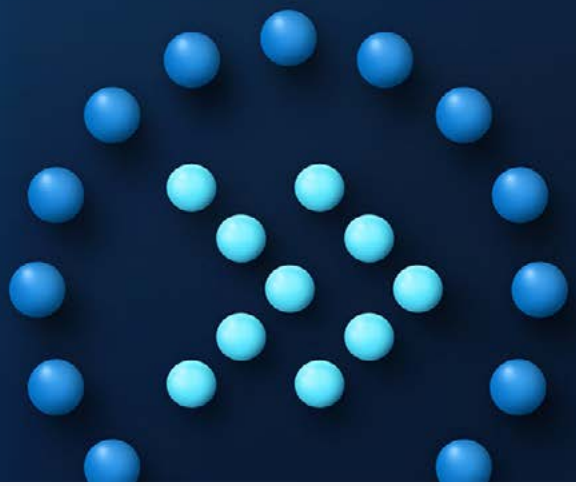
Microsoft

Windows Server 2012

End of Support– JETZT auf Windows Server 2022 umsteigen



Im Oktober 2023 endet der Support für Windows Server 2012 und Windows Server 2012 R2. Das Datum scheint jetzt noch in weiter Ferne zu sein, aber es ist nur von Vorteil, sich jetzt schon um einen geeigneten und verfügbaren IT-Partner zu kümmern.

Weltweit werden 59% aller Windows Server von 2003-2008R2 nicht mehr supportet, allein in Deutschland sind noch 60.000 Windows Server 2008 / 2008 R2 im Einsatz. Diese veralteten Systeme sind gefährlich und stellen ein großes Sicherheitsrisiko für Ihr Unternehmen und Ihre Daten dar. Außerdem werden die Bedrohungen immer ausgereifter und vielseitiger, Ihr Server sollte darauf vorbereitet sein.

Mit dem neuen Windows Server 2022 machen Sie einen großen Schritt in Richtung Absicherung Ihrer Daten und Gewährleistung Ihrer Produktivität.

Hybridfunktionen mit Microsoft Azure

Die Kombination aus lokaler Infrastruktur und Hybridfunktionen vereinfacht den Weg in die Cloud.

Fortschrittliche, mehrschichtige Sicherheit

Die im Betriebssystem integrierten Sicherheitsfunktionen schützen die Daten und Apps Ihres Unternehmens.

Höherer Schutz bei Remote-Zugriffen

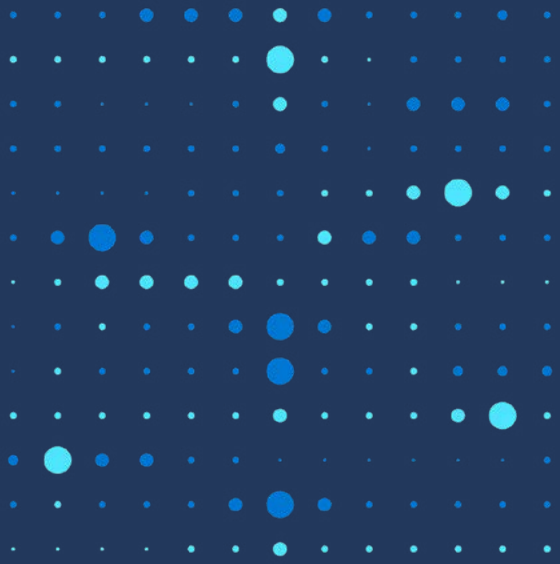
Dank vereinfachter Bereitstellung und optimierter Verwaltung von Remote-Apps und -Desktops erleichtern Sie Ihren Mitarbeitern die Arbeit.

Modernisierte Serverinfrastruktur

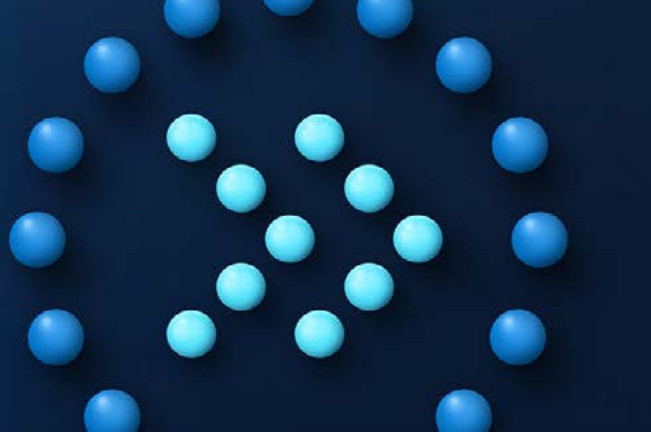
Indem Sie Ihre Windows Server Software Defined (WSSD) Datacenter mithilfe von Windows Server 2022 realisieren, profitieren Sie von einer höheren Skalierbarkeit, mehr Sicherheit und einer besseren Kosteneffizienz.

Starten Sie jetzt durch!

Windows Server 2022 als Basis für Ihre Zukunft.



Microsoft



Der neue Windows Server 2022 bietet jede Menge **Security-Features** (Secured Core-Sicherheitsfunktionen) für die Firmware und das Betriebssystem, die vor modernen Bedrohungen schützen.

Mithilfe von Advanced Threat Protection (ATP) lassen sich Zero-Day-Schwachstellen, Angriffe auf das Netzwerk und Datenlecks unterbinden und erkennen.

Präventive Abwehrmechanismen schützen sensible Informationen, indem fortschrittliche Malware, die das System manipulieren will, frühzeitig erkannt und abgewehrt wird.

Die virtualisierungsbasierte Sicherheit (VBS) schützt vor Angriffen, die Schwachstellen im Betriebssystem ausnutzen wollen, um Malware einzuschleusen.

Schnell und unkompliziert eine End-to-End-Verschlüsselung realisieren, um zu verhindern, dass Ihre Daten in nicht vertrauenswürdigen Netzwerken ausgespäht werden können.

Daten verschlüsseln und dabei auf Transport Layer Security (TLS) 1.3 setzen, sichert die Kommunikation zwischen zwei Endpunkten ab.

Windows Defender Exploit Guard unterbindet auf den Host zielende Eindringversuche

Modernisieren Sie jetzt Ihre Server-Landschaft und erhöhen Sie das Sicherheits-Level zum Schutz Ihrer Daten und Handlungsfähigkeit. Weitere Informationen finden Sie hier:

Zu den technischen Informationen **Zur Website**