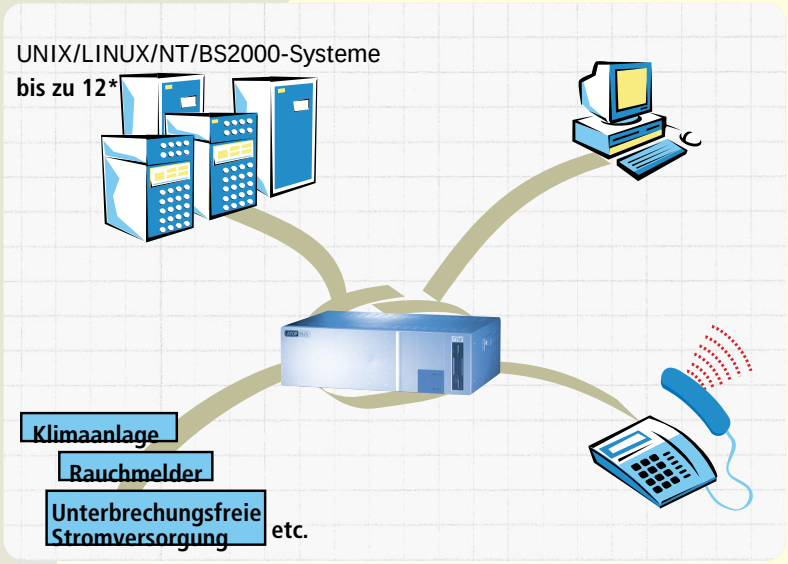
ATOP 3925 für UNIX-Server

Aktive Sicherheit im Unternehmen

Jetzt auch für alle gängigen UNIX- und LINUX-Derivate



Mit dem ATOP3925 steht Ihnen ein effektives Werkzeug zur Verfügung, das Ihnen erlaubt, die gewünschten UNIX und Linux Derivate auf Betriebssystem-ebene zu überwachen.

Zentral überwachen und managen

Der ATOP3925 ist eine zentrale, übergeordnete Instanz im Rechenzentrum, die mehrere Systeme von einer Stelle aus überwacht und steuert. Das hat den Vorteil, dass Sicherheits-maßnahmen, Alarmierungsprozeduren oder Routineabläufe nur einmal konfiguriert werden müssen. Und das funktioniert unabhängig von Systemhersteller und -plattform.

Herstellerunabhängige Sicherheitsmechanismen

Die meisten UNIX-Systeme verfügen über proprietäre Sicherheits-funktionen mit unterschiedlichen Inhalten und unterschiedlichen Mechanismen. Doch leider funktioniert das Zusammenspiel der Systeme nicht reibungslos.
Hier fungiert der ATOP3925 als übergeordnetes Security System, das allen UNIX-Systemen sämtliche Überwachungs- und Sicherheitsfunktionen zentral zur Verfügung stellt.

Ausfallsichere Verbindung

Der ATOP3925 ist direkt an einer Konsolschnittstelle mit den UNIX-Rechnern verbunden. Diese Sicherheit ist unerlässlich gerade bei unternehmenskritischen Systemen. Denn der Ausfall von zentralen Servern verursacht hohe Kosten.

Entlastung von Routinetätigkeiten

Der ATOP3925 "fühlt" in einstellbaren Zeitabständen den Puls von Betriebssystem und Anwendung und informiert recht-zeitig per Sprachausgabe auf Telefon oder Lautsprecher über kritische Bereiche. Das gibt Ihnen den nötigen Vorsprung, einem "Infarkt" des Systems entgegenzuwirken.

Notfallpläne sofort parat

Um für alle möglichen Ereignisse gewappnet zu sein, werden spezielle Notfallpläne ausgearbeitet und im ATOP3925 hinter-legt. Da die Notfallpläne jederzeit startklar sind, reagiert er sofort, ohne jede Zeitverzögerung und startet entsprechende Maßnahmen.

Gesicherte Sprachalarmierung

Per Lautsprecher, Telefon oder Handy erreicht der ATOP3925 immer den Richtigen. Die Alarmierungsprozedur unterliegt strengsten Sicherheitsvorkehrungen: der Empfänger muss sich indentifizieren und den Empfang jeder Nachricht quittieren, individuelle Alarmierungspfade und Eskalationsstufen werden bei Nichterreichbarkeit berücksichtigt.