Cyberresistenz

Vom Rand zur Cloud

Förderung der Cyberresilienz durch umfassenden Schutz und Datensicherheit

Mit der erweiterten Sicherheit für Computer, Server und andere Endpunkte sowie Backup- und Wiederherstellungsdiensten sind Ihre Tage, in denen Sie sich Sorgen über den Verlust geschäftskritischer Daten machen müssen, vorbei.

Leistungsstarker Schutz. Einfache Wiederherstellung. Auf diese Weise ermöglichen Carbonite und Webroot cyberresilienten Unternehmen, angesichts von Cyberkriminalität und Datenverlust furchtlos zu sein. Zusammen stellen diese Lösungen sicher, dass Unternehmen leistungsfähig bleiben, egal was auf sie zukommt.

Das Carbonite & Webroot Portfolio

Carbonite® Endpoint
Carbonite Endpoint ist eine umfassende, automatische Backup-Lösung für Endpunktgeräte und die darauf gespeicherten Daten. Carbonite Endpoint vereinfacht die Verwaltungsaufgaben, die mit der Bereitstellung des Schutzes im gesamten Unternehmen verbunden sind, unabhängig von der Größe, Verteilung oder Komplexität der Umgebung.

Mit Carbonite® Endpoint können Unternehmen wertvolle Daten auf den Geräten ihrer Mitarbeiter besser schützen, Datenverluste und Datenverstöße minimieren sowie verlorene Daten schnell wiederherstellen. Es bietet Unternehmen eine verbesserte Strategie für die Ausfallsicherheit von Daten durch erstklassigen Schutz, um das Risiko von Ransomware, Benutzerfehlern und Verlust oder Diebstahl von Geräten zu verringern.

Carbonite® Backup für Microsoft® 365
Carbonite Backup für Microsoft 365 bietet eine umfassende Sicherung aller Microsoft 365-Anwendungen, um den Datenschutz und bei Bedarf die Wiederherstellung zu gewährleisten. Mit der zentralen Verwaltung können Sie granulare Richtlinien für die zu schützenden Elemente erstellen und bis zu vier Mal pro Tag Backups mit flexiblen Aufbewahrungsoptionen ausführen.

Sie können granulare Daten wie Postfächer, Konversationen, Projekte und mehr wiederherstellen sowie ein Rollback auf Standortebene durchführen, um verlorene Daten einfach wiederherzustellen. Mit dieser Cloud-zu-Cloud-Backup-Lösung können Unternehmen für Cloud-Apps denselben robusten Datenschutz bereitstellen wie für physische, lokale Geräte und Daten.

Carbonite® Server
Alle Unternehmen benötigen eine unkomplizierte, umfassende Backup- und Wiederherstellungslösung, die dazu beiträgt, Daten sicher zu halten, Ausfallzeiten zu minimieren und Unternehmensabläufe zu schützen. Carbonite Server ist eine zuverlässige Gesamtlösung für Server-Backup und -Wiederherstellung für physische, virtuelle und Altsysteme. Zu den erweiterten Funktionen gehören:

Carbonite und Webroot bieten Ihnen das umfassendste Online-Sicherheitsangebot, das es gibt. Gemeinsam haben wir die Möglichkeit, Cyberkriminalität zu bekämpfen und Benutzer vor dem Verlust wertvoller Daten zu schützen.

Wir sind bestrebt, Ihr Komplettanbieter für Cyberresilienz für Unternehmen durch Cyber-Sicherheit, Datenschutz und Wiederherstellung zu werden. Unsere aktuellen Angebote umfassen:

- Carbonite® Server
- Carbonite® Endpoint
- Carbonite® Backup für Microsoft® 365
- Carbonite® Migrate
- Carbonite® Recover
- Carbonite® Availability
- Carbonite Safe®
- Webroot® Endpunktschutz für Geschäftskunden
- Webroot® DNS-Schutz
- Webroot® Schulung zur Steigerung des Sicherheitsbewusstseins
- Webroot BrightCloud® Threat Intelligence Services

- Sichere lokale und Cloud-Backups mit optionaler, integrierter Hardware, alles von einem Anbieter
- Cloud-Failover mit Ausfallsicherung auf Knopfdruck für kritische Systeme
- Granulare Wiederherstellung (Dateien, Ordner, Exchange, SharePoint, SQL, Active Directory, Oracle DB)
- Für immer inkrementelle Backups mit flexiblen Aufbewahrungsoptionen bis zu sieben Jahren

Carbonite® Migrate
Carbonite Migrate migriert schnell und einfach physische, virtuelle und Cloud-Arbeitslasten mit minimalem Risiko und fast ohne Ausfallzeiten. Der optimierte Prozess automatisiert und konsolidiert zahlreiche Schritte in nur wenigen einfachen Aufgaben und reduziert den Arbeitsaufwand, der zum Erreichen Ihrer Migrationsziele erforderlich ist. Die Funktionen umfassen:

- Strukturierte, wiederholbare Migration fast ohne Ausfallzeiten
- Hochautomatisierter Prozess, der häufige Risiken eliminiert und Migrationen rationalisiert
- Festlegung auf eine bestimmte Cloud, einen Hypervisor oder eine bestimmte Hardware ist nicht nötig

Carbonite® Recover
Carbonite Recover ist ein DRaaS-Angebot, das kritische Systeme sicher von einer primären Umgebung in die Carbonite-Cloud repliziert. Dies stellt sicher, dass jederzeit eine aktuelle Sekundärkopie für das Failover verfügbar ist, wodurch Ausfallzeiten und Kosten minimiert werden. Die Funktionen umfassen:

- Wiederherstellungszeiten in Minuten und Wiederherstellungspunkte in Sekunden, wodurch das Risiko von Produktivitäts- und Umsatzverlusten verringert wird
- Kontinuierliche Echtzeitreplikation für immer aktiven Datenschutz
- Unterbrechungsfreie Self-Service-Tests
- Bandbreitenoptimiert für begrenzte Auswirkungen auf das Netzwerk

Carbonite® Availability
Mit Carbonite Availability können Unternehmen die höchste Verfügbarkeit ihrer Windows® und Linux-Server sicherstellen, indem sie Ausfallzeiten und Datenverlust verhindern. Die kontinuierliche Replikation auf Byte-Ebene erzeugt eine sekundäre Kopie, ohne das primäre System oder die Netzwerkbandbreite zu belasten. Zu den erweiterten Funktionen gehören:

- Kontinuierliche Replikation, die Datenverlust minimiert
- Unglaublich schnelle Failover, die Ausfallzeiten minimieren
- Plattformunterstützung für physische, virtuelle und Cloud-basierte Systeme
- Automatisches Failover, ausgelöst durch Schwellenwertuntersuchungen

Carbonite Safe®
Sichern Sie Computer und Server automatisch in der Cloud mit Optionen zum lokalen Schutz von Dateien für eine schnellere Wiederherstellung. Carbonite Safe ist so konzipiert, dass es von Privatkunden und Home-Offices bis hin zu kleinen Unternehmen mit einem oder mehreren Servern skalierbar ist.

Webroot® BrightCloud® Threat Intelligence
Die Webroot® Plattform ist die Architektur, die jede Ebene unserer Lösungen für Verbraucher und Unternehmen enthält, genau wie unsere BrightCloud® Threat Intelligence Services für Technologiepartner, darunter:

- Webklassifizierung und Web-Reputation
- IP-Reputation
- Anti-Phishing in Echtzeit
- Sicherheit für Mobilgeräte SDK
- Datei-Reputation
- Streaming Malware Detection

Webroot® Endpunktschutz für Geschäftskunden
Die Grundlage einer fortschrittlichen Cyberresilienz-Strategie besteht in einem hochwirksamen Multi-Vektor-Schutz und in der Prävention. Cyberresilienz beginnt damit, die Angriffe auf Endpunkte und deren Benutzer zu stoppen. Fortschrittlicher, automatisierter Webroot Endpunktschutz der nächsten Generation für Geschäftskunden:

- Stoppt Malware, Ransomware, bekannte und unbekannte Infektionen
- Schützt vor dateibasierten und dateilosen Skripten, APTs, Exploits und Ausweichangriffen
- Stoppt Phishing und den Benutzeridentitäts- und Legitimationsdiebstahl
- Korrigiert lokale Endpunkt-Laufwerke automatisch und versetzt sie in den Zustand vor der Infektion, ohne ein neues Image zu erstellen

Webroot® DNS-Schutz
Jedes Unternehmen nutzt das Internet und jede Internetverbindung verwendet DNS. Wenn Sie nicht alle DNS-Anforderungen privat und sicher filtern, ist Ihr Unternehmen gefährdet. Die nächste Ebene einer umfassenden Strategie für Cyberresilienz muss die Sicherheit auf Domänenebene sein, die sowohl Datenschutz als auch Sicherheit bietet, indem DNS über HTTPS (DoH) unterstützt wird. Webroot DNS-Schutz:

- Filtert automatisch DNS- und DoH-Anforderungen an schädliche und gefährliche Domänen und blockiert 88 % der bekannten Malware, bevor sie Ihr Netzwerk oder Ihre Endpunkte erreichen kann*
- Stellt private DNS-Resolver in Google Cloud™ zur Verfügung, um die Überwachung von Internetnutzungsanfragen zu stoppen, die von Übeltätern oder solchen, die Daten für Profitzwecke ausbeuten, angefordert wird

- Bietet Netzwerk-, IP-Adress- und Benutzerrichtlinienverwaltung über Bandbreite und unproduktiven oder nicht konformen Internetzugang unter Verwendung von 80 URL-Kategorien
- Verwendet die aktuellsten, genauesten und zuverlässigsten DNS-Filterinformationen, die vom Webroot BrightCloud® Webklassifizierungsdienst unterstützt werden

Webroot® Schulung zur Steigerung des Sicherheitsbewusstseins

Wenn Benutzer unabsichtlich vertrauliche Informationen preisgeben oder auf den falschen Link klicken, können Kriminelle Sicherheitsebenen umgehen und erfolgreich in Netzwerke eindringen. Aus diesem Grund erfordert Cyberresilienz Cyber-Bewusstsein. Die hochautomatisierte Webroot Schulung zur Steigerung des Sicherheitsbewusstseins liefert messbare Ergebnisse mit minimalem Aufwand durch:

- Fortbildungsprogramme, die Mikrolernen, Phishing-Simulationen mit Effektivitätsmessung und Berichterstattung für Führungskräfte kombinieren
- Spezielle Compliance-Kurse für PCI, HIPAA, GDPR und mehr
- Kursmaterialien und Phishing-Vorlagen, die ständig aktualisiert werden, damit sie für die Schulung der Benutzer und die Änderung des Verhaltens relevant und effektiv sind
- Nachgewiesene Effektivität bei der Reduzierung der Klickraten und der Minimierung von Sicherheitsvorfällen

Nächste Schritte

Weitere Informationen zu Carbonite- und Webroot-Produkten finden Sie unter webroot.com und carbonite.com.

Kontaktieren Sie uns, um mehr zu erfahren – Carbonite EMEA

E-Mail: carb-salesemea@opentext.com

Telefon: Frankreich: +33 1 47 96 55 41 | Deutschland: +49 2162 91980 20 | Niederlande: +31 73 648 1400 | Großbritannien: +44 333 1234 200

Für alle anderen Länder wählen Sie bitte: +44 333 1234 200

Kontaktieren Sie uns, um mehr zu erfahren – Webroot EMEA

E-Mail: carb-salesemea@opentext.com

Telefon: 1 800 303 388

Kontaktieren Sie uns, um mehr zu erfahren – Webroot APAC

E-Mail: carb-apac_sales_team@opentext.com

Telefon: 1 800 013 992

* Basierend auf den internen Tests und Bedrohungen von Webroot, die von Webroot nach dem Scannen des realen Netzwerkverkehrs identifiziert wurden.

Über Carbonite und Webroot

Carbonite und Webroot, OpenText-Unternehmen, nutzen die Cloud und künstliche Intelligenz, um Unternehmen, Einzelpersonen und Managed Service Providern umfassende Lösungen für mehr Cyberresilienz anzubieten. Cyberresilienz bedeutet, dass Systeme trotz Cyberangriffen und Datenverlusten jederzeit aktiv und betriebsbereit sind. Mit diesem Ziel haben wir unsere Kräfte gebündelt, um Endpunktschutz, Netzwerkschutz, Schulungen zur Steigerung des Sicherheitsbewusstseins, Datensicherungs- und Notfallwiederherstellungslösungen sowie Threat Intelligence Services bereitzustellen, die von marktführenden Technologieanbietern weltweit verwendet werden. Webroot nutzt die Leistungsstärke des maschinellen Lernens zum Schutz von Millionen von Unternehmen und Einzelpersonen und sichert die vernetzte Welt. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie unter carbonite.com und webroot.com mehr über Cyberresilienz.