



Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung, des normalen und des gestörten IT-Betriebs

Erhöhen der Widerstands-
fähigkeit von Clients durch
Schutz, Verfügbarkeit und
Kompatibilität der Geräte mit
den Unternehmensstandards

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung von beidem, des normalen und des gestörten IT-Betriebs

Inhalt

Zusammenfassender Überblick	3
Symantecs Strategie der Information Integrity	4
Vorteile durch Konvergenz	5
Der Infrastrukturlebenszyklus	7
Stabile Geschäftsabläufe	7
Geplante Unterbrechungen der Geschäftsabläufe	7
Unvorhergesehene Unterbrechungen der Geschäftsabläufe	8
Schnelle Wiederherstellung nach einer Unterbrechung	9
Integrierte Verwaltungsinfrastruktur	10
Aspekte einer zusammengeführten Verwaltungsarchitektur	11
Normaler Betriebszustand	12
Übergang in einen gestörten Betriebszustand	13
Wiederherstellung nach Betriebsstörungen	14
Die Symantec LiveState-Architektur	16
"Statusverwaltung" von Systemen	16
Integrierte, vereinheitlichte Plattform	17
Symantec LiveState – Management-Objekte	19
Symantec LiveState – Image-Snapshots	19
Symantec LiveState – Installationspakete	19

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Inhalt (Forts)

Symantec LiveState-Produktfamilie aus Lösungen für Information Integrity	20
LiveState-Prozessablauf	21
Symantec LiveState Designer	22
Symantec LiveState Delivery	22
Symantec LiveState Patch-Manager	23
Symantec Discovery	23
Symantec LiveState Recovery	23
Fernsteuerung	24
Beispiel: Verhindern von Angriffen und schnelles Wiederherstellen von Systemen	24
Symantec LiveState und Symantecs Strategie für die Unternehmensverwaltung	25

Haftungsausschluss

Dieses Hintergrundpapier (White Paper) steht Symantec-Kunden, potenziellen Kunden und Partnern zur Verfügung. Darin wird die strategische Vision und Ausrichtung von Symantec im Bereich Systemverwaltung und Speicherverwaltung beschrieben. Dieses Dokument eignet sich vor allem für IT-Fachleute und soll ihnen als Leitfaden zum besseren Verständnis und zur Beurteilung der allgemeinen Ausrichtung von Symantec hinsichtlich der LiveState-Architektur und des LiveState-Lösungsangebots dienen. In diesem Dokument wird lediglich Symantecs Sicht der zukünftigen Strategie in diesem Bereich beschrieben, es beinhaltet jedoch keinerlei Verpflichtung, bestimmte Produkte oder Dienstleistungen anzubieten oder zur Verfügung zu stellen. Die in diesem Dokument beschriebenen Pläne hinsichtlich Architektur, Produkte und Dienstleistungen sowie die beschriebenen Funktionen können sich gegebenenfalls ändern. Funktionen werden Kunden, falls verfügbar, in einem allgemeinen Produkt-Release zur Verfügung gestellt.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Zusammenfassender Überblick

Der rapide Anstieg der Sicherheitsbedrohungen zusammen mit der wachsenden Abhängigkeit von Unternehmen von ihrer IT-Infrastruktur bedeutet für viele ein ernst zu nehmendes Risiko. Dazu gehören nicht nur finanzielle und rechtliche Risiken bzw. Risiken, die mit der Nichteinhaltung gesetzlicher Regelungen verbunden sind, sondern auch das Risiko des Vertrauensverlusts eines Unternehmens bei Kunden und Investoren.

Nicht nur kostenintensive Unterbrechungen durch "unvorhergesehene" Ereignisse wie Sicherheitsangriffe spielen hier eine Rolle. Unternehmen müssen auch mit kostenaufwändigen Störungen der Geschäftsabläufe aufgrund von "geplanten" IT-Aktivitäten wie die unternehmensweite Migration von Betriebssystemen und die Verteilung neuer Anwendungen und Plattformen fertig werden.

Die mangelnde Fähigkeit vieler Unternehmen, schnell und effektiv auf diese Bedrohungen und Störungen der Geschäftsabläufe zu reagieren, ist größtenteils sowohl auf beabsichtigte als auch ungeplante Barrieren zurückzuführen – Barrieren, die nicht nur die einzelnen Infrastrukturen für die System-, Speicher- und Sicherheitsverwaltung voneinander trennen, sondern auch zwischen IT-Mitarbeitern und -Prozessen bestehen. Unternehmen können diese Barrieren nur dann überwinden, wenn sie die Verwaltung ihrer Unternehmensinfrastrukturen unter einem vollkommen neuen Blickwinkel betrachten.

Die Herausforderung besteht darin, auf die gestiegene Anzahl an heutigen Bedrohungen zu reagieren, unternehmenskritische IT-Infrastrukturen zu schützen und die Betriebsbereitschaft unterbrochener IT-Abläufe schnell wieder herzustellen. Dazu müssen Unternehmen ihre separaten Prozesse und Infrastrukturen für die Speicher- und Systemverwaltung zusammenführen und stärker mit der Infrastruktur und den Prozessen für die Sicherheitsverwaltung integrieren.

Die innovative LiveState-Produktfamilie von Symantec aus Lösungen für die Informationsverfügbarkeit unterstützt Unternehmen bei der Beseitigung der technischen und betrieblichen Grenzen, die in der Vergangenheit zwischen Speicher-, System- und Sicherheitsverwaltung bestanden. Die Symantec LiveState-Produktfamilie basiert auf erstklassigen Speicher- und Systemverwaltungstechnologien. Sie bietet zudem eine einzige integrierte Plattform für die automatisierte Konfigurationsverwaltung mit Funktionen für Image-/Paketerstellung, Bestandserfassung, Softwarebereitstellung und -verteilung, Patch-Management und Systemwiederherstellung. Die Symantec LiveState-Produkte basieren auf einer offenen und modularen Architektur. Der Vorteil: Die einzelnen Produkte können separat voneinander eingesetzt werden – zusammen mit Programmen und Prozessen, die bereits im Unternehmen vorhanden sind – oder zu einer umfassenderen Lösung verbunden werden.

Die Symantec LiveState-Architektur wurde mit speziellen Integrationsschnittstellen zu den branchenführenden Lösungen von Symantec für die Sicherheitsverwaltung in Unternehmen entwickelt. Darüber hinaus sind Sicherheitskonfigurationsvorlagen für die Verteilung und Konfiguration von marktführenden Client-Sicherheitslösungen von Symantec vorhanden. Mit dieser innovativen Kombination aus Symantec-Lösungen lässt sich eine Unternehmensinfrastruktur verwirklichen, die deutlich einfacher zu verwalten und damit sicherer ist.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Dieser neue Ansatz bei der Unternehmensverwaltung befähigt Unternehmen, stabile normale Betriebszustände einzurichten sowie Störungen ihrer Betriebsabläufe zu bewältigen, zu reduzieren und zu beheben. Unternehmen können jetzt den Status ihrer Geschäftsabläufe einfacher und effizienter verwalten und schützen, ohne dazu zusätzliche IT-Mitarbeiter einstellen zu müssen.

Mithilfe der Symantec LiveState-Lösungen können Unternehmen auch die Widerstandsfähigkeit von Clients erhöhen, indem sie dafür sorgen, dass ihre wichtigen Systeme jederzeit geschützt, verfügbar und kompatibel mit den Unternehmensstandards sind – vom Kauf bis hin zur Außerbetriebnahme. Die Lösungen bieten optimierte, intelligente und effiziente Methoden zur Abwehr von Angriffen, Beseitigung von Schwachstellen sowie Reaktion und Wiederherstellung bei Ereignissen, die zu Ausfällen führen können. Sämtliche Aufgaben lassen sich mit einem geringeren Zeit- und Arbeitsaufwand sowie besseren Ergebnissen durchführen.

Symantecs Strategie der Information Integrity™

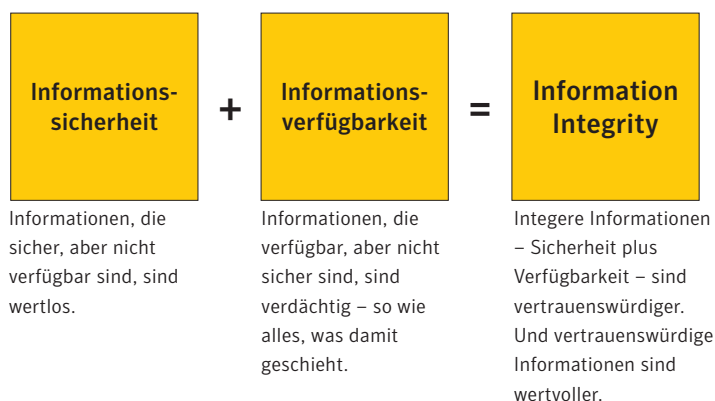


Abbildung 1. Informationen sind Ihr wichtigstes Kapital. Ein reibungsloser und sicherer Informationsfluss kann Ihr Unternehmen verändern.

Informationen sind die treibende Kraft Ihres Unternehmens. Ihre Sicherheit und Verfügbarkeit, überall und jederzeit, ist eine der wichtigsten Aufgaben. Deshalb hat Symantec einen neuen Ansatz für das Informations-Management entwickelt: Erstklassige Sicherheit verbunden mit herausragenden System- und Speicherverwaltungsfunktionen für Ihre Netzwerkressourcen. Das Ergebnis nennen wir "Information Integrity". Dieser neue Ansatz soll Sie bei einer Ihrer wichtigsten Aufgaben unterstützen: Dafür zu sorgen, dass Ihr Unternehmen reibungslos funktioniert – egal, was passiert.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Unternehmen müssen tagtäglich die unterschiedlichsten Anforderungen erfüllen. So war beispielsweise die Fragmentierung von Unternehmensumgebungen einer der Gründe, warum es für Unternehmen aller Größen bisher schwierig war, die Datensicherheit und Datenverfügbarkeit gleichzeitig zu optimieren. Selbst in mittelständischen Unternehmen müssen verschiedene Geräte, Betriebssysteme, Anwendungen und Netzwerke unterstützt werden. Hinzu kommen Funktionen für Angriffsprävention, Schutz vor Spionageprogrammen, Richtlinieneinhaltung, Virenschutz, Patch-Management, Lizenzüberwachung, Verteilung von Betriebssystemen und Anwendungen sowie System- und Datenwiederherstellung.

Diese unterschiedlichen Anforderungen führten in vielen Unternehmen zu ähnlich fragmentierten Lösungen mehrerer unabhängiger Technologieanbieter. Unternehmenswichtige System- und Sicherheits-Tools sind nicht immer miteinander kompatibel. IT-Verfahren und Sicherheitsfunktionen überschneiden sich oft oder setzen widersprüchliche Prioritäten. Für die Behebung von Problemen müssen möglicherweise Dutzende Anbieter herangezogen werden. Die Folge: Hohe Kosten, langsame Reaktionszeiten und die Unfähigkeit, Unternehmensziele zu erreichen.

Information Integrity kann die Produktivität und Effizienz im gesamten Unternehmen erheblich verbessern. Nicht nur Ihre aktuellen Sicherheitsfunktionen und IT-Verfahren werden optimiert, Information Integrity sorgt auch für eine effizientere Zusammenarbeit dieser Komponenten.

Wenn Informationen schnell verfügbar und vertrauenswürdig sind, können Sie die Betriebskosten senken, die Kundenzufriedenheit steigern und das Umsatz- und Gewinnwachstum beschleunigen. Und nicht nur das: Ihr Unternehmen kann gesetzliche Auflagen besser erfüllen, eine widerstandsfähigere IT-Infrastruktur aufbauen, einen mobilen Mitarbeiterstab wirksam unterstützen und erfolgreich neue Geschäfts- und Technologieinitiativen starten.

Kurz gesagt: Mithilfe der Information Integrity können Sie das gesamte Potenzial Ihres Unternehmens nutzen und den Wert Ihrer wichtigsten Unternehmensressource optimieren.

Vorteile durch Konvergenz

Unternehmen sind mit der schwierigen Aufgabe konfrontiert, ihre IT-Umgebungen zu verwalten und die fortlaufende Verfügbarkeit ihrer Unternehmensdienste zu gewährleisten. Störungen der Unternehmensdienste können vielfältige Ursachen haben, beispielsweise Benutzerfehler, Stromausfälle, falsch konfigurierte Systeme oder Cyber-Angriffe, die Softwareschwachstellen ausnutzen. Der Aufbau einer störungsfreien Umgebung ist angesichts der Komplexität der IT-Umgebung und der sich ständig ändernden Bedrohungen kaum möglich. Das Bedrohungsspektrum ist weit gefasst: steigende Anzahl von Schwachstellen, komplexe Angriffsformen und schädlicher Angriffscodes, der veröffentlicht wird, bevor Unternehmen Patches testen und im gesamten Unternehmen installieren können.

Die Zeitspanne für die Behebung von Schwachstellen wird außerdem immer kürzer. In den letzten vier bis fünf Jahren war eine ständige Zunahme der neu dokumentierten Schwachstellen zu verzeichnen. 1999 belief sich diese Zahl auf lediglich 10 Schwachstellen pro Woche, 2004 waren es bereits durchschnittlich 53 Schwachstellen pro Woche.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Laut dem Symantec-Bericht zu Bedrohungen aus dem Internet¹ konnten 80 Prozent dieser Schwachstellen per Fernzugriff ausgenutzt werden und 70 Prozent wurden als leicht ausnutzbar eingestuft.

Zudem beträgt die durchschnittliche Zeitspanne zwischen der Veröffentlichung einer Schwachstelle und dem Auftreten eines entsprechenden schädlichen Angriffscodes inzwischen 5,8 Tage. Gegenüber dem vorhergehenden Berichtzeitraum, in dem der Durchschnitt 7 Tage betrug, ist eine deutliche Verkürzung dieser Zeitspanne zu verzeichnen. Der Blaster-Wurm infizierte Netzwerke bereits 26 Tage nach der offiziellen Veröffentlichung der Schwachstelle.

Durch die rasante Zunahme bössartiger Computerangriffe und die dadurch verursachten enormen Kosten steht die Sicherheit bei vielen Vorständen und IT-Kontrollgremien ganz oben auf der Tagesordnung. Obwohl der Absicherung des Unternehmens eine große Bedeutung beigemessen wird, erfüllen die erzielten Ergebnisse noch längst nicht die Erwartungen und Anforderungen. Einige führen das Problem darauf zurück, dass sich trotz des deutlichen Anstiegs bei der Häufigkeit und Intensität der Bedrohungen die Zahl der Mitarbeiter in den meisten IT-Abteilungen, die mit dieser Bedrohungsflut fertig werden müssen, in den letzten Jahren nur geringfügig erhöht hat. Die Erhöhung des IT-Personals ist jedoch nicht nur kostenintensiv, sondern auch nicht die Lösung des Problems.

Damit Unternehmen den Wettlauf gegen ständig neu auftretende Sicherheitsbedrohungen gewinnen können, benötigen sie eine bessere, intelligentere und effizientere Methode, um Angriffe abzuwehren, Schwachstellen zu beseitigen und auf Ereignisse zu reagieren, die die normalen Geschäftsabläufe stören. Sicherheitsbedrohungen sind jedoch nur ein Teil der Ereignisse, die für Störungen von Geschäftsabläufen verantwortlich sind. Hinzu kommen Naturkatastrophen, Terrorbedrohungen, Stromausfälle, Hardware- und Softwarefehler sowie menschliches Versagen. All diese Ereignisse können zu einer Unterbrechung der normalen IT-Abläufe führen.

Die meisten IT-Abteilungen haben sich damit abgefunden, dass routinemäßig durchgeführte Software-Updates von Betriebssystemumgebungen ein notwendiger Bestandteil der Unternehmensverwaltung sind, obwohl diese Verfahren eine der Hauptursachen für die Unterbrechung der normalen Unternehmensaktivitäten sind. Die meisten IT-Fachleute sind sich zudem darin einig, dass der Schutz der Unternehmensdaten die Grundlage ist, um Systeme nach einem Ereignis, das zu einem Ausfall geführt hat, wiederherstellen zu können. Tatsache ist, dass die System-, Speicher- und Sicherheitsverwaltung jeweils eine wichtige Rolle bei der Verhinderung von Störungen und der Wiederherstellung von Systemen nach Ausfällen spielt. Allerdings werden diese drei Bereiche häufig zu isoliert betrachtet und bestehen aus unabhängigen Aufgabenbereichen und Betriebsabläufen. Diese eigenständige Funktionsweise ist oft mit manuell gesteuerten Richtlinien an den Integrationspunkten verbunden.

Ließe sich die IT-Umgebung mit einer bestimmten Konfiguration und nur geringfügigen Änderungen festschreiben, wäre dieser Mangel an Integration nicht so bedeutend. Angesichts heutiger äußerst dynamischer Unternehmens- und IT-Umgebungen ist es jedoch unrealistisch davon auszugehen, dass Konfigurationen statisch sind. Die sich ständig wandelnden neuen Anforderungen moderner Unternehmen erfordern ein Umdenken bei der Art und Weise, wie die IT-Umgebung verwaltet wird.

Bedrohungen, die sich ständig ändern

Die Zeitspanne für die Patch-Installation ist kurz:

- W32 Blaster-Wurm: 26 Tage zwischen Schwachstellenbekanntgabe und Auftauchen des Wurms. Die Schwachstelle wurde am 16. Juli 2003 veröffentlicht. Der Blaster-Wurm wurde am 11. August 2003 entdeckt.
- W32 Sasser-Wurm: 17 Tage zwischen Schwachstellenbekanntgabe und Auftauchen des Wurms. Die Schwachstelle wurde am 13. April 2004 veröffentlicht. Der Sasser-Wurm wurde am 30. April 2004 entdeckt.
- W32 Witty-Wurm: 30 bis 40 Stunden zwischen Schwachstellenbekanntgabe und Auftauchen des Wurms. Die Schwachstelle wurde am 18. März 2004 veröffentlicht. Der Witty-Wurm wurde am 19. März 2004 entdeckt.

Sich schnell ausbreitende Bedrohungen:

- Klez H: 4.516 Einsendungen pro Tag. Höchster Verbreitungsgrad innerhalb von 2 Wochen.
- BadTrans: 3.709 Einsendungen pro Tag. Höchster Verbreitungsgrad innerhalb von 7 Tagen.
- Bugbear B: 4.812 Einsendungen pro Tag. Höchster Verbreitungsgrad innerhalb von 2 Tagen.
- SoBig F: 1.800 Einsendungen pro Tag. Höchster Verbreitungsgrad innerhalb von 1 Tag.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Unternehmen müssen die Barrieren zwischen den Bereichen Systemverwaltung, Speicherverwaltung und Sicherheitsverwaltung beseitigen, um eine IT-Umgebung aufzubauen, die stabile normale Betriebszustände fördert. Dazu benötigen sie einen Ansatz, der diese isolierten Bereiche in einer einzigen, ganzheitlichen Infrastruktur vereint. Nur dann können sie den Wettlauf gegen ständig neu auftretende Bedrohungen gewinnen und erfolgreich den Kampf gegen geplante und unvorhergesehene Ereignisse, die die Geschäftsabläufe unterbrechen oder stören, bestehen. Mit der LiveState-Produktfamilie aus Lösungen für die Informationsverfügbarkeit unterstützt Symantec Unternehmen bei der Erreichung dieses Ziels.

Der Infrastruktur-Lebenszyklus

Stabile Geschäftsabläufe

Die Wirklichkeit in der heutigen dynamischen und unsicheren Geschäftswelt sieht für viele Unternehmen so aus, dass selbst unter normalen Betriebsbedingungen eine genauere Untersuchung zu dem Ergebnis führt, dass der "normale" Zustand ihrer IT-Umgebung von einem "stabilen" Zustand weit entfernt ist. Viele "normale" oder routinemäßig durchgeführte Geschäftsabläufe, wie beispielsweise die Verteilung neuer Unternehmensanwendungen oder Betriebssystemplattformen, können sich ebenso störend und kostenintensiv auf die Stabilität eines Unternehmens auswirken wie bössartige Angriffe auf die Infrastruktur.

Unabhängig davon, ob es sich um bössartige Angriffe, Systemausfälle oder normale Bereitstellungsaktivitäten handelt: Unternehmen sind ständig Ereignissen ausgesetzt, die zu einer Störung der Geschäftsabläufe führen können. Dabei spielt es keine Rolle, ob das Ereignis geplant war oder unerwartet auftrat. Jede Unterbrechungsminute kostet Geld und stellt ein potenzielles Risiko für das Unternehmen dar. Unternehmen haben erkannt, dass sie nicht nur die Anfälligkeit für Störungen reduzieren oder vollkommen ausschalten, sondern Systeme nach diesen Unterbrechungen auch schnell wiederherstellen müssen. Der Schlüssel zur Beseitigung oder deutlichen Reduzierung der Auswirkungen dieser Unterbrechungen ist ein ganzheitlicher Ansatz bei der System-, Speicher- und Sicherheitsverwaltung. Dieser Ansatz muss so gestaltet sein, dass er stabile normale Betriebszustände fördert und damit folgende Problembereiche abdeckt:

- Geplante Unterbrechungen der Geschäftsabläufe
- Unvorhergesehene Unterbrechungen der Geschäftsabläufe
- Schnelle Wiederherstellung nach einer Unterbrechung

Geplante Unterbrechungen der Geschäftsabläufe

Zu den normalen Aufgaben im IT-Bereich gehören die ständige Aktualisierung und Konfiguration von Servern, Desktops, Laptops und mobilen Geräten, um so dafür zu sorgen, dass die Umgebung verfügbar und sicher ist. Unabhängig davon, ob es sich bei diesen Aufgaben um eine Hardwareaktualisierung, die Verteilung eines neuen Betriebssystems oder nur um ein schnelles Service Pack-Update wie beispielsweise auf Windows® XP SP2 handelt, der Normalzustand des

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Unternehmens ändert sich regelmäßig. Diese Konfigurationsänderungen finden zwar geplant statt, sie können dennoch Störungen und hohe Kosten verursachen.

Dazu ein Beispiel: Die Herausforderung, Systeme zu migrieren und einzurichten, sobald eine neue Betriebssystemversion veröffentlicht wird, ist inzwischen so groß, dass einige IT-Manager die Systembereitstellung als karrierebedrohliches Ereignis ansehen. Diese Aufgabe besteht aus mehreren Schritten: Zunächst muss erfasst werden, was auf jedem Computer im Unternehmen installiert ist. Zusätzlich müssen die Standards für eine neue Betriebsumgebung festgelegt, die Umgebung für die Verteilung des Betriebssystems vorbereitet und zuletzt die Änderungen verteilt werden. Der gesamte Prozess erfordert ein hohes Maß an manuellen Aktivitäten und Fachwissen. Er kann sich als so schwierig erweisen, dass viele Unternehmen bis heute noch nicht auf Windows XP umgestellt haben, obwohl diese Betriebssystemversion ihnen zahlreiche Vorteile hinsichtlich Zuverlässigkeit, Sicherheit und Leistung bietet.

Die Bereitstellung gehört traditionell zu den Verwaltungsaufgaben, die im normalen Betriebszustand ausgeführt werden, sie ist jedoch äußerst zeitaufwändig und wirkt sich oft störend auf die Unternehmensaktivitäten aus. Durch eine verbesserte Automatisierung der Bereitstellungsaufgabe können diese Störungen reduziert und damit ein stabilerer Normalzustand erreicht werden.

Unvorhergesehene Unterbrechungen der Geschäftsabläufe

Das Kennzeichen unvorhergesehener Unterbrechungen sind eine plötzliche Bedrohung oder Störung in der Betriebsumgebung sowie die Notwendigkeit einer ungeplanten, nicht vorgesehenen Reaktion, um den normalen Betriebszustand wiederherzustellen.

Ein klassisches Beispiel für unvorhergesehene Betriebsunterbrechungen ist die Ankündigung oder Entdeckung einer neuen Sicherheitsschwachstelle wie beispielsweise ein Wurm oder eine komplexe Bedrohung. Sicherheitsschwachstellen sind selbstverständlich nicht die einzige Ursache für diese Art von Störungen. Dazu gehören auch Naturkatastrophen, Stromausfälle, Hardware- oder Softwarefehler oder menschliches Versagen. Alle diese Ursachen haben jedoch eines gemeinsam: Unternehmen müssen schnellstmöglich den normalen Betriebszustand wiederherstellen.

Die IT-Infrastruktur ist ständigen Angriffen durch unbefugte Zugriffsversuche ausgesetzt, die Schwachstellen in der Betriebssoftware des Unternehmens ausnutzen. Vorbeugende Maßnahmen zur Abwehr dieser Angriffe, beispielsweise durch Beseitigen von Schwachstellen durch Patch-Installation, Schützen wichtiger Daten und Konfigurieren von Sicherheitssystemen, führen zu dynamischen Änderungsprozessen, die den normalen Betriebszustand der Unternehmens- und IT-Umgebung beeinträchtigen. So störend wie sich diese vorbeugenden Maßnahmen auch auswirken können: Schwachstellen, die nicht rechtzeitig beseitigt werden, können erheblich höhere Schäden verursachen. Die Dringlichkeit dieser Präventivmaßnahmen bietet deshalb keinen großen Spielraum für langfristige Planungen.

Von den Maßnahmen zur Abwehr von Angriffen bereitet die Patch-Verwaltung Informationsmanagern das größte Kopfzerbrechen. Insbesondere die vollständige Beseitigung von Schwachstellen durch die Installation von Patches und die sichere Konfiguration von Computern (z. B. durch Schließen geöffneter Ports, Herunterfahren überflüssiger Dienste usw.) ist ein Problem, das sich nicht leicht lösen lässt. Dies ist hauptsächlich darauf zurückzuführen,

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

dass der Patch-Prozess bei der Aktualisierung der Software nicht mit der schnellen Entwicklung der Bedrohungssituation Schritt halten kann.

Die Zunahme der Viren, Würmer und komplexen Bedrohungen sind ein Beleg dafür, dass Programmierer von schädlichem Code Sicherheitsschwachstellen auch weiterhin ausnutzen werden. Mit jeder neuen Schwachstelle und dem Auftreten von schädlichem Programmcode wird die Zeitspanne für IT-Abteilungen, die ihnen für die Umsetzung geeigneter Reaktionsmaßnahmen bleibt, immer kürzer (siehe Abbildung 2).

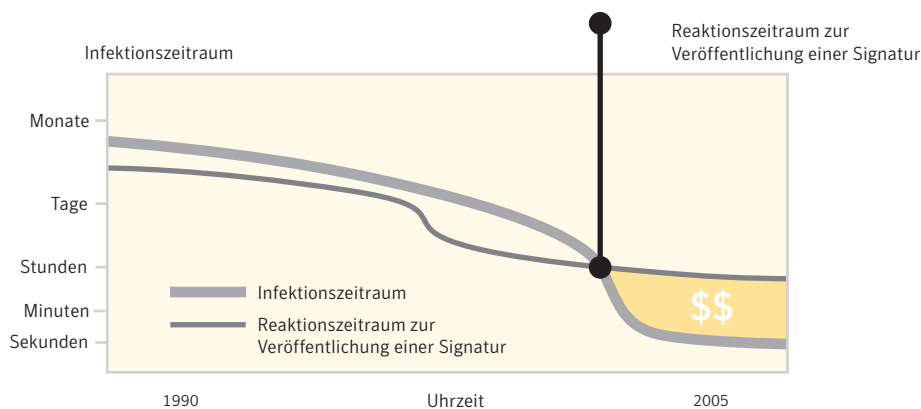


Abbildung 2. Die IT-Branche scheint an einem Punkt angekommen zu sein, an dem sich die neuesten Bedrohungen schneller ausbreiten als darauf reagiert werden kann.

Durch eine enge Integration von automatisierten Prozessen zur Schwachstellenprüfung, Patch-Management-Planung und Patch-Verteilung mit Systemverwaltungsprozessen wie die Softwarebereitstellung können Unternehmen bedeutend schneller auf neu entdeckte Schwachstellen reagieren. Auf diese Weise lassen sich Störungen, die zuvor mit dem Patch-Management-Prozess verbunden waren, reduzieren oder in manchen Fällen sogar vollständig ausschalten.

Schnelle Wiederherstellung nach einer Unterbrechung

Aufgrund der steigenden Zahl der Angriffe wächst auch die Wahrscheinlichkeit, dass Unternehmen betroffene Systeme und Daten wiederherstellen müssen. Deshalb benötigen selbst die sichersten Unternehmen einen Backup- und Wiederherstellungsplan, mit dem sie Systeme und Daten nach einem destruktiven Angriff oder einer anderen Betriebsunterbrechung erfolgreich wiederherstellen können.

Bei der Wiederherstellung des betriebsfähigen Zustands ist Zeit ein wichtiger Faktor: Der von einem erfolgreichen Angriff verursachte Schaden wächst proportional zu der Zeitspanne, die für die Wiederherstellung benötigt wird. Die Wiederherstellungsarchitektur sollte wichtige Server, Desktops, mobile Geräte wie Laptops und spezielle Geräte wie POS- und ATM-Systeme mit einbeziehen.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Die US-Regierung und die Europäische Union haben ebenfalls auf die Notwendigkeit einer zuverlässigen und automatisierten Datenwiederherstellung hingewiesen. Führungskräfte sind inzwischen persönlich dafür verantwortlich, dass IT-Prozesse richtig implementiert werden. Diese Rechenschaftspflicht bei der Infrastruktur wird von einer wachsenden Zahl an Verordnungen wie Sarbanes-Oxley, HIPAA, FISMA und Basel II gefördert.

Alle diese Faktoren unterstreichen den Bedarf an zuverlässigen und automatisierten Systemen für Daten-Backups und die Wiederherstellung nach Notfällen, die eng mit der Unternehmenssicherheit und Systemverwaltung verknüpft sind.

Integrierte Verwaltungsinfrastruktur

Heutige Umgebungen sind immer größeren Risiken ausgesetzt. Unternehmen müssen deshalb dafür sorgen, dass Komponenten der Sicherheits-, System- und Speicherverwaltung in ihrer Infrastruktur nicht nur unter normalen Bedingungen optimal arbeiten, sondern auch während einer durch einen Angriff verursachten Störung effektiv funktionieren. Sie müssen deshalb ihre normalen Betriebsabläufe so verwalten, dass Störungen reduziert werden und sie schnell und kosteneffizient auf Störungen reagieren können. Dies gelingt nur, wenn die Sicherheits-, System- und Speicherverwaltung in einer nahtlosen Verwaltungsinfrastruktur zusammengeführt werden.

Durch die Kombination der Aufgabenbereiche und Betriebsabläufe dieser drei Bereiche in einer vollständig integrierten IT-Infrastruktur ist es für Unternehmen deutlich einfacher, einen normalen Betriebszustand ihrer Geschäftsabläufe zu erreichen, der auch tatsächlich stabil ist. Damit sind sie in der Lage:

- Den Zustand ihrer Geschäftsabläufe einfacher und effizienter zu verwalten und zu schützen, ohne dazu zusätzliche IT-Mitarbeiter einstellen zu müssen
- Kostenintensive Störungen auszuschalten, die inzwischen in vielen Unternehmen zum normalen Betriebszustand gehören
- Den Wettlauf gegen die ständig neu auftretenden Sicherheitsbedrohungen zu gewinnen, indem sie integrierte und automatisierte Prozesse einrichten, mit denen sie Schwachstellen frühzeitiger erkennen und beseitigen sowie schneller auf bösartige Angriffe reagieren können
- Nach Störungen den funktionsfähigen Betriebszustand mit einem geringeren Zeit- und Arbeitsaufwand sowie mit besseren Ergebnissen wiederherzustellen

Aspekte einer zusammengeführten Verwaltungsarchitektur

In heutigen traditionellen IT-Betriebsumgebungen mit ihren isolierten Bereichen ist die Reaktion auf Betriebsstörungen keine leichte Aufgabe. Dies soll am Beispiel einer neu auftretenden Sicherheitsbedrohung mit einer hohen Risikostufe verdeutlicht werden.

Mit der Ankündigung einer neu auftretenden Bedrohung – durch einen Sicherheitsinformationsdienst, beispielsweise Symantec DeepSight™ Alert Services oder das Symantec DeepSight™ Threat Management System, oder über die Medien – werden die normalen Abläufe im gesamten Unternehmen teilweise blockiert, während die IT-Abteilungen die Bedrohung identifizieren, die Schwachstelle ermitteln, Korrekturen planen und auf einen Angriff warten. Die IT-Mitarbeiter wenden viel Zeit für die Absicherung der Server, Desktops, Laptops und mobilen Handheld-Geräte auf. Häufig werden selbst lückenlos überwachte Prozesse und automatisierte Verwaltungsfunktionen außer Kraft gesetzt und Verteilungsaufgaben von einzelnen Experten manuell durchgeführt, um bekannte Probleme zu beseitigen und Lücken in der Infrastruktur aufzudecken. Häufigkeit und Dauer der Störungen sowie die Schäden, die in dieser Zeit verursacht werden, stellen IT-Management-Lösungen, die zum Schutz des Unternehmens und zur Abwehr schädlicher Störungen entwickelt wurden, vor neue Probleme.

Die Zusammenführung der Speicher- und Systemverwaltung und deren Integration mit der Sicherheitsverwaltung befähigt Unternehmen zu einer deutlich besseren Reaktion und schnelleren Wiederherstellung bei Betriebsstörungen, die von Sicherheitsbedrohungen, Schwachstellen und anderen Ereignissen verursacht werden. Diese Verbesserung bei der Verwaltung eines gestörten Betriebszustands wird erreicht, da Unternehmen besser in der Lage sind, folgende Aufgaben durchzuführen:

1. **Verstehen** der Informationsumgebung sowie der Schwachstellen, Bedrohungen und Angriffe, die ernsthafte Störungen verursachen können
2. **Handeln**, um proaktive Sicherheitsmaßnahmen zu ergreifen, die Bedrohungen erfolgreich abwehren, und um Möglichkeiten zu erkennen, mit denen sich Störungen vermeiden und minimieren sowie der betriebsbereite Zustand der Unternehmensdienste schnell wiederherstellen lässt
3. **Steuern** der IT-Ressourcen, um so Risiken aktiv zu verwalten und den reibungslosen Geschäftsablauf zu gewährleisten. Damit eine zusammengeführte Infrastruktur jedoch letztlich erfolgreich ist, müssen sich normale und gestörte Betriebszustände mithilfe derselben Verwaltungsinfrastruktur verwalten lassen. Gleichzeitig muss sie die beachtlichen Unterschiede bei der Reaktion und den Maßnahmen berücksichtigen, die für die Verwaltung des jeweiligen Zustands erforderlich sind (z. B. proaktives oder reaktives Patching, geplante Betriebssystemmigration oder Systemwiederherstellung nach einem Notfall usw.).

Normaler Betriebszustand

Im normalen Betriebszustand unterstützt die zusammengeführte Speicher- und Systemverwaltungsinfrastruktur, die entsprechend in die Sicherheitsverwaltungsinfrastruktur integriert ist, regelmäßig durchgeführte IT-Prozesse. Dazu gehören regelmäßige Backups nach Zeitplan, monatliche Patch-Installationen, Anwendungsaktualisierungen oder täglich anfallende Helpdesk-Reparaturmaßnahmen.

Gleichzeitig benötigen IT-Mitarbeiter Zugriff auf Informationen, die ihnen helfen, die Quelle und Art potenzieller Störungen zu verstehen. Beispielsweise liefert das weltweite Symantec DeepSight-Netzwerk mit seinen Sicherheitssensoren die notwendigen Kenntnisse und Informationen, um Unternehmen vor möglichen Störungen zu warnen.

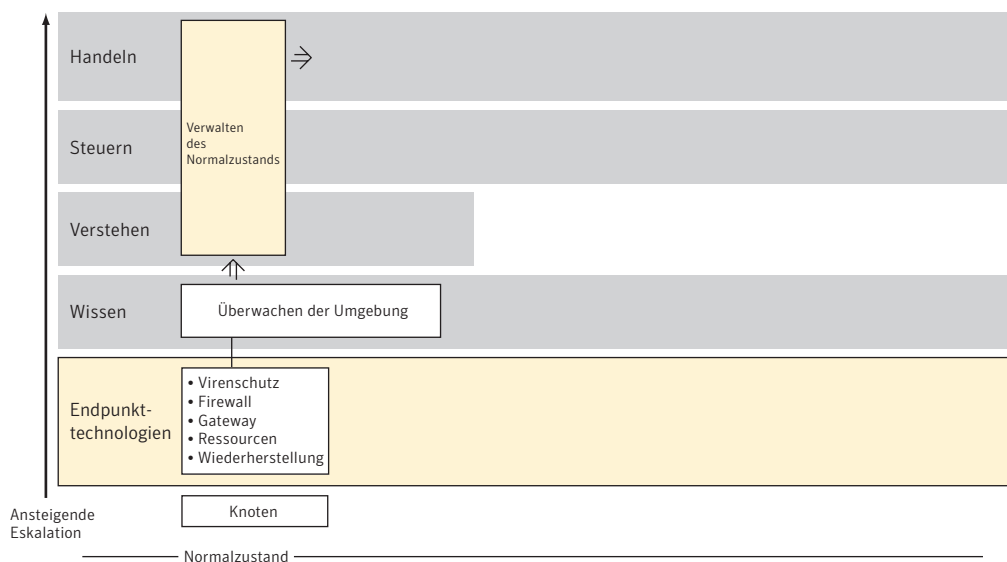


Abbildung 3. Übersicht über den normalen Betriebszustand

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Die System- und Datenwiederherstellung ist ein weiteres Beispiel für ähnliche Prozesse, die im normalen und gestörten Betriebszustand ausgeführt werden. Im normalen Betriebszustand werden häufig traditionelle Backup-Programme für die Datensicherung eingesetzt. Diese verfügen häufig jedoch nicht über Prozesse, die eine Wiederherstellung innerhalb der Zeitspanne ermöglichen, die für die meisten störenden Ereignisse erforderlich ist.

Da zahlreiche Verwaltungsaufgaben im normalen und gestörten Betriebszustand ähnlich ablaufen, kann man davon ausgehen, dass die Entwicklung einer Architektur für den gestörten Betriebszustand auch die Reaktionsfähigkeit der Verwaltungsaufgaben im normalen Betriebszustand verbessert.

Ein weiterer wichtiger Punkt: Die Verwaltung im normalen und gestörten Zustand muss unternehmensweit erfolgen. In der Übergangsphase muss die Verwaltungssoftware eine Verbindung zur gesamten Systemumgebung herstellen und diese verwalten können. Zur Systemumgebung gehören Server, Netzwerkgeräte, Desktops, Laptops, spezielle Systeme (POS, ATM) und Handheld-Geräte in vernetzten und drahtlosen Umgebungen.

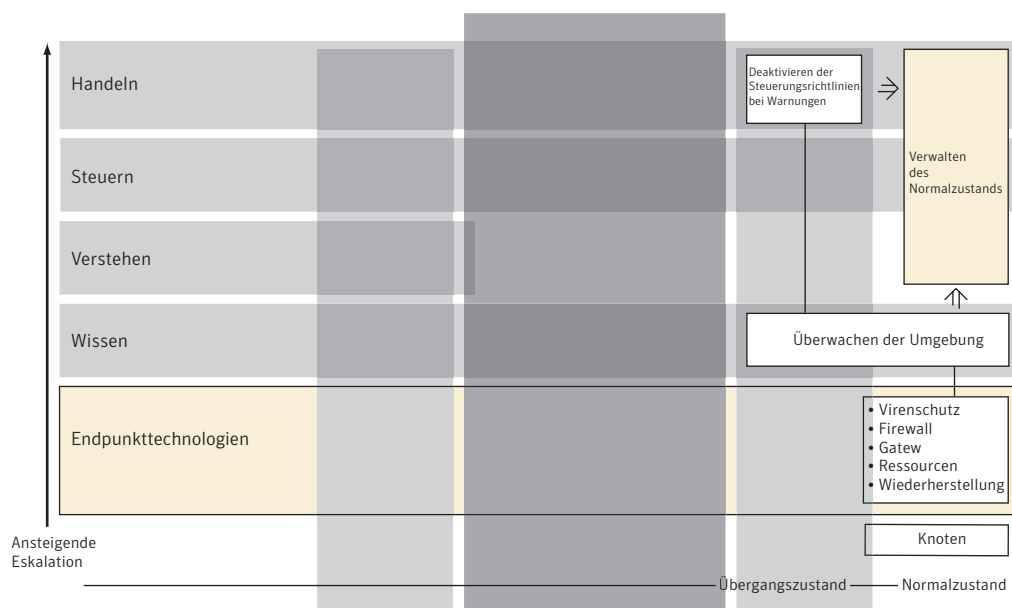


Abbildung 6. Der normale Betriebszustand der Infrastruktur wird wiederhergestellt, und der IT-Standardbetrieb wird fortgesetzt.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Wenn der Lebenszyklus eines Computers aufgrund eines unvorhergesehenen Ereignisses unterbrochen wird, muss das Verwaltungssystem in der Lage sein, seinen betriebsbereiten Zustand anhand eines vorherigen Zustands wiederherzustellen. Dieses kritische Element der Statusverwaltung wird bei der Definition des Lebenszyklus oft nicht berücksichtigt. Das bedeutet aber, die Wirklichkeit, in der Computer unvorhergesehenen und nicht kontrollierbaren Ereignissen ausgesetzt sind, zu ignorieren.

Integrierte Plattform

Symantec LiveState bietet eine einzige integrierte Plattform für die automatisierte Konfigurationsverwaltung mit Funktionen für Image-/Paketerstellung, Bestandserfassung, Softwarebereitstellung und -verteilung, Patch-Management und Systemwiederherstellung.

Die einheitliche Benutzeroberfläche vereinfacht die Einarbeitung in neue Anwendungen, so dass sich die Schulungskosten und der Zeitaufwand reduzieren lassen. Die gemeinsame Datenbank bedeutet zudem, dass neue LiveState-Anwendungen problemlos auf vorhandene Informationen über Clients (Client-Name, Betriebssystemtyp usw.) und Client-Gruppen ("Alle IIS-Server", "Alle Verkaufsmitarbeiter" usw.) zugreifen können.

Die offene und modulare Architektur der LiveState-Plattform bietet spezielle Integrationsschnittstellen zu den branchenführenden Sicherheitsverwaltungslösungen von Symantec, beispielsweise Symantec Enterprise Security Manager™ (Symantec ESM™). Der Vorteil: LiveState-Produkte können separat voneinander eingesetzt werden – zusammen mit Programmen und Prozessen, die bereits im Unternehmen vorhanden sind – oder bei Bedarf zu einer umfassenderen Lösung verbunden werden. Darüber hinaus sind Sicherheitskonfigurationsvorlagen für die Verteilung und Konfiguration von marktführenden Client-Sicherheitslösungen von Symantec vorhanden. Eine dieser Lösungen ist beispielsweise Symantec™ Client Security mit wichtigen Client-Sicherheitsfunktionen wie Virenschutz, Client-Firewall, Antispyware-Schutz und VPN-Richtlinieneinhaltung.

Zu den weiteren Funktionen der LiveState-Verwaltungsplattform gehören:

- Gemeinsame LiveState-Datenbank, die standardkonform (JDBC/ODBC), zuverlässig, skalierbar und plattformunabhängig ist und für die kein geschulter und/oder fest zugeordneter Datenbankadministrator erforderlich ist.
- Gemeinsames LiveState Agent-/Server-Protokoll, das für die sichere und effiziente Kommunikation über jede Art von vernetzten und drahtlosen Netzwerken optimiert ist. Das Protokoll enthält erweiterte Funktionen wie HTTP/HTTPS, Differenzierung auf Datei- und Byte-Ebene, Neustart ab Kontrollpunkt und Komprimierung.
- Wenn beispielsweise ein 10-MB-Patch an mobile/entfernte Computer verteilt werden muss, unterstützt das Protokoll die Übertragung des Patch in mehreren Teilen in aufeinander folgenden Sitzungen an die Geräte. Die Übertragung kann über langsame und/oder unterbrechungsanfällige Netze wie DFÜ, Frame-Relais oder drahtlose LANs in örtlichen Internet-Cafés erfolgen.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

- Konsole mit grafischer Benutzeroberfläche, die einfach zu bedienen ist und HTTP/HTTPS für die sichere und effiziente Kommunikation zwischen Konsole und Remote-Servern nutzt. Die einheitliche Konsolenoberfläche sowie benutzerfreundliche Funktionen wie Drag-and-Drop erleichtern die Einarbeitung neuer Administratoren.
- Gemeinsamer LiveUpdate™-Mechanismus für Software-Updates auf der Konsole.
- Gemeinsame Gruppen von verwalteten Servern und Clients.
- Gemeinsame Authentifizierungsdienste (Benutzername/Kennwort für Systemadministratoren).
- Gemeinsamer Dienst für die automatische Netzwerkerkennung (erkennt alle Geräte, die aktuell nicht verwaltet werden).

Die Infrastruktur für die automatisierte Verteilung von Agenten reduziert den Zeitaufwand für die Implementierung neuer Anwendungen, da die vorhandene Infrastruktur für die Verteilung neuer Anwendungs-Agenten und -Dienste genutzt wird.

Der Hauptvorteil der gemeinsamen LiveState-Plattform ist die deutliche Reduzierung der Komplexität bei der Verwaltung. Zudem können Unternehmen weitere LiveState-Anwendungen zu einem späteren Zeitpunkt problemlos zu ihrer Umgebung hinzufügen. Mit dieser innovativen Kombination aus Symantec-Lösungen lässt sich eine Unternehmensinfrastruktur verwirklichen, die deutlich einfacher zu verwalten und damit sicherer ist.

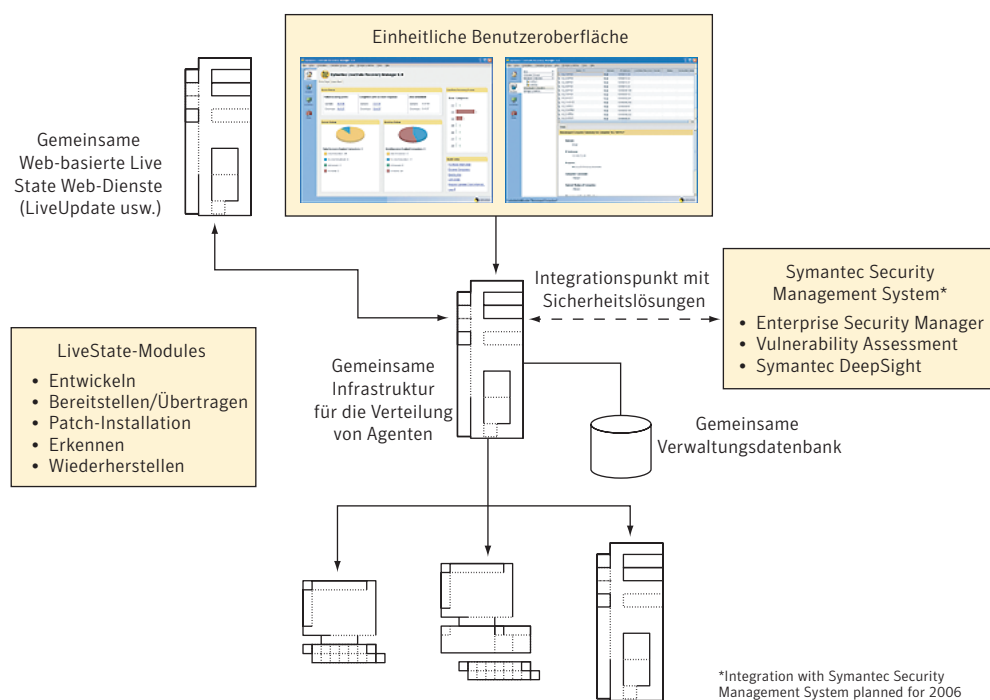


Abbildung 8. Gemeinsame Symantec LiveState-Plattform

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Symantec LiveState Management-Objekte

LiveState verwaltet hauptsächlich zwei Objekttypen. Diese beiden Elemente bilden die Kernobjekte des LiveState-Verwaltungsbetriebs:

- LiveState Image-Snapshot
- LiveState-Installationspaket

Diese Objekte bestehen aus offenen, übertragbaren und bearbeitbaren Containern und können echte und virtuelle Umgebungen darstellen. Durch diese universellen Objekte erhält LiveState die notwendige offene und skalierbare Architektur für den Einsatz in einer Vielzahl von Netzwerken, Umgebungen und Plattformen.

Symantec LiveState Image-Snapshots

Beim Erstellen von Snapshots, d. h. von Momentaufnahmen eines bestimmten Status, wird der Inhalt eines logischen Datenträgers in eine einzige übertragbare Datei kopiert. Diese Datei stellt dann einen mit einem Zeitstempel versehenen Snapshot dar, der zu einem bestimmten Zeitpunkt vom gesamten Status eines Computers erstellt wurde. Diese Snapshots können gespeichert, bearbeitet, repliziert, geladen und durchsucht werden. LiveState kann mithilfe dieser Snapshots Computer einfacher und schneller als andere Architekturen verwalten. LiveState-Snapshots können während des laufenden Betriebs als vollständige oder inkrementelle Images erstellt werden. LiveState-Snapshots werden in einer einzigen übertragbaren Datei zusammengefasst und gespeichert. Sie lassen sich daher einfach kopieren und replizieren. LiveState-Snapshots können auf jedem beliebigen lokalen oder NAS (Network-Attached-Storage)-Speichergerät gespeichert werden, ohne dass eine Neukonfiguration erforderlich ist.

Die Bearbeitung, Speicherung und Wiederherstellung von LiveState-Snapshots ist äußerst schnell und erreicht in der Regel Datenträgergeschwindigkeiten. Mit LiveState-Images lassen sich schnelle Installationen und schnelle Wiederherstellungen ausführen. LiveState-Snapshots können geladen und auf Viren überprüft werden, bevor sie eingesetzt werden. Auf diese Weise wird sichergestellt, dass sie die Umgebung nicht infizieren.

Symantec LiveState-Installationspakete

Installationspakete sind der zweite Typ von LiveState Management-Objekten. Diese Pakete enthalten ein Installationsprofil, das beschreibt, wie eine bestimmte Softwarekomponente installiert und konfiguriert werden soll. Mit LiveState-Installationspaketen lassen sich unbeaufsichtigte Installationen durchführen oder einzelne Anwendungen wiederherstellen.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

LiveState-Produktfamilie aus Lösungen für die Informationsverfügbarkeit

Die LiveState-Architektur und die entsprechenden LiveState-Anwendungen unterstützen Unternehmen bei der Verwaltung ihrer Geschäftsabläufe während normaler und gestörter Betriebszustände. Die LiveState-Produktfamilie besteht aus modularen Anwendungen für die Verwaltung des Übergangs vom normalen in den gestörten Betriebszustand und wieder zurück in einen kontrollierten und sicheren Zustand. Die Produktfamilie besteht aus fünf modularen Komponenten:

- **Installationsentwicklung:** Eine virtuelle Entwicklungsumgebung, die das Erstellen von Installations- und Wiederherstellungspaketen vereinfacht und Symantec Ghost™- und Symantec DeployCenter Library™-Images, unbeaufsichtigte Installationspakete mit dynamischer Parameterzuweisung sowie Paketformate anderer Hersteller (MSI, InstallShield usw.) unterstützt. Diese Umgebung zielt darauf ab, den für das Erstellen einer Installationsumgebung erforderlichen Arbeitsaufwand zu reduzieren und den Kenntnisstand zu verbessern.
- **Softwarebereitstellung und -übertragung:** Eine zentrale Bereitstellungsumgebung, die die lokale und per Fernsteuerung durchgeführte Installation von Computerbetriebsumgebungen wie Betriebssysteme, Anwendungen und Konfigurationswerte (z. B. Sicherheitseinstellungen) automatisiert.
- **Patch-Management:** Automatisierte Funktionen für zuverlässige Patch-Prüfungen, -Downloads und -Installationen.
- **Ressourcenverwaltung:** Automatische Netzwerkerkennung, Hardware-/Softwarebestandserfassung, Überwachung der Software- und Lizenznutzung sowie Web-basierte Berichterstellung.
- **Systemschutz und -wiederherstellung:** Zentral verwaltete und automatisierte Wiederherstellungsumgebung für lokale und Remote-Systeme. Diese Wiederherstellungslösungen auf Datenträgerbasis ermöglichen eine schnelle Wiederherstellung des betriebsfähigen Zustands.

Unsere Vision: Durch die Integration dieser Anwendungen mit den Sicherheitsinformationen, die von den weltweiten Sensornetzwerken von Symantec und den Sicherheitsverwaltungstechnologien in den Unternehmen unserer Kunden zusammengetragen werden, leistungsstarke und integrierte Verwaltungsumgebungen zu entwickeln. Mithilfe dieses integrierten Funktionsspektrums können Unternehmen normale und gestörte Betriebszustände in ihrer Infrastruktur besser verwalten. Ein Beispiel, wie dies in der Praxis aussieht, wird weiter unten in diesem Dokument beschrieben.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

LiveState-Prozessablauf

Obwohl der LiveState-Prozessablauf kein Bestandteil der LiveState-Architektur ist, stellt er dennoch einen wichtigen Aspekt der Architektur dar. Abbildung 9 beschreibt den LiveState-Prozessablauf durch die einzelnen Lebenszyklusstadien eines Systems.

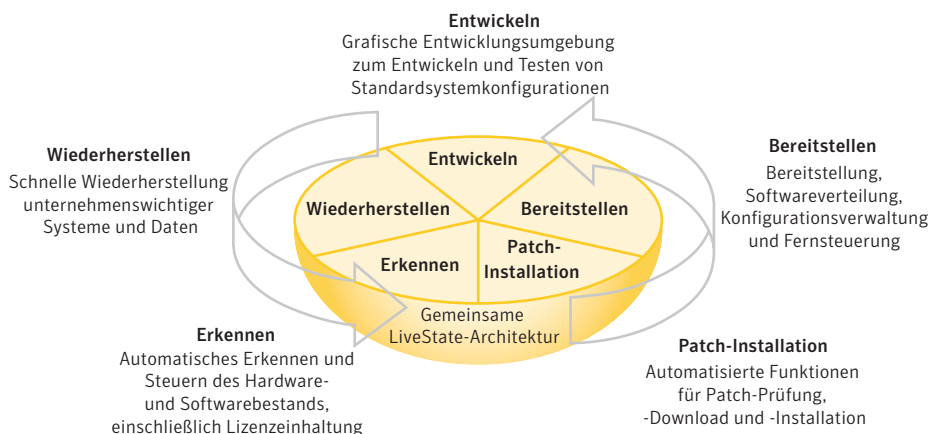


Abbildung 9. Symantec LiveState-Prozessablauf

LiveState nutzt für die Ausführung des LiveState Management-Zyklus die LiveState Management-Objekte und LiveState-Anwendungen zusammen mit den folgenden Aspekten des LiveState-Prozessablaufs:

- Symantec LiveState™ Designer (Installationsentwicklung)
- Symantec LiveState™ Delivery (Bereitstellung und Verteilung)
- Symantec LiveState™ - Patch-Manager (Patch-Installation)
- Symantec LiveState Discovery™ (Bestandserfassung)
- Symantec LiveState™ Recovery (Systemwiederherstellung)

Zusätzlich wird Symantec pcAnywhere™ für Symantec LiveState für die Helpdesk-Fehlerbeseitigung und Problembehebung auf einzelnen Computern angeboten.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Symantec LiveState Designer

Der Prozessverlauf bei der Verwaltung von Systemzuständen ist zirkulär. Als Ausgangspunkt lässt sich am ehesten die in Abbildung 9 gezeigte Paket- und Image-Entwicklung angeben.

Symantec LiveState Designer enthält alle Programme und Anwendungen, die zum Erstellen eines Modell-Image oder Installationspakets erforderlich sind. Symantec LiveState Designer verfügt über eine Reihe grafischer Programme, um Installationspakete oder Images von einem Referenzcomputer zu erstellen, die sich anschließend bearbeiten und verteilen lassen. Ein parametergestützter Ansatz reduziert den Zeitaufwand für die Paketentwicklung, da sich ein einziges Installationspaket dynamisch für mehrere Zielinstallationen konfigurieren lässt.

Bei der Installationsentwicklung können Bestandsinformationen aus Symantec LiveState Discovery herangezogen werden, um den Inhalt der LiveState-Pakete und -Images festzulegen. Die fertigen LiveState-Pakete werden in LiveState Delivery für die anschließende Zustellung an den Zielrechner registriert.

Zusammen mit den Paket- oder Image-Erstellungsprogrammen können weitere Programme eingesetzt werden. So lassen sich beispielsweise mit Symantec™ Client Migration benutzerspezifische Daten, Einstellungen und Konfigurationsinformationen extrahieren. Durch Erfassen von Benutzereinstellungen kann der Installationsentwickler eine benutzerspezifische Konfiguration von einer Installation auf eine andere übertragen. Symantec Client Migration unterstützt sowohl ein Administrator-gesteuertes als auch ein sicheres, Web-basiertes Selbstbedienungs-Tool für die Erfassung und Wiederherstellung von Benutzerdaten und -einstellungen.

Symantec LiveState Delivery

Symantec LiveState Delivery besteht aus einer skalierbaren, mehrschichtigen Architektur, mit der sich Images oder Pakete an Tausende von Systemen in einer hochgradig verteilten Infrastruktur verteilen lassen. Nach dem Erstellen eines Installationspakets oder Image eines Modellcomputers und dem Zusammenfassen des Inhalts und der Anweisungen in einem Paket wird die Verteilung des Pakets geplant. Mit Symantec LiveState Delivery lassen sich die verschiedensten Pakettypen an Zielgeräte verteilen, darunter Symantec Ghost- oder Symantec DeployCenter-Images, Anwendungsinstallationspakete, Sicherheitskonfigurationsaktualisierungen und Wiederherstellungskonfigurationen.

Symantec LiveState Delivery Enterprise Manager ist eine Zusatzanwendung der Professional Services von Symantec. Die Anwendung bietet Funktionen für eine richtliniengesteuerte Verwaltung zur Herstellung des "gewünschten" Zustands und ist eng mit Microsoft® Active Directory™ sowie anderen Unternehmensinformationsquellen wie beispielsweise SQL-Datenbanken integriert.

Symantec LiveState Delivery vereinfacht und automatisiert vorhandene manuelle IT-Prozesse. Diese Prozesse werden in unbeaufsichtigte Verfahren umgewandelt, die sich gleichzeitig auf mehreren Systemen ausführen lassen – unternehmensweit und praktisch auf allen Geräte- und Netzwerktypen. Da die Prozesse dynamisch ablaufen, wird eine hohe Flexibilität erzielt.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Symantec LiveState - Patch-Manager

Symantec LiveState - Patch-Manager stellt fest, auf welchen Geräten Patches fehlen, lädt die Patches auf einen lokalen Verwaltungs-Server herunter (zusammen mit entsprechenden Patch-Informationen aus der Unterstützungsdatenbank) und installiert anschließend die Patches sicher auf allen betroffenen Systemen.

Die Lösung bietet ein intuitives Verfahren für die Verwaltung dynamischer Client-Gruppen und der flexiblen Zeitplanung von Patch-Management-Aufgaben. Symantec LiveState - Patch-Manager nutzt das LiveState Agent-/Server-Protokoll zur effizienten Patch-Erkennung und Verteilung von Patches an lokale und mobile/Remote-Clients über Hochgeschwindigkeits- und langsame Netzwerke. Zudem erstellt LiveState-Patch-Manager zahlreiche unterschiedliche Berichte, die zur Überprüfung der Richtlinien Einhaltung herangezogen werden können.

Symantec LiveState Discovery

Symantec LiveState Discovery liefert Informationen zu den in einer vernetzten Umgebung vorhandenen Ressourcen. Anhand dieser Informationen lassen sich Zielvorgaben für die unterschiedlichsten Projekte festlegen. Diese Projekte können beispielsweise Migrationsaufgaben, Hinzukauf von zusätzlichen Speichergeräten, Durchführen von Speicheraktualisierungen, Neuzuweisen von Softwarelizenzen und Sicherstellen der Einhaltung von Unternehmensstandards auf Geräten umfassen.

Symantec LiveState Recovery

Der Symantec LiveState Recovery-Client ermöglicht das Erstellen von LiveState-Datenträger-Snapshots bei laufendem Betrieb (d. h. das System muss nicht offline geschaltet werden) von jedem Computer, auf dem der Symantec LiveState Recovery-Dienst installiert ist. Dieser aufgezeichnete Zustand sowie alle davor oder danach gespeicherten Zustände entsprechen einem zeitlichen Wiederherstellungspunkt für dieses Gerät. Mithilfe dieser zeitlichen Wiederherstellungspunkte kann LiveState Recovery verwaltete Geräte schnell wiederherstellen. Symantec LiveState Recovery kann eine komplette Systemwiederherstellung durchführen (Bare Metal Restore) oder nur einzelne Dateiodner oder -objekte wie beispielsweise wichtige Systemdateien und Treiber wiederherstellen.

LiveState Recovery unterstützt eine Reihe von Unternehmensfunktionen, beispielsweise:

- Microsoft Volume Shadow Copy Service (VSS), der für VSS aktivierte Datenbanken (z. B. Microsoft SQL Server und Microsoft Exchange) während der Snapshot-Aufzeichnung in einen "inaktiven" Modus versetzt, ohne sie offline zu schalten. (Die Ausführung benutzerdefinierter Skripte vor und nach dem Vorgang wird für nicht VSS-fähige Anwendungen unterstützt.)
- VERITAS Virtual Volume Manager (jetzt von Symantec) für die automatische Konvertierung von einfachen Datenträgern in dynamische Datenträger und umgekehrt

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

- Leistungsrosselung zur Minimierung der Auswirkungen auf Netzwerke und Benutzer
- Sichere Verschlüsselung von Image-Dateien für die Wiederherstellung, die an jeder Stelle im Netzwerk gespeichert werden können, einschließlich lokale Speichergeräte sowie NAS- und SAN-Geräte

Die Zusatzanwendung LiveState Recovery-Manager bietet zentrale und richtliniengesteuerte Verwaltungs- und Berichtsfunktionen für LiveState Recovery-Umgebungen.

Fernsteuerung

Unternehmen müssen inzwischen hochgradig verteilte Umgebungen verwalten. Darin ist es nicht immer möglich, vor Ort an einem Zielcomputer zu arbeiten. Deshalb müssen jetzt zahlreiche Funktionen, die in der Vergangenheit lokal auf ein Gerät beschränkt waren, per Fernzugriff verwaltet werden. Aktivitäten wie die Neukonfiguration, Wiederherstellung und Neuinbetriebnahme sind ein wesentlicher Bestandteil bei der Verwaltung standortferner Rechenzentren.

Seit mehr als einem Jahrzehnt ist Symantec pcAnywhere der Standard bei der Fernsteuerungssoftware. Durch die Integration mit anderen Symantec LiveState-Anwendungen wie Symantec LiveState Delivery und Symantec LiveState Recovery wird die Symantec LiveState-Architektur um leistungsstarke und sichere Funktionen für Fernzugriff und Fernverwaltung erweitert.

Beispiel: Verhindern von Angriffen und schnelles Wiederherstellen von Systemen

Die Strategie von Symantec für die Zusammenführung von Sicherheits-, System- und Speicherverwaltung zielt darauf ab, eine integrierte und ganzheitliche Unternehmenslösung zu entwickeln, die Geschäftsabläufe effektiv während normaler und gestörter Betriebszustände verwaltet.

Eine schematische Übersicht (Abbildung 10) zeigt, wie Symantec DeepSight-Warnungen das Verwaltungssystem veranlassen, gemäß vordefinierter Richtlinien zu reagieren. Diese Richtlinien wiederum lösen folgende Maßnahmen aus:

- Der Sicherheitsarbeitsablauf erhöht seine Schutzmaßnahmen.
- Der Systemarbeitsablauf sucht nach Schwachstellen und installiert Patches oder andere Abhilfen auf dem Gerät.
- Der Speicherarbeitsablauf erstellt differenziertere Symantec LiveState-Wiederherstellungspunkte.

Das System wechselt in einen gestörten Zustand, bis die Schwachstelle behoben ist. In der Zwischenzeit werden bekannte Verhaltensweisen mithilfe einer Blockiertechnologie abgewehrt. Das Speichersystem erstellt eine Wiederherstellungsposition für den Ernstfall. Die zusammengeführten Bereiche arbeiten wie ein einziges Verwaltungssystem und liefern so ein Beispiel dafür, wie die Verwaltung normaler und gestörter Betriebszustände durch ein integriertes Vorgehen gesteuert werden kann.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

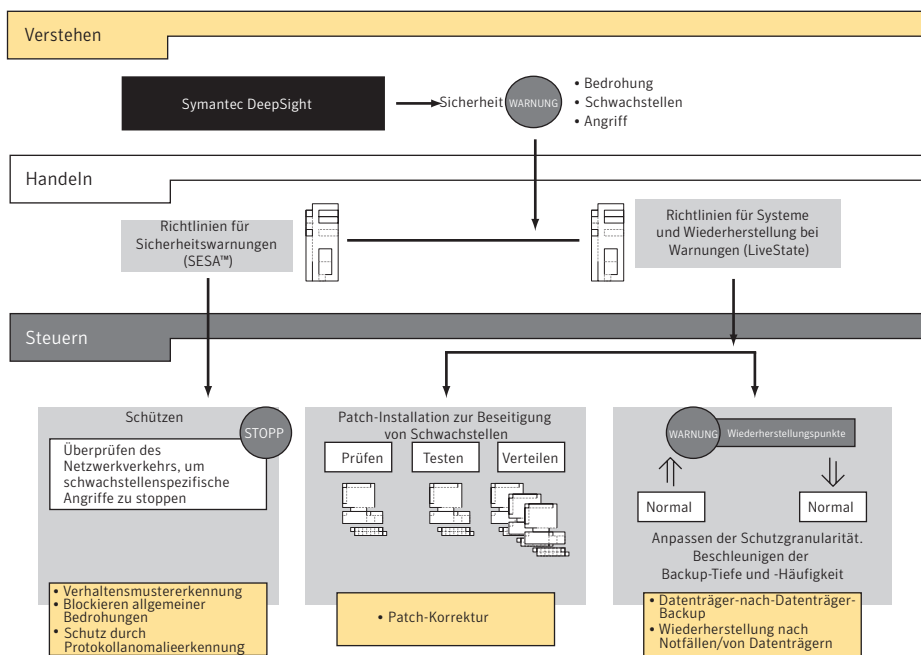


Abbildung 10. Beispiel: Angriffsprävention und Wiederherstellung

Symantec LiveState und Symantecs Strategie für die Unternehmensverwaltung

Die heutige hohe Anzahl an Bedrohungen und die zunehmende Abhängigkeit von Unternehmen von der Verfügbarkeit der von der IT-Infrastruktur verwalteten Informationen erfordern eine Zusammenführung der Speicher- und Systemverwaltung und deren Integration mit der Sicherheitsverwaltung.

Der fortlaufende Kampf zum Schutz von Unternehmen vor dem rapiden Anstieg der sich schnell ausbreitenden, bösartigen Angriffe sowie anderen Ereignissen, die zu Ausfällen führen können, erzwingt ein Umdenken bei der Verwaltung von IT-Infrastrukturen.

Die Symantec LiveState-Plattform und -Produktfamilie aus Lösungen für die Informationsverfügbarkeit unterstützt die Zusammenführung wichtiger IT-Prozesse in den Bereichen System-, Speicher- und Sicherheitsverwaltung. Dieser ganzheitliche Ansatz bei der Unternehmensverwaltung befähigt Unternehmen, stabile normale Betriebszustände mithilfe von Automatisierung und Standardisierung einzurichten sowie Störungen ihrer Betriebsabläufe erfolgreich zu beheben.

Mit dieser Strategie kann Symantec Unternehmen dabei unterstützen, den Wettlauf gegen ständig neu auftretende Sicherheitsbedrohungen zu gewinnen und die Auswirkungen von Störungen der Betriebsabläufe deutlich zu reduzieren. Unternehmen erhalten eine bessere, intelligentere und effizientere Methode, um Angriffe abzuwehren, Schwachstellen zu beseitigen und auf Ereignisse zu reagieren, die die normalen Geschäftsabläufe unterbrechen.

Symantec LiveState™ – Einheitliche Plattform zur effizienten Verwaltung des normalen und gestörten IT-Betriebs

Die Symantec LiveState-Lösungen erhöht die Widerstandsfähigkeit von Clients durch Erkennen, Bereitstellen, Konfigurieren, Patch-Installation und Wiederherstellen von Geräten im gesamten Unternehmen – einschließlich Laptops, Desktops, Handheld-Geräte und Server. Mit Symantec LiveState profitieren IT-Organisationen von Symantecs erstklassigen Technologien, um dafür zu sorgen, dass ihre wichtigen Systeme jederzeit geschützt, verfügbar und kompatibel mit den Unternehmensstandards sind – vom Kauf bis hin zur Außerbetriebnahme.

Über Symantec

Symantec ist einer der weltweit führenden Anbieter von Lösungen, mit denen Privatanwender und Unternehmen die Sicherheit, Verfügbarkeit und Integrität ihrer Daten sicherstellen können. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien, und vertreibt seine Produkte in 40 Ländern. Weitere Informationen finden Sie unter www.symantec.de.

Symantec verfügt über Niederlassungen in mehr als 40 Ländern. Die Adressen und Telefonnummern der Niederlassungen in den einzelnen Ländern finden Sie auf unserer Webseite.

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

Symantec, das Symantec-Logo, LiveUpdate und pcAnywhere sind in den USA eingetragene Marken der Symantec Corporation. Information Integrity, SESA, Symantec Client Migration, Symantec Client Security, Symantec DeepSight Alert Services, Symantec DeepSight Management Services, Symantec DeployCenter, Symantec LiveState 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 und Symantec Vulnerability Assessment sind Marken der Symantec Corporation. Microsoft, Active Directory, ActiveX und Windows sind eingetragene Marken der Microsoft Corporation in den USA und anderen Ländern. Andere Marken- und Produktnamen sind Marken der jeweiligen Rechtsinhaber und werden hiermit anerkannt. Jegliche technische Informationen, die von Symantec Corporation zur Verfügung gestellt werden, sind Eigentum der Symantec Corporation und von dieser urheberrechtlich geschützt. KEINE GEWÄHRLEISTUNG. Die technische Dokumentation wird ohne Mängelgewähr geliefert und Symantec Corporation übernimmt keine Gewährleistung für deren Genauigkeit oder Verwendung. Die Verwendung der technischen Dokumentation oder der darin enthaltenen Informationen hat der Benutzer zu verantworten. Die Dokumentation kann technische oder andere Ungenauigkeiten oder typografische Fehler enthalten. Symantec behält sich das Recht vor, Änderungen ohne vorherige Ankündigung vorzunehmen. Copyright © 2005 Symantec Corporation. Alle Rechte vorbehalten. Gedruckt in Deutschland. 7/05 WP-00069-GE