecessary services, etc.) presents a large problem—primarily because the threat landscape evolves more quickly than the patch process can update the software.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

The ever-increasing array of viruses, worms, and blended threats are proof that exploit writers will continue to exploit security vulnerabilities. With each new vulnerability and exploit, the window of opportunity that IT departments have to react continues to decrease (see Figure 2).



**Figure 2. Stopping the bullet. The IT industry appears to have reached an inflection point, where the latest threats now spread faster than the ability to respond.**

Tightly integrating automated vulnerability scanning, patch management planning, and patch deployment with system management processes such as provisioning, helps organizations respond significantly more quickly to discovered vulnerabilities, as well as lessen, and in some cases even eliminate, the disruptions previously associated with the patch management process.

### **The need for rapid recovery from disruption**

As the rate of attacks increases, the probability of having to recover affected systems and data rises. This makes it increasingly important that even the most secure enterprise have a backup and disaster recovery plan that will enable it to recover successfully in the event of a destructive attack or other operational disruption.

Recovery from a disrupted state must be exceptionally fast since the damage from a successful exploit is proportional to the time it takes to recover. It is also important to note that the scope of the recovery architecture should typically include critical servers as well as desktops, mobile devices such as laptops, and specialized devices such as POS and ATM systems.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

The U.S. government and the European Union have also highlighted the need for reliable, automated data recovery. Executives are now personally responsible for ensuring that IT processes are properly implemented. This level of infrastructure accountability is driven by a growing number of regulations, including Sarbanes-Oxley, HIPAA, FISMA and Basel II.

All of these factors point to the need for reliable automated data backup and disaster recovery that tie to both enterprise security and systems management.

### **Seamless management infrastructure**

In today's heavily exploited environment, organizations must ensure that the security, systems, and storage management elements of their infrastructures not only perform successfully during normal conditions but also operate effectively during the disruption caused by an exploit. In other words, for enterprises to manage their normal operations in a way that minimizes disruptions as well as enables it to respond in a timely and cost-effective way to disruptions, the disciplines of security, system, and storage management must be converged into a seamless management architecture.

Combining the responsibility and operations of an enterprise's systems management, storage management, and security management into a wholly integrated IT infrastructure facilitates an enterprise's ability to establish a normal state of business operations that is truly healthy, allowing it to:

- Manage and protect the state of business operations with greater ease, efficiency, and effectiveness without increasing IT manpower
- Eliminate costly disruptions that have become common to the normal operating state of most organizations
- Stay ahead of the rising security threat curve by establishing integrated and automated processes that enable organizations to discover and remove vulnerabilities sooner, and respond more quickly to malicious attacks
- Recover from disruptions to a healthy operating state in less time, with less effort, and with greater success

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

### **Converged management architectural considerations**

Today's traditional, siloed IT operational environment makes responding to abnormal or disrupted operations challenging. Consider again the scenario of an emerging critical security threat.

With the announcement—from a security intelligence service such as Symantec DeepSight™ Alert Services or the Symantec DeepSight™ Threat Management System, or even news media outlets—of an emerging threat, the entire enterprise goes into lockdown mode as the IT departments identify the threat, determine the vulnerabilities, plan corrections, and wait for an exploit. The IT organization works long hours to secure servers, desktops, laptops, and handheld mobile devices. Often, even the most controlled processes and automated management functions succumb to manual deployment by individual experts in order to correct known problems and hunt for leaks in the infrastructure. The frequency, duration, and damage done during disruptive states give rise to new challenges faced by the IT management solutions designed to protect the business and combat harmful disruptions.

A convergence of storage and systems management, coupled with integration with security management, can significantly improve an organization's ability to respond and recover from disrupted operations caused by security threats, vulnerabilities, and other events. This improved ability to manage through disruptions is driven by the organization's enhanced ability to:

1. **Understand** its information environment and the vulnerabilities, threats, and exposures that could cause significant disruption
2. **Act** to implement proactive safeguards that successfully address threats, and identify opportunities to prevent and minimize disruptions and allow for the rapid return of business services
3. **Control** IT resources to proactively manage risk and keep the business up and running

Finally, to be successful, a converged infrastructure must allow the organization to manage both normal and disruptive states with the same management infrastructure, while supporting the substantial differences in the responsiveness and types of actions required when managing each state (e.g., proactive versus reactive patching, planned OS migration versus emergency system recovery, etc.).

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## Normal state operations

During normal state operations, the converged storage and systems management infrastructure, appropriately integrated with the security management infrastructure, supports routine IT processes such as periodically scheduled backups, monthly patching, application updates, day-to-day help desk repairs, and more.

At the same time, IT personnel must have access to information and intelligence that helps them *understand* the origin and nature of potential disruptions. For example, Symantec’s worldwide DeepSight network of security sensors provides the knowledge and understanding necessary to warn enterprises of impending disruptive states.

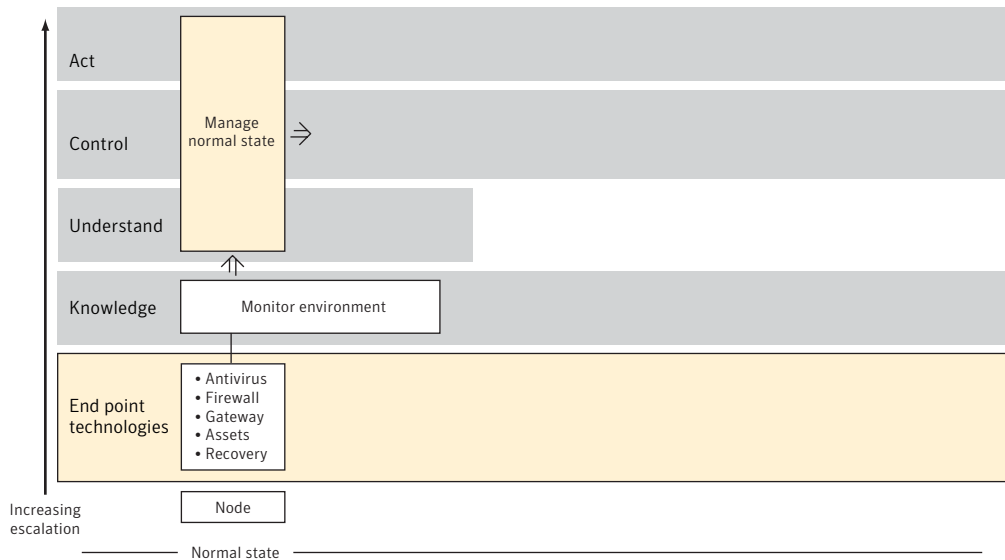


Figure 3. State view of normal operations

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## Transition to a disrupted state

Once the management state is recognized as “disrupted,” action must be taken in a controlled or managed fashion with the goal of returning the system to its normal state as soon as possible. The “Control” phase provides the rules of execution and the instructional intelligence that the infrastructure must follow during the “Act” phase.

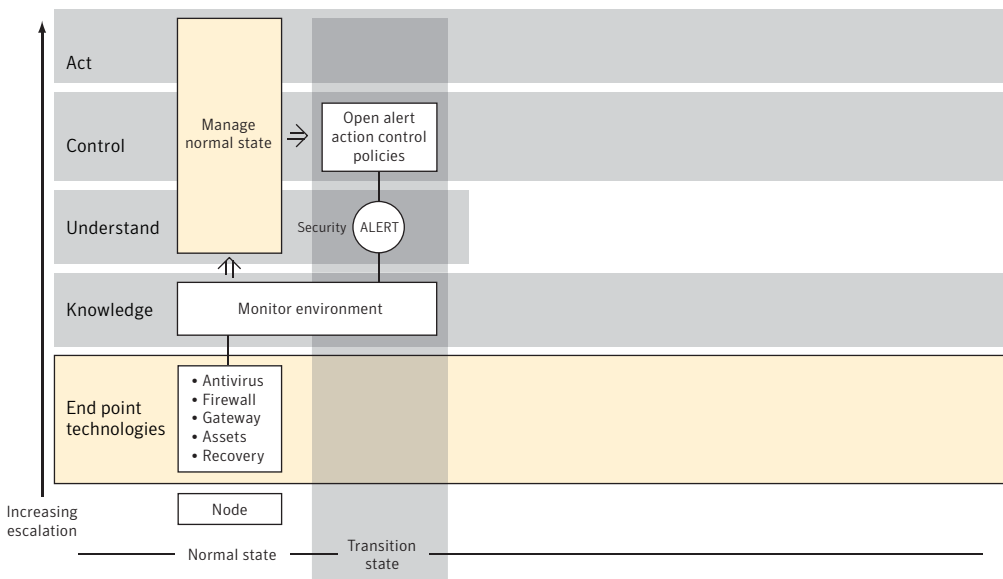


Figure 4. Incident or threat causes transition from normal to disrupted state.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## Recovery from disrupted operations

During the “Act” phase the infrastructure must respond to the disruption in a way that restores it to a normal or “safe” state. Act phase activities include many of the same tasks that are undertaken during the normal state but with an increased focus on the speed and reliability with which they occur.

As an example, security patches must be deployed quickly without disruption whereas the normal process of upgrading OS’s and applications is typically done in the course of change management. While security patches are being planned and deployed, the enterprise is vulnerable to damage. As a consequence, until patches can be successfully deployed, application activity should be monitored in real time, and any activity that appears malicious should be blocked (behavior blocking).

Alternatively, other configuration management actions can be undertaken to protect the infrastructure in the meantime. For example, in the case of an ActiveX® vulnerability, IT can push an automated configuration task to all users that simply turns off ActiveX controls on all Internet Explorer browsers.

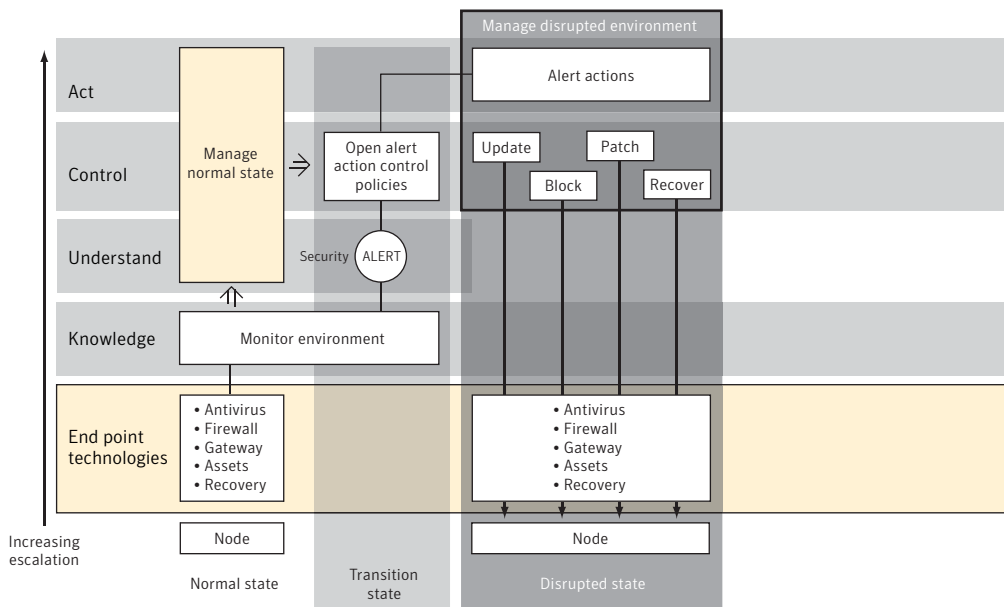


Figure 5. Action is taken to respond to the disruption in a way that restores it to a normal or “safe” state.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

Systems and data recovery is another example of similar processes executed during normal and disrupted states. Traditional backup tools are typically used to back up data during normal operations, but they seldom focus on processes that allow recovery within the window required by most disruptive events.

Since many normal and disruptive state management tasks are similar, it is logical to conclude that architecting for the disruptive state allows the realization of improvements in the responsiveness of normal state management tasks.

Additionally, it is critical to recognize the importance of managing in the normal and disrupted state with an enterprise-wide scope. During the transition phase the management software must be capable of connecting to and managing the entire computing environment. This environment includes servers, network devices, desktops, laptops, specialized systems (POS, ATM), and handheld devices in both wired and wireless environments.

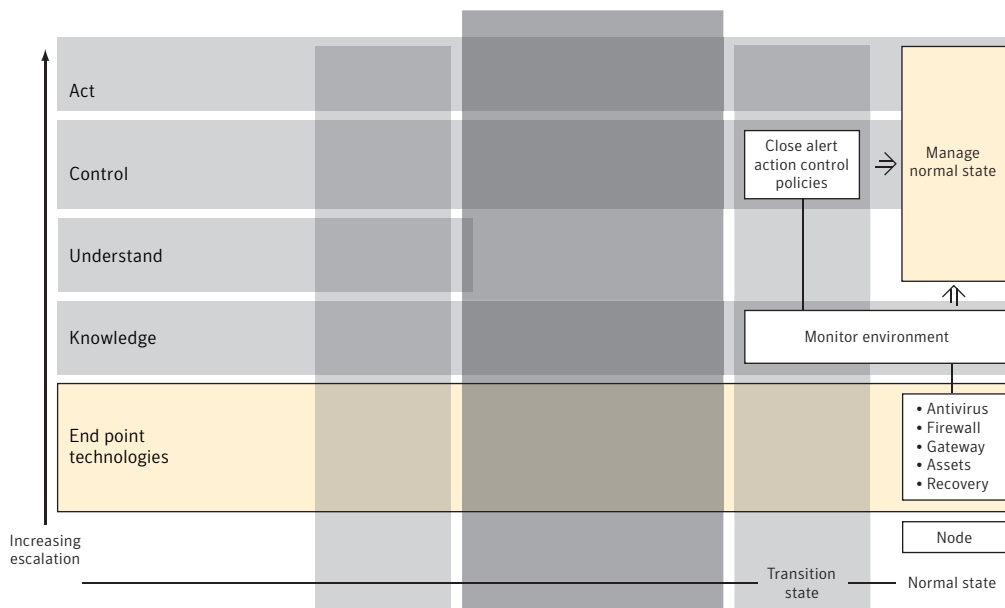


Figure 6. The infrastructure returns to its normal state and standard IT operations continue

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## The Symantec LiveState architecture

Based on world-class storage and systems management technologies and a single unified platform, the Symantec LiveState family of information availability solutions enables businesses to reduce cost and complexity while successfully managing through both normal and disrupted IT operations. This family of modular solutions offers organizations a way to help eliminate the barriers between their storage and systems management operations, as well as provide integration with security management operations. The LiveState architecture brings together these typically isolated management silos into one holistic infrastructure that lets organizations establish a healthy normal state and successfully overcome the management challenges brought on by disrupted states.

## Systems “state management”

A simple way to model the lifecycle of a computer is to think of it as having many discrete states that change over its operating life. For example, in a typical lifecycle an image of an operating machine is created, the image is deployed to a specific hardware target, it is booted, and the new hardware becomes operational.

During the system’s operational life its current state changes as new applications are installed, optimizations are applied, user settings are personalized, and security settings are configured. These state changes are regularly tracked and updated to correspond to a standard or normal state that has been defined by administration. At the system’s end of life, it is finally retired.

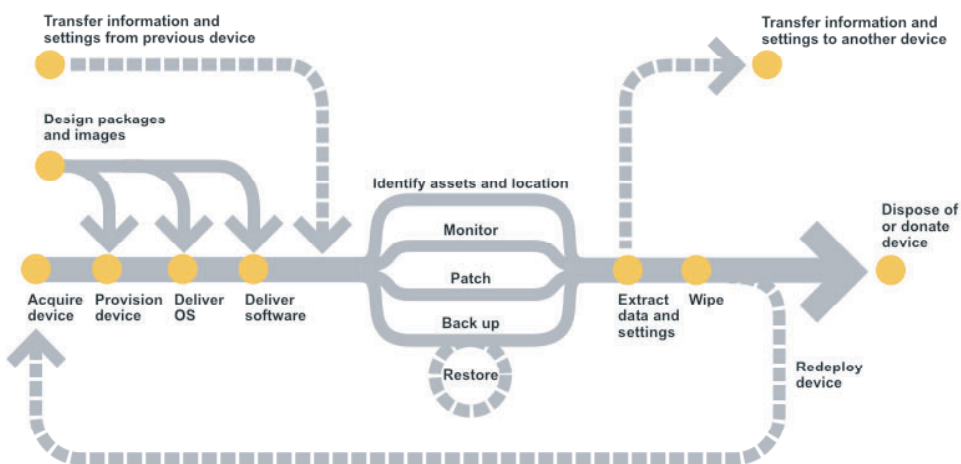


Figure 7. Managing the device lifecycle using Symantec LiveState

## What is Symantec LiveState?

Symantec LiveState is a common management object used for information availability applications such as software/OS management, provisioning, patch management, asset discovery, and recovery.

Symantec LiveState can be represented as a time-stamped point-in-time (PIT) snapshot of a computer’s entire state, or as an installation profile that describes how a particular software component should be installed and configured.

Symantec LiveState objects are stored in open, portable, and editable containers, and they can represent both real and virtual environments.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

Finally, if the lifecycle of a computer is interrupted as the result of an unplanned event, the management system must be able to put it back in operation using a previous state. This critical element of state management is often left out of the lifecycle definition, but doing so ignores the real world where computers are impacted by unplanned and uncontrolled events.

### Single unified platform

Symantec LiveState is a single unified platform for automated configuration management, including image/package design, asset discovery, provisioning and software delivery, patch management, and system recovery.

Its common look-and feel makes it easier for administrators to learn how to use new applications, minimizing training costs and ramp-up time. Similarly, the common database means that new LiveState applications can easily access existing information about clients (such as client name, OS type, etc.) and client groups (such as “All IIS Servers,” “All Salespeople,” etc.).

The LiveState platform is designed as an open and modular architecture with specific integration interfaces to Symantec’s industry-leading security management solutions such as Symantec Enterprise Security Manager™ (Symantec ESM™). As a result, LiveState products work on their own—with tools and processes you already have—but can be assembled into a more comprehensive solution if desired. In addition, security configuration templates are provided for deploying and configuring Symantec’s market-leading client security solutions, such as Symantec™ Client Security, which provides critical client security functions such as antivirus protection, client firewall, intrusion prevention, antispymware protection, and VPN policy compliance.

Additional features of the LiveState management platform include:

- Common LiveState database, which is standards-based (JDBC/ODBC), robust, scalable, platform-independent, and does not require a trained and/or dedicated database administrator (DBA).
  - Common LiveState agent/server protocol, which has been optimized for secure and efficient communication over any type of wired and wireless network, incorporating advanced features such as HTTP/HTTPS, file/byte-level differencing, checkpoint-restart, and compression.
- For example, if a large 10 MB patch needs to be deployed to remote/mobile computers, this protocol allows the patch to be “trickled” to the device in phases over successive connection sessions using low-speed and/or intermittent networks such as dial-up, frame relay, or wireless LANs in local coffee shops.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

- Console that is graphical, easy-to-use, and leverages HTTP/HTTPS for secure and efficient communication between console and remote servers. A common console look-and-feel and ease-of-use features such as drag-and-drop simplify training for new administrators.
- Common LiveUpdate™ mechanism for software updates to the console.
- Common grouping of managed servers and clients.
- Common authentication services (username/passwords for system administrators).
- Common network auto-discovery service (finds all devices that are not currently being managed).

Finally, the automated agent deployment infrastructure minimizes the time to implement new applications by leveraging the existing infrastructure to deploy new application agents and services.

The principal benefit of the common LiveState platform is that it reduces complexity and makes it easier for organizations to easily add other LiveState applications to their environments in the future. This innovative combination of Symantec solutions promotes a significantly more manageable and therefore more secure enterprise infrastructure.

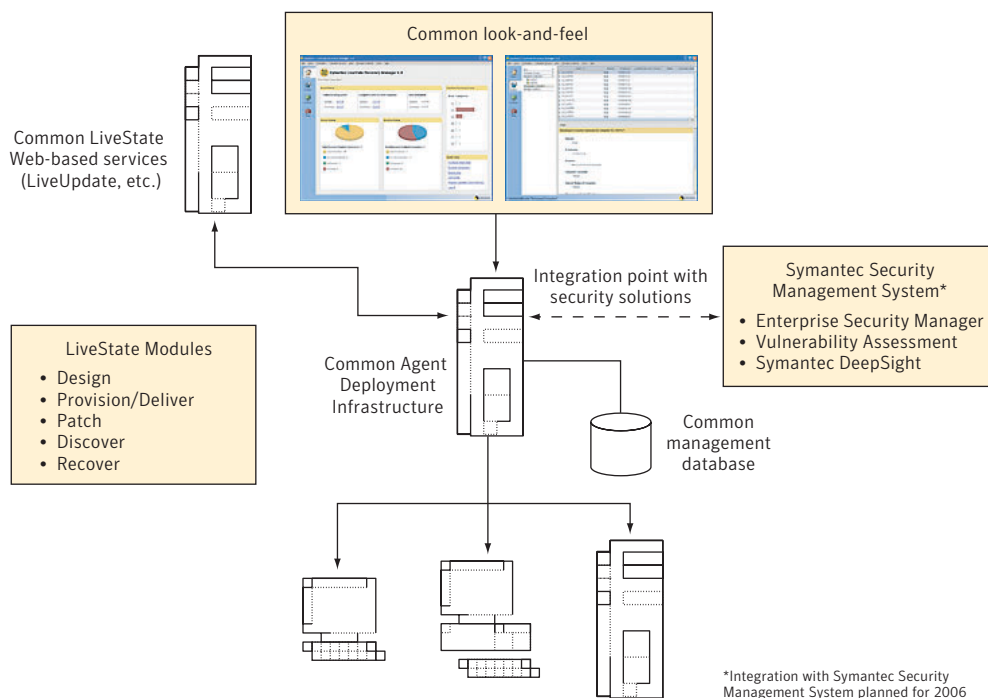


Figure 8. Common Symantec LiveState platform

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## **Symantec LiveState management objects**

LiveState manages two object types throughout much of its operations. These two elements represent the core objects of LiveState's management operations:

- LiveState image snapshot
- LiveState installation package

These objects are open, portable and editable containers, and they can represent both real and virtual environments. The use of these universal objects enables LiveState to function in an open and scalable fashion across a wide variety of networks, environment and platforms.

### ***Symantec LiveState image snapshots***

Creating a snapshot is the process of copying the contents of a logical volume into a single portable file. This file then represents a time-stamped point-in-time (PIT) snapshot of a computer's entire state. These snapshots can be stored, edited, replicated, mounted, and browsed. The use of snapshots gives LiveState the ability to manage computers in a simpler and faster way than other architectures. LiveState snapshots can be taken live and in a full or incremental fashion. LiveState snapshots are abstracted and stored as a single portable file and therefore are easy to copy and replicate. Once taken, LiveState snapshots can be stored on any storage device without requiring any reconfiguration, including both local storage and network-attached storage (NAS).

Manipulating, storing, and recovering LiveState snapshots is very fast, typically running at disk speeds. LiveState images can be used for high-speed deployment as well as high-speed recovery operations. LiveState snapshots can be mounted and scanned for viruses prior to their use to ensure that they don't contaminate the environment.

### ***Symantec LiveState installation package***

The installation package is the second type of LiveState management object. These packages represent an installation profile that describes how a particular software component should be installed and configured. LiveState installation packages can be used for unattended install-based deployments as well as for the recovery of single applications.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

### **Symantec LiveState family of information availability solutions**

The LiveState architecture—and the corresponding LiveState applications—are designed to help businesses manage enterprise operations in both normal and disrupted states. Accordingly, the LiveState family of products is a modular suite of applications that participate in the management of the transition from the normal to the disruptive state and back again in a controlled and safe manner. This family is made up of five modular parts:

- **Installation design:** A virtual design environment that simplifies the creation of installation and recovery packages, including support for Symantec Ghost™ and Symantec DeployCenter Library™ images, unattended installation packages with dynamic parameterization, and third-party packaging formats (MSI, InstallShield, etc.). The goal is to improve and reduce the amount of expertise and effort required to create an installation environment.
- **Software provisioning and delivery:** A centralized delivery environment that automates the local and remote installation of computer operating environments, including operating systems, applications, and configuration values such as security settings.
- **Patch management:** Automated and ultra-accurate patch scanning, download, and remediation.
- **Asset management:** Auto-discovery, hardware/software inventory, software usage and license monitoring, and Web-based reporting.
- **System protection and recovery:** A centrally managed automated recovery environment for both local and remote systems. These disk-based recovery solutions enable IT departments to return to full working condition quickly.

It is our vision that as these applications will be integrated with the “security intelligence” collected from Symantec’s worldwide sensor network and the security management technologies employed by our customers, a powerful convergence of management environments will emerge. This converged set of capabilities will allow organizations to better transition their infrastructures through normal and disrupted state changes. An example of how this might work in a real-world scenario is described later in this document.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

## LiveState process flow

While not an element of the LiveState architecture, the LiveState process flow is an important aspect of the architecture. Figure 9 depicts the LiveState process flow through each stage of a system's lifecycle.

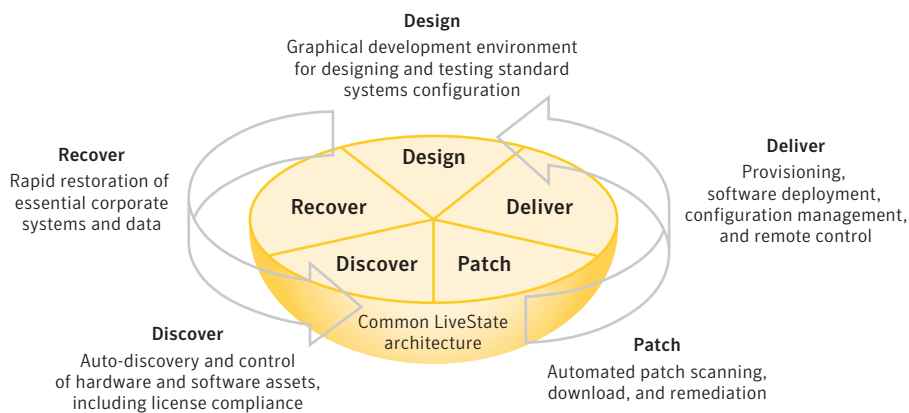


Figure 9. Symantec LiveState process flow

To execute the LiveState Management cycle, LiveState will use the LiveState Management objects and LiveState applications in conjunction with the following aspects of the LiveState process flow:

- Symantec LiveState™ Designer (mastering)
- Symantec LiveState™ Delivery (provisioning and deploying)
- Symantec LiveState™ Patch Manager (applying patches)
- Symantec Discovery™ (asset discovery & inventory)
- Symantec LiveState™ Recovery (system recovery)

In addition, Symantec pcAnywhere™ for Symantec LiveState is also provided for help desk troubleshooting and one-to-one remediation.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

### ***Symantec LiveState Designer***

The process of managing system states is a circular one and the closest to defining a starting point is the design packages and images task shown in Figure 9.

Symantec LiveState Designer contains all of the tools and applications needed to master an image or create an installation package. Symantec LiveState Designer provides a set of graphical tools to create installation packages or to take images of reference machines for modification and deployment. A parameter-based approach minimizes package development time by allowing a single installation package to be dynamically configured for different target installations.

During deployment planning, asset information from Symantec Discovery can be used to determine the content of LiveState packages and images. After creation, LiveState packages are then registered with LiveState Delivery for subsequent delivery to the target machine.

Other tools can be used in conjunction with the mastering tools like Symantec™ Client Migration, a solution for extracting user-specific data, settings, and configuration information. Extracting user settings allows the installation designer to move a user-specific configuration from one installation to another. Symantec Client Migration supports both an administrator-driven and a secure, Web-based self-service model for extracting and restoring end-user data and settings.

### ***Symantec LiveState Delivery***

Symantec LiveState Delivery is built upon a highly scalable multi-tier architecture that enables delivery of images or packages to tens of thousands of systems across a highly distributed infrastructure. After the correct install or image mastering is complete and the content and set of instructions are packaged, it is scheduled for delivery. Symantec LiveState Delivery is used to transport packages of many types to target devices, ranging from Symantec Ghost or Symantec DeployCenter images to application installation packages, security configuration updates, and recovery configurations.

Symantec LiveState Delivery Enterprise Manager, an add-on application provided with Professional Services, offers policy-based, “desired state” (rules-based) management with tight integration to Microsoft® Active Directory™ and other enterprise information sources such as SQL databases.

Symantec LiveState Delivery simplifies and automates existing manual IT processes, and transforms them into unattended operations that can be performed on multiple systems simultaneously—across the enterprise and across virtually all types of devices and networks—in a dynamic and adaptive manner.

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

### ***Symantec LiveState Patch Manager***

Symantec LiveState Patch Manager determines what devices are missing patches, downloads the patches to a local administrative server (along with knowledge base information about them) and then securely deploys the patches to all affected systems.

Symantec LiveState Patch Manager provides a highly intuitive process to manage dynamic grouping of clients and flexible scheduling of patch management tasks. It leverages the LiveState agent/server protocol to efficiently support patch discovery and deployment to both local and mobile/remote clients, over both high-speed and low-speed networks. LiveState Patch Manager also provides many reports that can aid in compliance reporting.

### ***Symantec Discovery***

Symantec Discovery provides information about the assets present within a networked environment. This information can then be used to determine targets to be included for various projects such as migrating, making additional storage purchases, performing memory upgrades, reassigning software licenses, and helping ensure devices are compliant with corporate standards.

### ***Symantec LiveState Recovery***

The Symantec LiveState Recovery client allows LiveState volume snapshots to be taken “hot” (without taking the system offline) from any computer on which the Symantec LiveState Recovery service is installed. This stored state, plus any state stored before and after, become point-in-time (PIT) restore points for that device. Point-in-time restore points are used by LiveState Recovery to rapidly restore any managed device. Symantec LiveState Recovery can restore entire bare metal systems, as well as individual file folders or objects such as critical operating system files and drivers.

LiveState Recovery supports a range of enterprise capabilities including:

- Microsoft Volume Shadow Copy Service (VSS), for automatically setting VSS-aware databases—such as Microsoft SQL Server and Microsoft Exchange—to a quiet state without taking them offline during snapshots. (Pre- and post-operation custom scripting actions are supported for non-VSS applications.)
- VERITAS Virtual Volume Manager (now from Symantec) for automatic conversion from simple to dynamic disk (and vice versa).

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

- Performance throttling for minimizing impact on networks and end users.
- Secure encryption of recovery image files, which can then be stored anywhere on the network, including local attached storage, NAS, and SAN devices.

A related add-on application, called LiveState Recovery Manager, provides centralized, policy-based management and reporting for LiveState Recovery environments.

### **Remote control**

Organizations work in highly distributed environments, and physically touching a target computer is not always practical. Consequently, many functions that at one time were restricted to being local to the device now need to be handled by remote access management. Activities such as reconfiguration, recovery, and reprovisioning have become a necessary element for managing remote and darkened data centers.

For more than a decade, Symantec pcAnywhere has been the standard in remote control software. Its integration with other Symantec LiveState applications such as Symantec LiveState Delivery and Symantec LiveState Recovery brings a powerful and very secure remote access and management capability to the Symantec LiveState architecture.

### **Sample scenario: Preventing exploits and recovering rapidly**

Symantec's strategy for the convergence of security, systems, and storage management is to enable the creation of an integrated, holistic enterprise solution that effectively manages in both normal and disrupted states of operation.

A high-level view of this envisioned schema (Figure 10) shows Symantec DeepSight alerts driving the management system to execute on predetermined alert action policies. In turn, these policies drive:

- Security workflow to increase its defenses
- Systems workflow to screen for vulnerabilities and patch or remediate the device
- Storage workflow to create more granular Symantec LiveState restore points

This system moves into a disrupted state until the vulnerability is patched. Meanwhile, blocking technology is used to stave off known behaviors, and the storage system is used to create a worst-case restore position. Working as a single management system, the converged disciplines provide an example of how both normal and disrupted state management can be controlled by a unified approach.

# Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

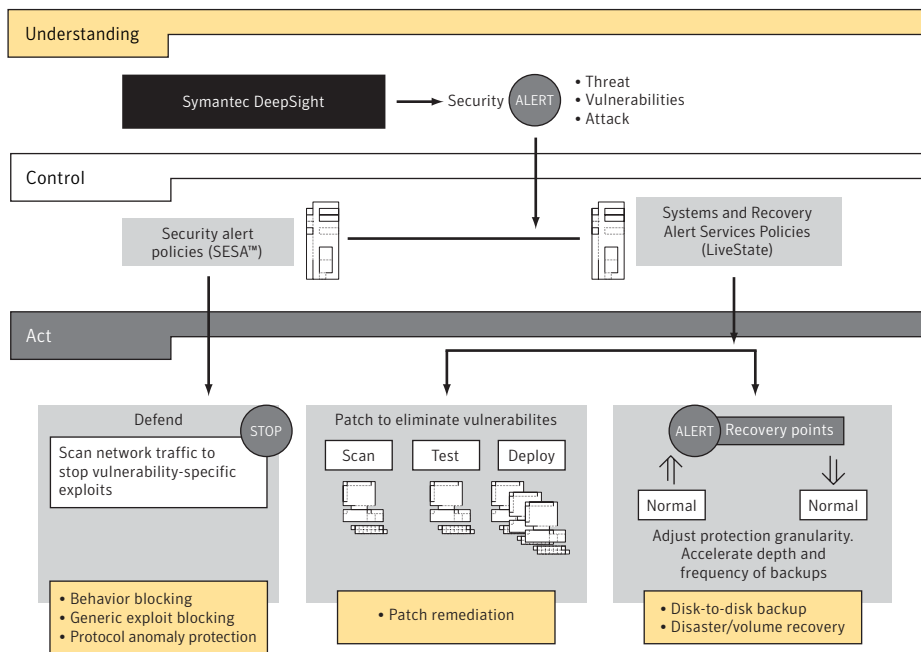


Figure 10. Sample scenario: exploit prevention and recovery

## Symantec LiveState and Symantec’s enterprise management strategy

In today’s increased threat environment—and with organizations increasingly dependent on the availability of information managed by our IT infrastructure—a unified approach to storage and systems management, coupled with integration to security management, is becoming mission critical.

The ongoing struggle to protect businesses’ livelihood from the exponential increase in rapid-spreading, malicious attacks, as well as other disruptive events, requires a dramatic shift in how enterprises approach the management of their IT infrastructures.

The Symantec LiveState platform and family of information availability solutions support the convergence of critical IT processes—spanning systems, storage, and security management—into a holistic methodology that lets organizations establish healthy, normal operating states via automation and standardization, as well as successfully recover from disrupted states.

As a result, Symantec can help organizations stay ahead of the security threat curve and significantly minimize the effects of disruptions in business operations. Symantec can help

## Symantec LiveState™—A Unified Platform for Successfully Managing Both Normal and Disrupted IT Operations

businesses gain a better, smarter, and more efficient way to combat attacks, eliminate vulnerabilities, and respond to and successfully manage through any event that disrupts the normal course of business.

The Symantec LiveState family of solutions helps ensure client resilience by discovering, provisioning, configuring, patching, and recovering devices throughout an organization, including laptops, desktops, handheld devices, and servers. With Symantec LiveState, IT organizations can capitalize on Symantec's best-in-class technology to keep their critical systems secure, available, and compliant with corporate standards—from acquisition to disposal.



## About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

Symantec has worldwide operations in more than 40 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec, the Symantec logo, LiveUpdate, and pcAnywhere are U.S. registered trademarks of Symantec Corporation. Information Integrity, SESA, Symantec Client Migration, Symantec Client Security, Symantec DeepSight Alert Services, Symantec DeepSight Management Services, Symantec DeployCenter, Symantec Discovery, Symantec Enterprise Security Manager, Symantec ESM, Symantec Ghost, Symantec LiveState, Symantec LiveState Delivery, Symantec LiveState Management, Symantec LiveState Patch Manager, Symantec LiveState Recovery, Symantec Security Management System, and Symantec Vulnerability Assessment are trademarks of Symantec Corporation. Microsoft, Active Directory, ActiveX, and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. All other brand and product names are trademarks of their respective holder(s). Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. Copyright © 2005 Symantec Corporation. All rights reserved. Printed in the U.S.A. 7/05 10333245