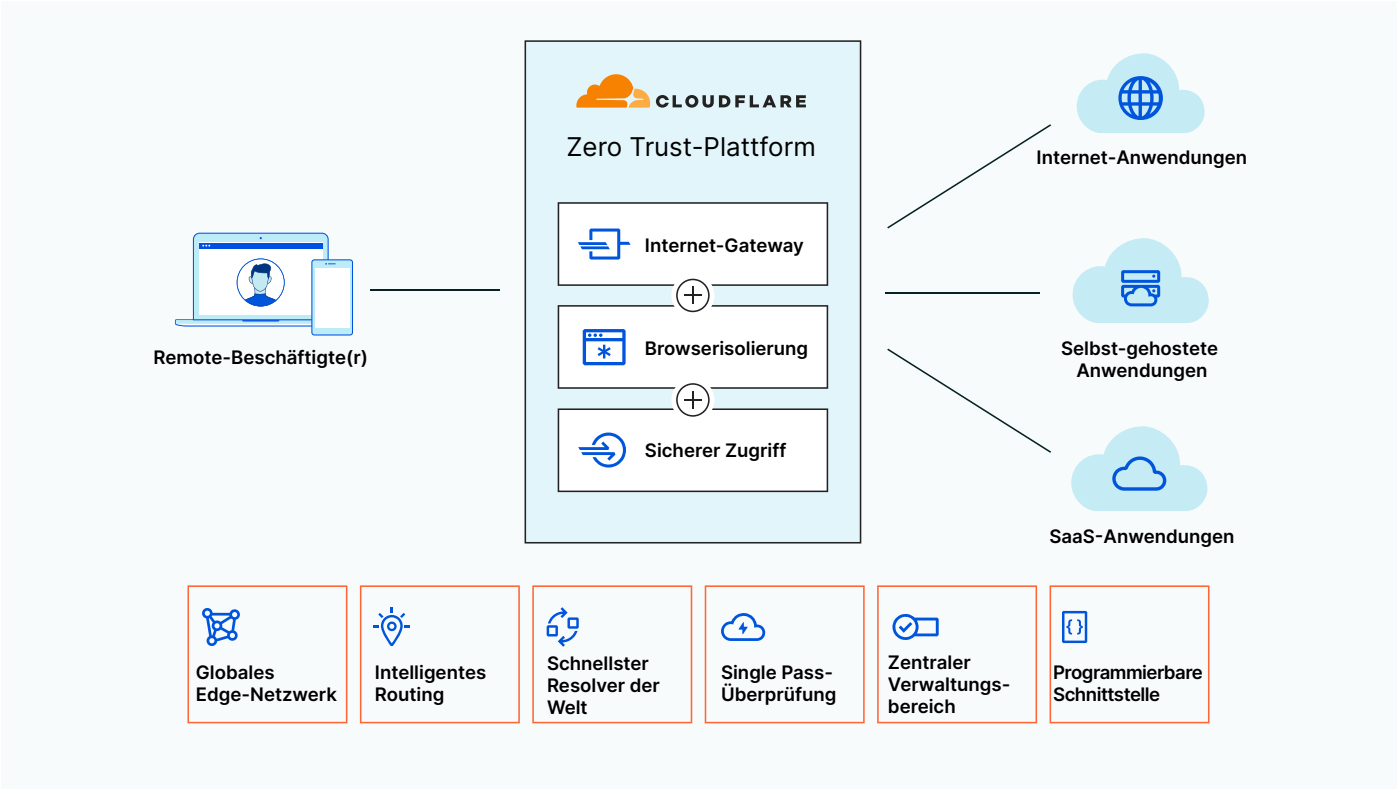
Anbindung von Remote-Beschäftigten mit Cloudflare langfristig gewährleisten

Als die Coranavirus-Pandemie von heute auf morgen die Umstellung auf Remote-Arbeit erzwang, mussten Unternehmen alles daransetzen, dass Ihre Mitarbeiter weiterhin auf ihre Systeme zugreifen konnten. Manche Lösungen wurden aus strategischen Erwägungen heraus gewählt, doch bei anderen handelte es sich um taktische Notbehelfe. Dazu zählte etwa die Beibehaltung langsamer und unzuverlässiger VPN-Verbindungen, das Spilt-Tunneling von Internet-Traffic und die Anwendung eilig entwickelter Provisorien für den Remote-Zugang. Jetzt werden langsam die Schwächen dieser Herangehensweise sichtbar, da in Bezug auf Transparenz, Sicherheit und Komplexität bekannte Problem fortbestehen.

Sicherheitslücken bei Remote-Arbeitssystemen zu beheben, sollte nicht Wochen oder gar Monate dauern. Mit der Zero Trust-Lösung von Cloudflare können Administratoren schon in einer halben Stunde mehr als 20 der dringlichsten Anwendungsfälle in puncto Sicherheit und Konnektivität der Belegschaft bewältigen.

Die Lösung: Zero Trust von Cloudflare



Die Zero Trust-Sicherheitsplattform von Cloudflare verschafft einen größeren Einblick, verringert Komplexität und senkt das Risiko beim Fernzugriff von Beschäftigten auf Anwendungen und das Internet. Sie wird auf dem schnellsten Edge-Netzwerk der Welt ausgeführt, um rascher einsatzbereit zu sein und eine höhere Leistung bieten zu können als die Lösungen anderer Anbieter.

Eine Zero Trust-Plattform kann auf dreierlei Weise die Sicherheit von Remote-Beschäftigten verbessern

Reduzierung des Risikos

Die Abhängigkeit von VPNs hat ein Failover-Risiko und Schwachstellen in der Firmeninfrastruktur geschaffen, die von Cyberkriminellen ausgenutzt werden können. Hat ein Angreifer erst einmal Zugang, kann es sich lateral zwischen verschiedenen Ressourcen bewegen, um Daten zu stehen. Trotz größter Anstrengungen, solche Bedrohungen zu blockieren und abzuwehren, werden Endpunkte weiterhin durch unentdeckte Malware kompromittiert.

Zero Trust-Sicherheitsplattformen erzwingen eine Identitäts- und Kontext-basierte Authentifizierung bei jeder Anfrage an Ihre Firmenanwendungen, sodass kaum noch Spielraum für laterale Bewegungen bleibt und die Risiken von Remote-Arbeit reduziert werden. Bei Browserisolierung werden Endpunkte von der Aktivität im Browser abgeschirmt, wodurch bekannt und unbekannte Bedrohungen ferngehalten werden.

Erhöhung der Transparenz

Als sich die Nutzer noch in Firmenbüros befanden, war die Verwaltung von Aktivitätsprotokollen unkompliziert. Doch ein Audit Trail ist deutlich schwieriger aufrechtzuerhalten, wenn die Mitarbeitenden von unterschiedlichen externen Standorten aus arbeiten und dazu neue Geräte nutzen. SaaS-Anwendungen verfügen oft über unterschiedliche Protokollierungsmöglichkeiten und VPN-Protokolle lassen sich häufig nur schwer parsen.

Zero Trust-Plattformen stellen Transparenz wieder her, indem sie Anfragen von sämtlichen Remote-Geräte abfangen und protokollieren – selbst von unverwalteten. Administratoren können die Aktivität von Remote-Arbeitenden auf intern gehosteten Applikationen und SaaS-Anwendungen überwachen und verfügen über einen Audit Trail, mit dem sie Zwischenfällen auf den Grund gehen können. Die Protokolle werden in einem Dashboard gebündelt und automatisch an den gewünschten SIEM-Anbieter übermittelt.

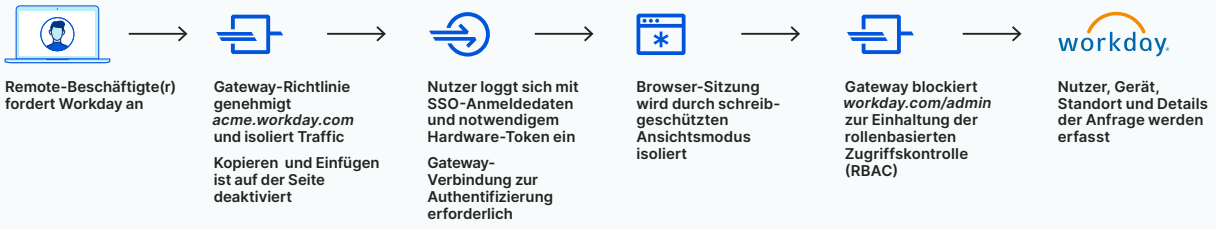
Beseitigung von Komplexität

Behelfslösungen zur Anbindung von Remote-Beschäftigten erweisen sich langfristig als zu anfällig. Administratoren sind gezwungen, Richtlinien zur Filterung des Traffics für mehrere nicht miteinander kompatible Tools zu verwalten und die Nutzer werden durch die unzureichende Performance frustriert.

Zero Trust-Plattformen vereinfachen die Art und Weise, in der sich die Nutzer verbinden, ebenso wie die Arbeit der Administratoren. Bei geringerer Abhängigkeit von veralteten VPN-Lösungen können Administratoren Standard-Sicherheitskontrollen auf den gesamten Datenverkehr anwenden – unabhängig davon, wie die Verbindung hergestellt wird oder an welcher Stelle im Netzwerk-Stack sie verortet ist. Darüber hinaus lassen sich sämtliche Richtlinien über ein einziges Dashboard verwalten.

Zero Trust-Sicherheit in Aktion

Anwendungsfall: Verhindern von Datenverlusten in SaaS-Anwendungen



Bei einer Architektur, die auf die Überprüfung in einem Arbeitsgang ausgelegt ist, wird der Traffic der Remote-Beschäftigten überprüft, isoliert, protokolliert und vor Internetbedrohungen geschützt. Die User verbinden sich dabei mit Rechenzentren, die sich ganz in ihrer Nähe befinden.