Acronis Protected Workspace: Schutz für die größte Schwachstelle

Laptops, Desktops und Workstations sind zwar unverzichtbare Arbeitsgeräte, sie bergen jedoch auch erhebliche Sicherheitsrisiken. Da die Mitarbeitenden sie überall nutzen, sind sie einer Vielzahl von Bedrohungen ausgesetzt.

Für Managed Service Provider (MSPs) sind diese Geräte die wichtigsten, aber auch die am stärksten gefährdeten Ressourcen, die es zu schützen gilt. Ihr Schutz ist allerdings schwierig, da MSPs dafür häufig mehrere Tools einsetzen müssen. Wenn diese Tools nicht nativ integriert sind, kann es äußerst problematisch sein, sie miteinander zu kombinieren. Das kann zu Sicherheitslücken führen.

Darüber hinaus bedeutet die Verwaltung mehrerer Tools, dass mit unterschiedlichen Benutzeroberflächen gearbeitet werden muss. Das erhöht die Komplexität, schafft neue Risiken und erfordert oft spezielle Fachkenntnisse. Sicherheitsinfrastrukturen für Workspaces, die aus mehreren Einzellösungen bestehen, erhöhen zusätzlich die Betriebskosten, schaffen Ineffizienzen und verschlechtern insgesamt den Schutz.

Da Cyberkriminelle KI als Waffe einsetzen, um nahezu unbegrenzte Angriffsvarianten zu entwickeln, kommt es mittlerweile täglich zu Zero-Day-Angriffen. Dabei steht viel auf dem Spiel: Erfolgreiche Angriffe führen zu Ausfallzeiten, Produktivitätsverlusten und Reputationsschäden – sowohl für MSPs als auch für ihre Kund:innen. Hinzu kommen Probleme mit der Compliance, die in vielen Branchen entstehen.

Nativ integrierte Sicherheit, Data Protection und Endpunktverwaltung für Workspaces

Geschäftliche Herausforderungen beim Schutz von Workspaces für MSPs

Da vielen Unternehmen die erforderlichen Ressourcen fehlen, um die Sicherheit ihrer Workspaces selbst zu verwalten, wenden sie sich diesbezüglich an MSPs. Sie benötigen einen Service Provider, der alle Laptops und Desktop-PCs an jedem Ort so schützt, dass die Daten sicher sind, die Produktivität aber nicht beeinträchtigt wird.

Für Service Provider gestaltet sich diese Aufgabe schwierig, da die Geschäftstätigkeit ihrer Kund:innen von hoher Geschwindigkeit und globaler Ausrichtung geprägt ist. Ein Teil des Problems ist die Größenordnung. MSPs müssen eine riesige Angriffsfläche schützen, die durch Hunderte oder Tausende von Geräten entsteht. Schon ein einziger kompromittierter Endpunkt kann zu einem Cyberangriff führen, durch den der gesamte Geschäftsbetrieb der Kund:innen zum Erliegen kommt.

Unternehmen haben häufig auch Mitarbeitende, die Geräte an verschiedenen Standorten verwenden und Daten rund um den Globus versenden. Remote-Arbeitsplätze stellen eine zusätzliche Herausforderung für den Schutz von Workspaces dar. Die hohe Mobilität der Geräte, weltweite Geschäftsaktivitäten und die Erwartung schneller Reaktionen machen die Geräte der Mitarbeitenden sehr anfällig für Cyberangriffe. In Branchen wie dem Gesundheits- und Finanzwesen können unzureichend gesicherte Workspaces zudem die Einhaltung gesetzlicher Vorschriften gefährden.

Was den Workspace-Schutz für MSPs so schwierig macht

Der Schutz von Workspaces ist für MSPs besonders herausfordernd, da Cybersicherheitstools, die Geräte schützen, nicht die Effizienz bieten, die Service Provider benötigen. Eine fragmentierte Infrastruktur, bei der Virenschutz, Backup und Remote Monitoring and Management (RMM) beispielsweise in verschiedenen Applikationen getrennt voneinander zu finden sind, macht den Schutz von Workspaces kostspielig und fehleranfällig.

Für jede Schutzkomponente ist eine eigene Softwarelösung und Konfiguration erforderlich. Die Anzahl der Kombinationsmöglichkeiten auf verschiedenen Geräten ist dabei praktisch unbegrenzt. MSPs benötigen Personal, um alle Einzellösungen zu verwalten. Sie müssen entweder mehrere Techniker:innen einstellen oder Zeit investieren, um ihre Techniker:innen in der Verwendung vieler getrennter Lösungen zu schulen – und hoffen, dass ihnen dabei keine Fehler unterlaufen.

Die Verwaltung unterschiedlicher Tools in mehreren Konsolen führt zu langsamen Reaktionszeiten und überlasteten Techniker:innen, die Fehler machen. Darüber hinaus besteht das Risiko von fehlerhaften Integrationen, die erhebliche Sicherheitslücken verursachen können.

Da Workspaces nur selten vollständig ausgeschaltet werden, sind sie ein permanentes Ziel für Cyberangriffe. Zudem vertrauen die Mitarbeiter:innen von Kundenunternehmen ihren Geräten häufig zu sehr, wodurch eine zusätzliche Schwachstelle entsteht. Um Workspaces zu schützen, benötigen MSPs eine Lösung, die umfassende Sicherheitsfunktionen bietet und sich gleichzeitig einfach verwalten lässt.

„Eine fragmentierte Infrastruktur für die Workspace-Sicherheit hat in vielen Unternehmen zu höheren Betriebskosten, größerer Komplexität und weniger effektiven Sicherheitsmaßnahmen geführt.“

Gartner, 2025 Strategic Roadmap for Workspace Security

Acronis Protected Workspace ist eine speziell für MSPs entwickelte Lösung

Acronis Protected Workspace umfasst eine Reihe nativ integrierter Services, mit denen MSPs die Geräte ihrer Kund:innen mit minimalem Risiko und maximaler Effizienz schützen können. Die Services sind pro Workload oder pro Gigabyte verfügbar und umfassen:

Services in Acronis Protected Workspace

Acronis Backup für Workstations	Speichert und schützt die Daten auf Kundengeräten (Laptops, Desktops und Workstations).
Acronis Advanced Backup für Workstations	Erweitert die Cloud-Backup-Funktionen, um die Workspace-Daten von Kund:innen in mehr als 20 Workload-Typen zu schützen. Dieser proaktive Schutz eliminiert Ausfallzeiten nahezu vollständig.
Acronis Endpoint Detection and Response (EDR)	Überwacht Endpunkte aktiv, stoppt Angriffe, bevor sie Schaden anrichten können, und ermöglicht die Wiederherstellung mit einem einzigen Klick.
Acronis Extended Detection and Response (XDR)	Bietet vollständigen aktiven Schutz, der entwickelt wurde, um Vorfälle schnell zu verhindern, zu erkennen, zu analysieren, darauf zu reagieren und Daten wiederherzustellen.
Acronis Remote Monitoring and Management (RMM)	Ein erstklassiger Verwaltungs- und Überwachungsservice mit einem sicherheitsorientierten Ansatz. Automatisieren und beschleunigen Sie alle Prozesse mithilfe von KI und ML in Verbindung mit einer leistungsstarken Scripting-Engine. Entdecken und schützen Sie mit Device Sense™ miteinander verbundene Workspaces.
Acronis Data Loss Prevention (DLP)	Verhindert Datenlecks von Endpunkten, ohne dass eine komplexe Installation oder spezielle Datenschutzkenntnisse erforderlich sind.
Acronis Active Protection	Schützt aktiv alle Daten auf den Kundensystemen, einschließlich Dokumente, Mediendateien, Programme usw.
Acronis Malware-Schutz	Schützt Kundensysteme proaktiv und in Echtzeit vor komplexen Cyberangriffen. Dazu kommen KI-basierte statische und verhaltensheuristische Technologien zum Einsatz, die vor Viren, Malware und Ransomware schützen.

MSPs haben auch die Möglichkeit, sich für lösungsbasierte Pakete zu entscheiden:

Workstation Backup	Endpunktschutz + RMM	Ultimate Protection
Acronis Backup für Workstations inklusive 300 GB Storage	Acronis Active Protection	Paket: Security + RMM
	Acronis Malware-Schutz	Paket: Backup + Cloud-Storage
	Acronis EDR	Acronis Advanced Backup
	Acronis XDR	Acronis DLP
	Acronis RMM	

Die Vorteile von nativ integriertem Workspace-Schutz

Um Workspaces zu schützen, zu verwalten und wiederherzustellen, benötigen MSPs eine einheitliche, effiziente und gewinnbringende Vorgehensweise. Acronis Protected Workspace bietet MSPs alle erforderlichen Services zum Schutz von Workspaces in einer einzigen, nativ integrierten Lösung. Diese ermöglicht es, alles mit einem einzigen Agenten und einer einzigen Lizenz von einer zentralen Konsole aus zu verwalten. Mit diesem einfachen, aber wirkungsvollen Konzept können Techniker:innen mehr Workspaces besser schützen und verwalten.

Acronis Protected Workspace bietet auch die folgenden Vorteile:

- **Native Integration** mit Endpunktschutz, RMM und Backup in einer einzigen Konsole.
- **Umfassender Schutz** durch KI-gestützte Anti-Malware, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Ransomware-Erkennung und Verhaltensanalyse. Der Schutz entspricht dem NIST Cybersecurity Framework.
- **Effiziente Arbeitsabläufe** durch schnelleren Ticketabschluss, besseren Kundenservice und geringere Schulungskosten.
- **Flexibilität** durch MSP-freundliche Lizenzmodelle, die die Zusammenstellung individueller Schutzpakete ermöglichen.

„Acronis ist unsere Kernplattform und deckt alle Bereiche ab. Die Effizienz, die Acronis bietet, ist unübertroffen. Wir sparen Zeit, reduzieren Kosten und minimieren den Schulungsaufwand. Da alles in einer einzigen Konsole zusammengefasst ist, lässt sich unser Portfolio nahtlos und effektiv verwalten."

– Joshua Aaronson, Mitgründer von Panda Technology

Acronis Protected Workspace ist die All-in-one-Lösung für MSPs zum Schutz von Geräten

Mit Acronis Protected Workspace können MSPs die Herausforderungen bewältigen, die der Schutz von Laptops, Desktop-PCs und Workstations mit sich bringt, ohne dabei unterschiedliche Sicherheitslösungen verwalten zu müssen. Service Provider können sich durch besseren Schutz, schnellere Reaktionszeiten und einen erstklassigen Kundenservice von der Konkurrenz abheben.

Erleben Sie Acronis Protected Workspace in Aktion

KONTAKT

Acronis

Weitere Informationen finden Sie auf www.acronis.com.