



مُصدري

الموارد البشرية

مقال شعري متخصص بالموارد البشرية يصدر عن
الهيئة باللغتين العربية والإنجليزية بالتعاون مع
مؤسسات عالمية

أبريل 2021

مستقبل البنية التحتية للأعمال التي تدعم السحابة

تفعيل عمل البنية التحتية
للأعمال الافتراضية

للتواصل

الهيئة الاتحادية للموارد البشرية الحكومية
الإمارات العربية المتحدة
أبوظبي، ص.ب. 2350
هاتف: +97124036000
دبي، ص.ب. 5002
هاتف: +97142319000

هيئة اتحادية | Federal Authority



www.fahr.gov.ae
hrecho@fahr.gov.ae
@FAHR_UAE
مركز الاتصال الموحد: 600525524

المجلة مخصصة من المجلس الوطني للإعلام برقم 306،
ومسجلة كعلامة تجارية لدى وزارة الاقتصاد في دولة
الإمارات العربية المتحدة



المشرف العام

د. عبد الرحمن العور

أسرة التحرير

عائشة السويدي

إبراهيم فكري

محمود المرزوقي

موزة السركال

آسيا البلوشي

عمر البلوشي

محمد أبوبكر

محمد النمر

للتواصل

الهيئة الاتحادية للموارد البشرية الحكومية

الإمارات العربية المتحدة

أبوظبي، ص.ب. 2350

هاتف: +97124036000

دبي، ص.ب. 5002

هاتف: +97142319000

هيئة اتحادية | Federal Authority



www.fahr.gov.ae

hrecho@fahr.gov.ae

@FAHR_UAE

مركز الاتصال الموحد: 600525524



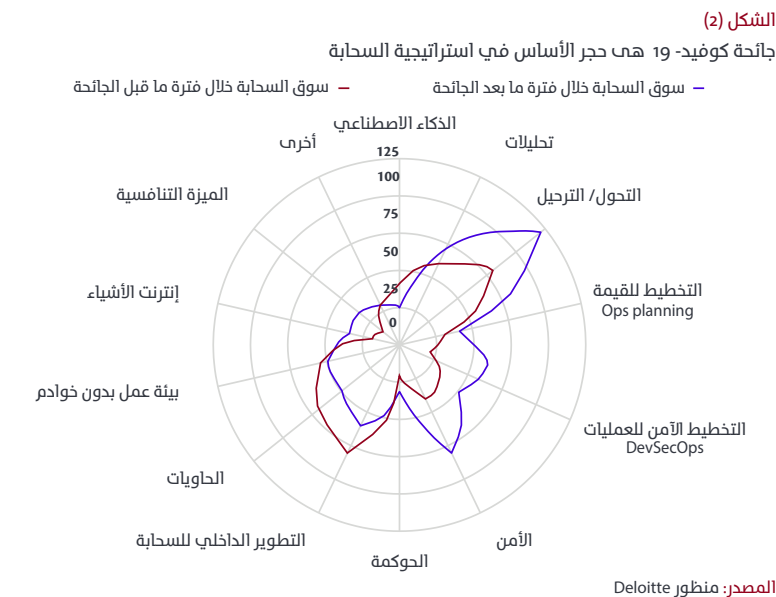
مستقبل البنية التحتية للأعمال التي تدعم السحابة

تفعيل عمل البنية التحتية
للأعمال الافتراضية

Kavita Saini, Aparna Prusty, Rupesh Bhat, and
Nairita Gangopadhyay
Deloitte



في ظل عمل معظم الموظفين على مستوى العالم عن بعد، شهد مقدمو الخدمات السحابية العامة طفرة هائلة في الطلب على خدماتهم، واضطرت المؤسسات لرفع مستوى وحجم السحابة والتحول إليها بسرعة، مما يترك مجالاً لمزيد من التحسين، وقد كشف العمل عن بعد عن صعوبة الوصول إلى البنية التحتية المحلية، مما يسلط الضوء على مخاطر البنية التحتية الرئيسية، ونتوقع أن نرى تحولاً في استراتيجيات السحابة نحو الترحيل السحابي، والأمن، والعمليات، وتخطيط القيمة، (و DevSecOps) وهي اختصار للتطوير والأمن والعمليات، كما نتوقع أن نشهد على مستوى العالم تراجعاً في الطلب على المبادرات السحابية الأصلية والحاويات والمبادرات بدون خادم (الشكل 2).



**العمل عن بعد خلال
جائحة كوفيد – 19 رفع
الطلب على خدمات
الحوسبة السحابية
بشكل غير مسبوق**

تسببت جائحة كوفيد - 19 في حدوث تحول جوهري في افتراضات هندسة الأعمال، حيث اضطرت العديد من المؤسسات لتغيير ملفات استراتيجيات البنية التحتية السحابية لديها. وفي حقيقة الأمر ومن خلال استطلاع أجرته (Logic Monitor) اتفق 87% من صناع القرار في مجال تقنية المعلومات على مستوى العالم على أن الجائحة من شأنها أن تؤدي إلى تسريع انتقال المؤسسات إلى الخدمات السحابية، وفي ظل وجود تكهنات بحدوث انخفاض في أعباء العمل المحلية بحلول العام 2025، فقد بدأ هذا الانتقال بالتسارع (الشكل ١).

الشكل (١)

استراتيجيات السحابة التي تنامت وتيرة سرعتها بفعل تداعيات جائحة كوفيد- 19

قبل ظهور جائحة كوفيد- 19	أثناء جائحة كوفيد- 19
<p>الطلب على السحابة</p> <p>توقع 20% من المؤسسات أن يكون نصف عبء العمل / البيانات المؤسسية على الأقل ضمن سحابة عامة في غضون 12 شهراً.</p>	<p>الطلب على السحابة</p> <ul style="list-style-type: none"> • 59% من الشركات تتوقع أن يتجاوز استخدام السحابة ما هو مخطط له مسبقاً بسبب الجائحة. • زادت استفسارات البحث لكبار المديرين التنفيذيين السحابيين في المجال الرقمي بنسبة 224%. • 6 من المؤسسات المالية العالمية أعلنت عن مبادرات سحابية جديدة منذ بداية الوباء.
<p>العمل عن بُعد</p> <p>3% من الموظفين تقريباً عملوا بدوام كامل عن بُعد في يناير 2020.</p>	<p>العمل عن بُعد</p> <ul style="list-style-type: none"> • 64% من الموظفين بدوام كامل باتوا يعملون عن بعد اعتباراً من أبريل 2020. • تأثر 81% من القنص العاملة العالمية (2.7 مليار شخص) بتوجهات البقاء في المنزل اعتباراً من مايو 2020.
<p>أدوات التواصل والمشاركة</p> <p>20 مليون مستخدم نشط يومياً في Microsoft Teams في نوفمبر 2019.</p>	<p>أدوات التواصل والمشاركة</p> <p>75 مليون (تقريباً أربعة أضعاف) مستخدم نشط يومياً لبرنامج Microsoft Teams بحلول مايو 2020.</p>
<p>البنية التحتية</p> <p>ارتبط 17% من مستخدمي سطح المكتب و 15% من مستخدمي الهواتف المحمولة إلى VPN في ديسمبر 2019.</p>	<p>البنية التحتية</p> <ul style="list-style-type: none"> • نمت اتصالات Azure VPN بنسبة 94%. • تضاعفت ذروة استخدام WAN 40 مرة منذ فرض الإغلاق في أوائل مارس. • نمت اتصالات VPN بنسبة 72% عن مستويات ما قبل الجائحة.
<p>العائدات من السحابة</p> <ul style="list-style-type: none"> • نمو بنسبة 37% لخدمات الويب (AWS) Amazon في الربع الثاني من عام 2019. • نمو بنسبة 22% في إيرادات Microsoft Intelligent Cloud في الربع الثالث من عام 2019 (بما في ذلك منتجات الخادم والخدمات السحابية وخدمات المؤسسات والإيرادات). 	<p>العائدات من السحابة</p> <ul style="list-style-type: none"> • نمو إيرادات Google Cloud Platform بنسبة 43% في إيرادات السحابة للربع الثاني من عام 2020. • 29% نمو خدمات أمازون عبر الإنترنت في الربع الثاني من عام 2020. • 27% نمو في إيرادات Microsoft Intelligent Cloud في الربع الثالث من عام 2020.

أنفقت الشركات في جميع أنحاء العالم 34.6 مليار دولار أمريكي على الخدمات السحابية في الربع الثاني من العام 2020، بزيادة قدرها 11% تقريباً عن الربع السابق. كما صرحت ساتيا ناديلا، الرئيس التنفيذي لشركة Microsoft ، "في غضون شهرين فقط شهدنا تحولات رقمية كبيرة تعادل التحولات الرقمية التي نشهدها عادة خلال عامين".



الشكل (3)

تعمل تحديات الأعمال على تسريع استيعاب حلول البنية التحتية السحابية

		
نهج الحلول التكنولوجية	التكنولوجيا والتحديات التشغيلية	تحديات الأعمال
<ul style="list-style-type: none"> • ستدعم الحلول السحابية المتعددة (وليس الاستراتيجيات فقط) العمل الافتراضي والقوة العاملة وأماكن العمل مع التركيز على أدوات وممنات الكفاءة التشغيلية من أجل تقديم حلول متكاملة. • ستعمل مراكز البيانات الافتراضية على تمكين الوصول المركزي إلى البيانات عن بعد أو إدارة البيانات الموزعة. 	<ul style="list-style-type: none"> • لم يعد من الممكن الوصول إلى مراكز البيانات المادية بسبب متطلبات أماكن العمل البعيدة. • تشدد أحجام العمل عن بعد على البنى التحتية التقليدية، مما يفرض استراتيجيات الرفع والتغيير التي تتطلب قدرًا أكبر من الكفاءة التشغيلية. 	<p>يزداد تعقيد التكنولوجيا مع تغيير نماذج الاستهلاك والوصول عبر البنية التحتية غير المتجانسة.</p>
<ul style="list-style-type: none"> • يساهم الأمن الموحد في إدارة الوعي بالمواقف ونقاط الوصول مع تغير السياقات ويشجع على تبادل المعلومات الخاصة باستخبارات التهديدات في الوقت الحقيقي ومعالجتها. 	<ul style="list-style-type: none"> • تصبح البنية التحتية المادية غير قابلة للوصول بسبب أوامر البقاء في المنزل وتوسيع نقاط الوصول وتحويل المحيط الأمني. • البنية التحتية للتكنولوجيا غير المتجانسة والتغيرات في طبيعة نقاط الوصول إلى شبكة ودية العمل والاستهلاك. 	<p>تنشأ المخاطر الأمنية عندما تُظهر هياكل الأعمال والتكنولوجيا المتشابهة بإحكام إمكانية تعرضها للضغوط.</p>
<ul style="list-style-type: none"> • نظام التطوير والعمليات (DevOps) هو نهج مجرب وحقيقي لتحقيق قيمة أفضل في أسرع وقت ممكن، كما أنه أكثر أمانًا وأقل عناءً من برامج تكنولوجيا المعلومات، علاوة على أن يشهد التطورات الجديدة في بيئة العمل ذات التوزيع المتزايد. 	<ul style="list-style-type: none"> • تؤثر القوى العاملة الموزعة التي لا يمكن جمعها معًا فعليًا على الفرق وطرق العمل عبر البنية التحتية غير القياسية مما يدفع الشركات إلى تنفيذ تغييرات البنية التحتية للتكنولوجيا. 	<p>تتطلب الكفاءة التشغيلية طرقًا مرنة للعمل من أجل تلبية احتياجات العمل المتغيرة بسرعة.</p>

المصدر: Deloitte analysis

الحلول المتعددة للسحابة، وليس الاستراتيجيات، لدعم العمل الافتراضي والموظفين ومكان العمل

تشكل استراتيجيات السحابة متعددة الوسائط والهجينة القاعدة الآن، حيث وجدت دراسة أن 93% من المؤسسات التي تستخدم المنظومة السحابية، تستعين باستراتيجية البنية التحتية متعددة الوسائط السحابية، ويستخدم 87% منها نموذج بنية أساسية سحابية هجينة (عامة وخاصة). وهناك إجماع عند ما يقرب من 85% من المؤسسات على أن السحابة الهجينة هي نموذج تشغيل تكنولوجيا المعلومات الأمثل، حيث أفاد 61% من المستجيبين بضرورة تنقل التطبيقات عبر الحوسبة السحابية، وتجاوزت العديد من المؤسسات التحدي الأولي المتمثل في اختيار العديد من مقدمي الحوسبة السحابية، وتحديد البيانات المراد تخزينها في سحابة عامة أو خاصة وإدارة التدفق الفعال للبيانات، و قابلية التشغيل البيئي عبر البنى التحتية السحابية المتعددة الخاصة بهم.

من المحتمل أن يكون التحدي التالي في إدارة التعقيد السحابي هو تكوين الأدوات والبرامج والتكنولوجيا لتقديم حل متكامل متعدد الوسائط السحابية - بما يتضمن

المؤسسات
الديناميكية لديها
فرصة مثالية لتوظيف
التكنولوجيا في
تمكين موظفيها من
العمل عن بعد

نظرًا لأن المؤسسات صارت تستجيب لجائحة كوفيد- 19 بتركيز متجدد على السحابة، فإنها تواجه تعقيدات تكنولوجيا المعلومات ومخاطر الأمن وتحديات الكفاءة التشغيلية، بينما تعمل بعض المؤسسات على تقليل أولويات أو تأخير خطط الترحيل إلى السحابة غير الضرورية، حيث نجد الفرصة سانحة لدى القادة والمؤسسات لديهم فرصة لتحديث الآليات الرئيسية التكنولوجية الخاصة بهم باستخدام بنية أساسية سحابية قابلة للتطوير.

أظهر بحث ديلويت أن "المزيج السحري" لحل التعقيد السحابي في المؤسسات يتمثل في توفر الأدوات الفعالة 34%، والمنهجيات 34%، والأشخاص 32%، وبالنسبة للعديد من المؤسسات فإن هذا الأمر يعني إعادة تفعيل البرامج السحابية، وتوظيف استراتيجيات التطوير، والتركيز على الأمن السيبراني، وتوفير الحلول متعددة الوسائط السحابية للبنى التحتية غير المتجانسة، من أجل تحسين العمليات وخفض المخاطر وإدارة التعقيدات، وتحظى المؤسسات الديناميكية بفرصة مثالية لتوظيف التكنولوجيا في تمكين موظفيها من العمل عن بعد. (الشكل 3)



ذلك من إدارة الهوية والوصول، أو مراقبة الشبكة، أو إدارة البيانات الوصفية، أو الذكاء الاصطناعي لعمليات تكنولوجيا المعلومات (AIOps) لإدارة أنظمة القوى العاملة والأنظمة الأساسية المستخدمة لأداء العمل. يجب أن تراعي الحلول المتعددة للحوسبة السحابية التنسيق والتكامل عبر هذه الأدوات والتقنيات لإدارة البيانات والموارد وسير العمل، والمساعدة على ضمان الحصول على أفضل مستوى من تدفق البيانات، من خلال بنية هيكلية من الحلول المتكاملة، بما في ذلك التخزين وقواعد البيانات والأنظمة الأساسية وحتى الأمن. عندئذ فقط يمكن للبنية الأساسية متعددة الوسائط السحابية دعم تطبيقات الأعمال بكفاءة وأمان لزيادة القيمة على أساس كل تطبيق على حدة.

ما يمكن أن يمثل تحديًا خاصًا للحلول متعددة الوسائط السحابية خلال جائحة كوفيد - 19، هو إيجاد تطبيق جيد مناسب لتلك التقنيات بسرعة. غالبًا ما يكون الاستفادة من أي منصة أو خدمة سحابية متاحة، ومع ذلك فإن الانتقال إلى تطبيق غير مناسب لأي نظام أساسي جديد، عادة لا يحالفه النجاح.

يجب على المؤسسات أولاً فهم التطبيق نفسه، وفهم البيانات المتصلة، والبنية الأساسية، ومن ثم تقييم ما إذا كانت أي من هذه التقنيات الجديدة مناسبة. يُعد Kubernetes، وهو مشروع مفتوح المصدر أطلقته شركة جوجل لأتمتة نشر حاويات البيانات وإدارتها وتوسيع نطاقها، مثالاً على ذلك. تظهر الدراسة السحابية السنوية لشركة Flexera أن الشركات تستخدم ما متوسطه 2.2 شبكة سحابية عامة و 2.2 شبكة سحابية خاصة، كما أن 20% من المؤسسات تستخدم Kubernetes في

الإنتاج أو للتطوير والاختبار، ولكن هذا لا يعني أن على الآخرين التسرع في استخدام Kubernetes. بل يتعين على الشركات أن تسعى بجدية للتفكير فيما تحتاجه من موارد إدارة السحابة لدعم تطبيق الأعمال الأساسي - في هذه الحالة يمكن النظر في البنى التحتية للعمل عن بعد وبيئات العمل التشاركية - والعمل لتحديد الأدوات المناسبة التي توفر الخدمات الصحية (الشكل 4)

الشكل (4)

تطوير البنية التحتية لتكنولوجيا المعلومات التي تدعم مستقبل العمل والقوى العاملة ومكان العمل

تحدي جديد	حالياً	المستقبل	المزايا
مراكز البيانات			
• تواجه مراكز البيانات الداخلية مخاطر استمرارية الأعمال.	• جعل مراكز البيانات افتراضية لتحقيق مكاسب طويلة الأجل في إدارة أعباء العمل.	• إنشاء خدمات مشتركة بقاعدة بيانات افتراضية واحدة أو عن طريق إدارة البيانات بطريقة موزعة.	• التخلص من التكرار وتمكين فهم البيانات والاتصال بواجهة برمجة التطبيقات والحكومة المحسنة.
تكنولوجيا المعلومات			
• التحولات في البنية التحتية غير المتجانسة للأستهلاك تزيد من تعقيد تكنولوجيا المعلومات.	• قبول الوسائط المتعددة عبر الاستراتيجيات التي تم قبولها الآن على نطاق واسع باعتبارها الإستراتيجية المثلى.	• تطوير حلول سحابية متعددة تركز على الوصول وإدارة الشبكة والعمليات وتعقد نقطة النهاية من أجل الوصول إلى حلول متكاملة، والإدارة والعمليات ونقطة النهاية.	• تحقيق نماذج استهلاك مرنة مع تحسين إدارة التكلفة.
العمليات			
• تستمر عمليات تكنولوجيا المعلومات (ITOps) في التطور إلى ما بعد العمليات السحابية (CloudOps).	• تنفيذ العمليات السحابية (CloudOps).	• التوسع في العمليات السحابية (CloudOps) لتشمل AIOps، والتي تتجاوز المراقبة التفاعلية إلى الاستجابة الآلية.	• تمكين المراقبة التنبؤية.

المصدر: Deloitte analysis





سمح تخزين البيانات الافتراضي لكبار تجار التجزئة، مثل The Home Depot ، بالاستجابة بشكل أسرع لاحتياجات المستهلكين عبر سلسلة التوريد الخاصة بها. تتبع مؤسسة Home Depot أكثر من 50000 منتج عبر 2000 موقع، وتقوم بتحليل المنتجات التي يتم بيعها وتحديد توقيت البيع ومكانه من خلال الاستعانة بالإنترنت الأشياء (IoT)، والميزة التنافسية والحوسبة السحابية، وتصحيح المسار وفقاً لذلك.

تشهد البنية التحتية غير المتجانسة تحولات في الاستهلاك وزيادة تعقيد نقطة النهاية، لم تعد المؤسسات تدير الأنظمة في مركز بيانات واحد. بل صارت تُدير شبكة الهواتف المتحركة وأجهزة إنترنت الأشياء والميزة التنافسية. كل هذه الأشياء تعمل معاً على تضخيم تعقيد البيانات (كما في مثال Home Depot). كان هذا الاتجاه نحو بنية تحتية غير متجانسة قيد التنفيذ بالفعل، لكن جاءت جائحة كوفيد-19 لتغيّر نماذج الاستهلاك عبر تلك الشبكة من خلال تغيير مكان العاملين وآلية العمل. استفاد أولئك الذين لديهم بالفعل بنية أساسية سحابية من قدرتهم على تقليص تكاليف البنية التحتية للقوى العاملة للبنية التحتية غير المستخدمة، أو زيادة الموارد في الأماكن التي شهدت إقبالاً أكبر، ونتيجة لذلك تأثرت نماذج أعمال شركات الطيران، وتجار التجزئة، وشركات التأمين، واحتياجات القوى العاملة بشكل متباين بالجائحة، وبالتالي فإن مطالب البيانات والبنية التحتية الخاصة بكل قطاع ستكون مختلفة.

على سبيل المثال بسبب العمل عن بُعد، قفز معدل الاستهلاك السحابي في شركة Audi Business Innovation GmbH، وهي وحدة تابعة لشركة Audi لصناعة السيارات، بنسبة 12% بين شهري مارس وأبريل، حيث يستخدم الموظفون المزيد من أدوات وبرامج الطاقة والحوسبة عن بُعد المستأجرة، ونظراً لأن الشركة كانت منخرطة بالفعل في المنظومة السحابية، فقد تمكنت من ضبط نماذج الاستهلاك والمنصات لديها مع توقع خفض الإنفاق بنسبة 30%. لقد غيّرت جائحة كوفيد-19 نوعية البيانات التي ترسلها المؤسسات إلى مراكز البيانات خارج مقرها، وكيفية الوصول إلى الشبكات عبر القنوات غير المتعارف عليها، وما هو حجم إنترنت الأشياء داخل الشركة، والجوال، والميزة التنافسية، والبيانات السحابية التي يجب إدارتها عبر الشبكة باستخدام نقاط الوصول المتغيرة. كل هذا يمكن أن يزيد من التعقيد.

تتضمن بعض الاعتبارات الرئيسية لإدارة البنية التحتية متعددة الوسائط السحابية، بناء خدمات بيانات مشتركة، وإدارة البنية التحتية غير المتجانسة، وحل تعقيد نقطة النهاية، واعتماد منهجيات جديدة في عمليات تقنية المعلومات (ITOps) بما في ذلك عمليات الذكاء الاصطناعي (AIOps).

تواجه مراكز البيانات المحلية مخاطر استمرارية الأعمال: فقد أدنى عدم قدرة المؤسسات على الوصول إلى مكان العمل، بما في ذلك البنية التحتية لموقع العمل، خلال أزمة تفشي الجائحة إلى جعل تحويل مركز البيانات إلى مركز افتراضي معضلة كبيرة، مما جعل المؤسسة على المحك فيما يتعلق باستمرارية الأعمال.

أنقذت شركة fintech العملاقة الملايين من خلال نقل عشرات الآلاف من أعباء العمل إلى السحابة لتقليل الآثار المترتبة على عدم قدرة مراكز البيانات من الوصول إلى البنية التحتية لمواقع العمل، هناك مساران لبناء خدمات بيانات مشتركة: أحدهما يدمج البيانات في قاعدة بيانات مادية موحدة. والآخر من خلال إدارة البيانات بطريقة موزعة، مع الاستفادة من المحاكاة الافتراضية للنظر إلى جميع البيانات كقاعدة بيانات واحدة، على الرغم من أنها قواعد بيانات موزعة مختلفة، باستخدام نماذج قواعد بيانات مختلفة. أيًا كان النهج الذي تختاره المؤسسة، فإن الفكرة هي أن يكون لها مسار واحد للتعامل الفريد والمبيعات والمنتج وبيانات أخرى، بحيث يسمح لها هذا النهج بما يلي:

- القضاء على التكرار لزيادة الكفاءة وتكلفة البنية التحتية المدارة
- فهم قاعدة البيانات بمزيد من التفصيل، جنباً إلى جنب مع البيانات الوصفية
- اختيار تقنية قاعدة البيانات المناسبة التي تتلاءم مع احتياجاتها، مع العلم أن قواعد البيانات السحابية الأصلية هي الخيار الأفضل بشكل عام
- تمكين خدمة قاعدة البيانات مع API أو الوصول إلى خدمات الويب
- تنفيذ خدمات الحوكمة والأمن والإدارة



إن أدوات عمليات الذكاء الاصطناعي بالإضافة إلى أدوات العمليات الأخرى قادرة على تحليل البيانات القادمة من جميع الأنظمة والأجهزة لتحديد أي خلل في الأنظمة، حتى قبل معرفة البشر بها، وذلك إذا تم تركيبها وبرمجتها بشكل صحيح، إذ يمكنها اكتشاف السلوكيات الخاطئة، واتخاذ الإجراءات التصحيحية. قبل تفشي جائحة كوفيد - 19 استقطبت مؤسسات البنية التحتية على مستوى العالم العديد من مالكي عمليات الذكاء الاصطناعي، وذلك في إطار سباقها المتاحم في مجال الذكاء الاصطناعي.

الأمن الموحد لمستقبل الأعمال والعاملين ومكان العمل

بينما ألفت جائحة كوفيد- 19 بظلالها السلبية على الأعمال والعاملين ومكان العمل، مما أجبر تكنولوجيا المعلومات على إدارة البنية التحتية الغير متجانسة بشكل متزايد بالأدوات والتقنيات الجديدة إضافة إلى أن العديد من البنى التحتية نفسها تواجه تحديات أمنية جديدة، وذلك بالنظر إلى أن مكان وماذا وكيف العمل قد تغير، نظرًا لتحولات تركيز تكنولوجيا المعلومات لاستيعاب الطرق الجديدة التي يتم بها تنفيذ العمل عبر مواقع أماكن العمل المتغيرة، فقد تغير السياق ذاته للمراقبة الأمنية مع تركيبة بنية تحتية جديدة تمامًا -حتى استخدام الإنترنت المنزلي، والأجهزة المحمولة الشخصية، وما إلى ذلك، قد تغير بالمثل.

مثل هذه المعطيات عززت الحاجة إلى التركيز على استراتيجيات الأمن الفيدرالية المعروفة بنجاحها في إدارة أمن البنية التحتية الموزعة وغير المتجانسة عبر المستويات، ودفع الوعي الظرفي.

تسمح أطر العمل السحابية الموحدة للمؤسسات بنشر خدمات الحوسبة السحابية المتعددة ودمجها وإدارتها، حيث يمكنها المساعدة في تحديد وتنفيذ بروتوكولات الأمن الموحدة عبر طبقات التطبيق والشبكة والنظام ومركز أمن السحابة. يجب أن يكون التركيز على المراقبة الدفاعية الاستباقية (الإنذار المبكر والقيادة والتحكم) وإدارة هجمات نقاط الوصول ضد البرامج الضارة والتهديدات المستمرة المتقدمة واختراقات الشبكة عبر طبقات البنية التحتية وتخزين البيانات والمنصات الموثوق بها ومواقع الويب وأنظمة التشغيل. يجب القيام بكل هذه الأمور للمساعدة في تمكين تبادل معلومات التهديد الديناميكي .

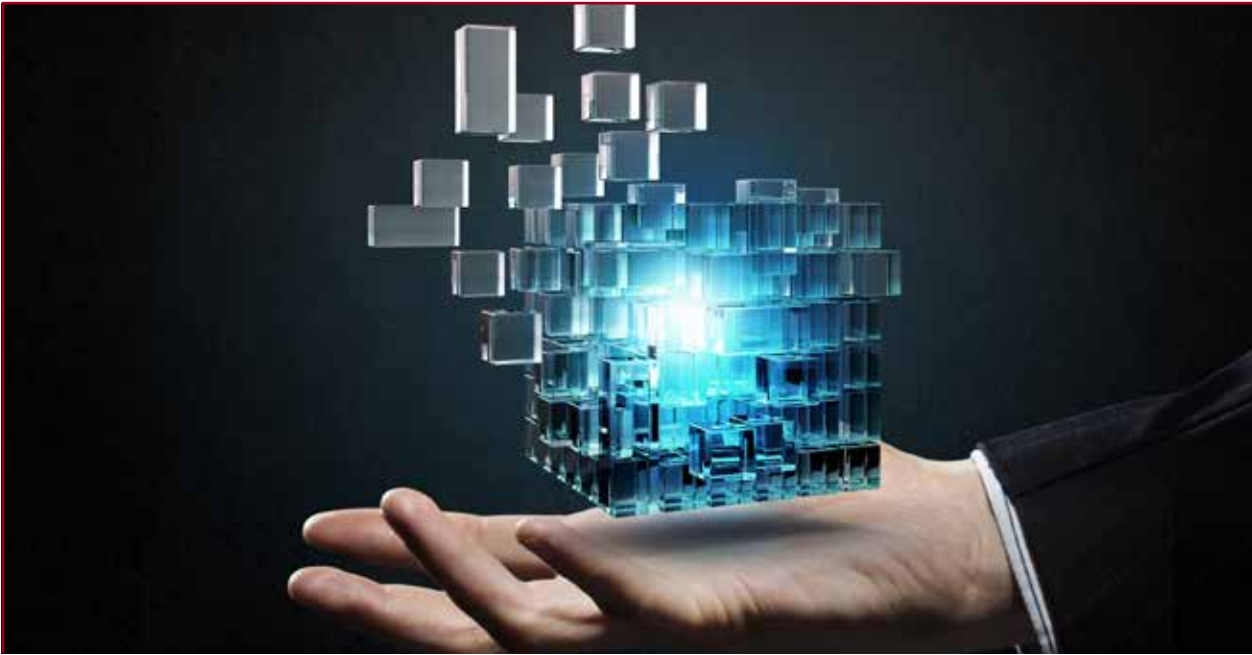
أنشأت وزارة الأمن الداخلي الأمريكية ، على سبيل المثال ، نظامًا بيئيًا دفاعيًا عبر الإنترنت ومشاركة المعلومات الاستخباراتية، والذي تم من خلاله دمج تقنيات دفاعية مختلفة (جوانب من دفاع الهدف المتحرك وأمن أنظمة الحوسبة السحابية) في اتحادات المؤسسات عبر شبكة من المنظمات لتعزيز الأمن ضد الهجمات المعروفة والجديدة . في ظل النضج الذي يتمتع به الأمن الفيدرالي ، تركز المؤسسات بشكل متزايد على خدمات الانترنت،و الأمن كخدمة لاتحاد سحابي ، و بيئة متعددة الوسائط السحابية ، و إطارًا مُمكنًا للبلوك تشين blockchain ، وأنظمة بيئية للشبكة (الشكل 5).

من المحتمل أن البنية التحتية للشركة كانت بالفعل عبارة عن مجموعة من العديد من المنصات المختلفة، بعضها يتم استقباله على السحابة، والبعض الآخر في أماكن العمل، وكبي تنجح المؤسسات في إدارة التحول في استهلاك الأجهزة بسبب تفشي الجائحة (العاملون في المنزل على أجهزة الكمبيوتر المحمولة والهواتف المحمولة خارج نطاق شبكة الشركة) فإنها بحاجة إلى فهم الواجهات، ونماذج الأمن، والحوكمة والمضي قدمًا من هذه النقطة.

غالبًا ما تبدأ إدارة البنية التحتية غير المتجانسة وتنتهي بأخذ مخزون شامل للنظام، ثم يتم إنشاء خطة إدارة لتنفيذ العمليات السحابية أو العمليات السحابية (CloudOps)، والتي تجمع بين الشبكة والأمان والأداء وإدارة الجهاز، ومهام مكتب المساعدة، كما يمكن أن تبسط العملية التشغيلية التصميم لنموذج تشغيل مادي يشمل الأدوات والتقنيات.

يمكن للمؤسسات أن تتجاوز التعقيدات في نقطة النهاية عن طريق تقليل عدد نقاط النهاية الخاضعة للإدارة، وتقليل عدد أنظمة المعالجة والتشغيل وقواعد البيانات، واستخدام أدوات الإدارة والحوكمة والأتمتة لإدارة ما تبقى من تعقيدات.

تبنى منهجيات جديدة في العمليات التقنية (ITOps) بما في ذلك عمليات الذكاء الاصطناعي (AIOps) مع الأهمية المتزايدة التي باتت تكتسبها الحوسبة السحابية، ازدادت أهمية تقنيات الذكاء الاصطناعي، ومن خلال متابعة مجال البنية التحتية السحابية عن كثب، نلاحظ أن هذا المجال شهد تطوراً كبيراً، حيث انتقل من مجرد المراقبة التفاعلية إلى المراقبة التنبؤية، ونحن الآن ننتقل إلى عصر جديد من عمليات الذكاء الاصطناعي، حيث توفر هذه العمليات وغيرها من أدوات المراقبة والإدارة الحديثة إمكانية تصميم عمليات مؤتمتة قادرة على الاستجابة للأحداث، وإطلاق العمليات التصحيحية (مثل اكتشاف أخطاء الحزمة المقبلة من جهاز شبكة واحد، والتوجيه مؤقتًا حول هذا الجهاز حتى يتم استبداله).



الأمان غير المتجانس للبنية التحتية لتكنولوجيا المعلومات غير المتجانسة: نظرًا لأن المؤسسات تتطلع إلى تأمين بنية متعددة المستويات تشمل السحابة والميزة التنافسية والجوال وإنترنت الأشياء ، يتعين عليها تأمين كل طبقة بنية ضد التهديدات الخاصة بهذا المستوى. في الواقع ، تتطلب إدارة البنية التحتية غير المتجانسة نموذج أمن غير متجانس يتم تويده عبر مزودي التكنولوجيا لمختلف المستويات على مستوى نقطة النهاية ، يجب على المؤسسات الجمع بين مراقبة البنية التحتية ومعالجتها مع التطوير والأمن والعمليات ، إلى جانب الذكاء الاصطناعي لإدارة التهديدات التنبؤية والآلية والمراقبة والدقة ، كل ذلك على مستوى جهاز الحاسوب المكتبي / الجهاز المحمول. في نموذج الأمن الموحد ، يمكن للمؤسسات الوصول إلى كل طبقة بنية تحتية أو جهاز أو عملية وإغلاق فجوات الأمان بتجزئة الشبكة. فيظل تفشي جائحة كوفيد- 19 ، أصبح سطح الهجوم الآن أكبر حيث أصبحت شبكة البنية التحتية للعمل أكثر تشتتًا أو توزيعًا ، مما يزيد من أهمية المراقبة الاستباقية المكثفة عبر جميع الأجهزة التي تتجاوز من مرحلة "اكتشاف التهديدات" إلى مرحلة "معالجة التهديدات".

دخول موثوق به في عالم افتراضي عن بُعد: وجدت إحدى الدراسات في هذه الصناعة أن 33% من الهجمات التي تهدد أمن المؤسسات على البنية التحتية السحابية ترجع إلى الافتقار إلى معايير الحوكمة والأمان المناسبة المتعلقة بالتحكم في الوصول المستند إلى الأدوار. الوصول إلى الهوية يُعد واحد من أكبر نقاط الضعف ، حيث أفاد 33% من المشاركين في دراسة أجرتها شركة Sophos أن أدوار إدارة الوصول إلى الهوية قد تأثرت بانتهاكات أمان السحابة والتهديدات الرئيسية (بما في ذلك البرمجيات الخبيثة وبرامج الفدية وحوادث اختراق التشفير).

تُعد إدارة الأمن المركزية مفهوم منذ زمن طويل لإدارة الأمن عبر الموارد الموزعة. وتظل إدارة الهوية التي تركز على امتيازات الوصول حجر الزاوية لتأمين الشبكة، لا سيما مع ظروف العمل عن بعد والتي أدت إلى زيادة مساحة سطح هجوم الشبكة عن بُعد. في ظل اندثار محيطات الرقابة، يمكن لنهج عدم الثقة في الأمن السيبراني أن يساعد المؤسسات في الحفاظ على سلامة وأمن بياناتها وأصولها خارج المحيط عبر مجموعة من الأجهزة.

الشكل (5)

الأمن الموحد لمستقبل العمل والقوى العاملة وأماكن العمل

تحدي جديد	حالياً	المستقبل	لماذا نمضي إلى هناك
تطلب البنية التحتية لتكنولوجيا المعلومات غير المتجانسة نموذج أمان غير متجانس.	تنفيذ الأمن الموحد لتأمين البنية التحتية عبر التطبيق والشبكة وطبقات النظام بالإضافة إلى مركز أمان C2.	إدارة الحوسبة الموحدة وصولاً إلى مستوى نقطة النهاية عبر المستويات/الأجهزة (السحابة، والحافة، الهاتف المتحرك، وإنترنت الأشياء).	زيادة الوعي بالمواقف، وإدارة هجمات نقاط الوصول بشكل أفضل، وتمكين استخبارات التهديدات الأكثر ديناميكية ومعالجتها.
الوصول الموثوق به مهم بشكل متزايد في عالم بعيد.	تنفيذ ضوابط الوصول على أساس المهام، وإدارة الأمن المركزية، وإدارة الوصول إلى الهوية.	استخدام ميزات الأمان المضمنة بدون إخفاء الهوية، والمصادقة متعددة العوامل (MFA)، وإدارة الوصول المتميز (PAM).	تعزيز إدارة الوصول إلى الشبكة.
يصبح أمن المنطقة المحيطة غير فعال عندما يصبح محيط المكتب غير ذي صلة.	يحتاج أمن المنطقة المحيطة إلى مركز بيانات محمي مادياً لمرعاة نقاط الوصول لأولئك الذين يحتاجون إلى الوصول عن بعد، متى أمكن ذلك، وإلى البدائل الافتراضية التي تتطلب نماذج أمان جديدة.	تطلع إلى استبدال الأمن على مستوى المنطقة المحيطة بالأمن على مستوى الجهاز؛ مع عمل محاكاة افتراضية للخدمات وأجهزة سطح المكتب وأجهزة إنترنت الأشياء البعيدة؛ وتأمين كل مكون، بما في ذلك مستودعات الكائنات وتجزئة الشبكة وخدمات الويب.	إدارة الأمن عبر منطقة التهديدات المتغيرة.
تزايد صعوبة مشاركة المعلومات الأمنية والتعاون عبر الفرق الموزعة والحلول السحابية المتعددة.	تنفيذ حلول المراسلة الفورية (IM) عبر الشبكة الموحدة.	التحول بعيداً عن حلول المراسلة الفورية ذات المورد الواحد إلى حلول المراسلة الفورية المتكاملة الموحدة للاستفادة الكاملة من تقنية موفري الخدمات السحابية.	تعزيز قابلية التشغيل البيئي لنظام الأمن والتعاون ومشاركة المعلومات. تجنب تجميد المورد.

المصدر: Deloitte analysis

من المرجح أن تستمر هذه الاتجاهات في التطور، بالإضافة إلى العديد من الاتجاهات الجديدة التي تم استحداثها من خلال أوامر العمل عن بُعد ، مما يؤدي إلى تشغيل بنية تحتية جديدة للعمل تتعلق بالوصول الموثوق إلى الشبكة ، والأمن القائم على المحيط ، والرسائل الفورية الموحدة (IM) ، والحوسبة الموحدة حتى مستوى نقطة النهاية.



**يحتاج الأمن الآن إلى
مراعاة نقاط الوصول
لأولئك الذين يحتاجون
إلى الوصول عن بعد ،
حيثما أمكن ، والبدايل
الافتراضية - كل هذه
الاعتبارات تتطلب على
الأرجح نماذج أمن جديدة**

الوصول عن بعد ، حيثما أمكن ، والبدايل الافتراضية - كل هذه الأشياء تتطلب على الأرجح نماذج أمن جديدة. يجب على المؤسسات استبدال الأمن على مستوى محيط العمل على أن يحل محله الأمن على مستوى الجهاز ، والخدمات الافتراضية ، وأجهزة سطح المكتب الافتراضية ، وأجهزة إنترنت الأشياء عن بُعد ، وتأمين كل مكون ، بما في ذلك مستودعات الأشياء وخدمات الإنترنت .

حلول المراسلة الفورية المتكاملة / الموحدة: يمثل الاتجاه الناشئ في الأمن الموحد في التحول بعيداً عن حلول المراسلة الفورية لمورد واحد إلى حلول مراسلة فورية متكاملة ومتحدة للاستفادة بشكل كامل من تقنية موفري السحابة وتجنب مرحلة الإغلاق للموردين. يمكن الآن دمج خدمات أمازون عبر الإنترنت و بروتوكول الحوسبة السحابية لشركة جوجل (GCP) مع Microsoft Active Directory ، مما يجعل إدارة الأمن السحابي عبر البنية التحتية متعددة الوسائط السحابية أكثر سهولة. يمكن للمؤسسات ، على سبيل المثال ، استخدام التكامل الموحد لبروتوكول الحوسبة السحابية لشركة جوجل GCP للتكامل مع حل Active Directory المنزلي ، والذي يمكنهم من تبسيط اتصالات الأمان الافتراضية من أجل اكتشاف التهديدات ومعالجتها بشكل أسرع.

هذا التحول في الكيفية التي يتعاون بها الأشخاص عبر الأمن ، يمكن ملاحظته على نطاق أوسع بكثير الآن عبر جميع ممارسات عمليات التطوير التي يتم إجرائها على نطاق أوسع في كافة أنحاء المؤسسة.

عمليات التطوير في عالم موزع وطرق عمل متغيرة

نجحت العديد من الشركات مع عمليات الترحيل السحابية الصغيرة ، ولكن عندما يتعلق الأمر بتوسيع نطاق السحابة ، نجدها تتعثر في مرحلة عنق الزجاجة ، سواء على الصعيد التنظيمي أو مستوى العمليات. ومن هنا ، يمكن لعمليات التطوير تبسيط العمليات. تحدث عمليات التطوير على التواصل والتعاون الرائع (بمعنى آخر ، العمل الجماعي) لتعزيز جودة البرامج بشكل أسرع وأكثر وثوقية.

ينتقل النهج من التحكم المستند إلى الشبكة إلى المبادئ القائمة على الهوية مع ضوابط الوصول وإدارة الهوية كمحور رئيسي. مع انعدام الثقة ، تتخذ المؤسسات نهج "لا تثق أبداً وتحقق دائماً" لتحسين وضعها السيبراني عبر الأفراد والأجهزة. على سبيل المثال ، قامت وزارة الدفاع الأمريكية بتضمين ميزات أمان خالية من المجهولية مرتكزة على البنية التحتية السحابية الموحدة. يتيح هذا للمسؤولين مراقبة وتتبع والتحكم في جميع البرامج والأجهزة ووصول المستخدم إلى الحوسبة السحابية الخاصة به في الوقت الفعلي.

استجابةً للجانحة ، أعلنت وكالة الأمن السيبراني وأمن البنية التحتية عن سياسة اتصال إنترنت موثوقة مؤقتة للتعامل على وجه التحديد مع العمل عن بعد . رفعت المؤسسات شعار "عدم الثقة أبداً ، والتحقق دائماً ، وفرض أقل الامتيازات" وأخذته كنهج لتأمين الهويات المميزة . قامت شركة Cosmo Films ، وهي شركة تصنيع ، بتحويل بنيتها التحتية بالكامل من مصنع / وحدة مكتبية مركزية إلى نموذج لامركزية مع مستويات وصول: يقول جاغديب كومار ، كبير مسؤولي تقنية المعلومات في المؤسسة "لدينا مستويات وصول مخصصة بناءً على احتياجات المستخدم وقد وفرنا الإتاحة وإمكانية الوصول لسلة البيانات والمعلومات الهامة للمستخدمين في جميع أنحاء الهند دون أية تحديات جغرافية أو منطقة زمنية".

الأمن المحيط بالمكتب: لقد أدى تأثير جائحة كوفيد-19 على موقع العمل (المنزل الآن) إلى أنها جعلت من النماذج الأمنية لمحيط العمل التقليدي بمثابة تقليد عفا عليه الزمن. لم يعد داخل المكتب المحمي جسدياً أشخاص يعملون داخل محيطه؛ لذلك ، يجب أن يأخذ الأمن الآن في الاعتبار نقاط الوصول لأولئك الذين يحتاجون إلى





الشكل (6)

استراتيجيات التطوير والعمليات (DevOps) يمكنها إتاحة طرق جديدة للعمل

☆	🚶	📍	🎯
المزايا	المستقبل	حالياً	تحدي جديد
العمليات			
• تمكين الفرق من الاستجابة والتعامل الفوري للتركيز على العمل التكتيكي الذي يوفر قيمة فورية.	• مضاعفة المرونة لمواءمة العمليات التجارية والتقنية والحفاظ على المرونة اللازمة في أوقات عدم اليقين.	• اتباع استراتيجية التحول والاعتماد لإعادة التخرج السحابي.	• تتطلب استراتيجيات العمل سريعة التحول رد فعل سريع وطولاً مرنة.
التعاون			
• تمكين تبادل المعرفة في الوقت الحقيقي وتسهيل إدارة المعرفة وتوليد الذكاء الاجتماعي.	• استخدم (ChatOps) عبر فرق المشروع والإدارات والمؤسسات.	• تبني أدوات الاتصال والتعاون للفرق الافتراضية الموزعة.	• يتطلب العمل عن بعد المزيد من طرق العمل التعاونية.
الأتمتة			
• إنشاء عمليات آلية وقابلة للتكرار	• الاتجاه إلى الأتمتة الشاملة من خلال دمج خدمات الذكاء الاصطناعي السحابي والتعلم الآلي.	• اعتماد أدوات DevOps للتزويد الآلي.	• تتطلب البنية التحتية المرنة والديناميكية تقليل التدخل البشري اليجوي.
الفرق			
• تحقيق الأهداف والغايات المشتركة بالإضافة إلى أكبر قدر ممكن من المواءمة بين فرق الإنتاج بالكامل.	• إعادة تصور الأدوار التقليدية وتبني نموذج تشغيل تكنولوجيا المعلومات كخدمة مع ارتفاع المهندسين المعماري في العمل.	• تنفيذ مركز سحابي لفرق التميز.	• توقفت سلاسل التوريد التقليدية بشكل لا رجعة فيه.
العمليات			
• بيئة بناء وتطوير موحدة ومتسقة، تعزيز الحوكمة، وتجربة العملاء.	• استمر في التحول إلى العمليات والحوكمة ودعم العملاء.	• تحول إلى دمج DevSecOps في استراتيجية DevOps الخاصة بك.	• يستمر "DevOps" في التحول لتقديم نظام "DevOps" متكامل.

المصدر: Deloitte analysis

نتوقع زيادة التركيز على أدوات التعاون الافتراضية، والأتمتة الضخمة، والتحسين المستمر عبر دورة حياة المنتج بأكملها حيث تواصل المؤسسات في التحول تجاه اليسار نحو العمليات التطويرية من البداية إلى النهاية.

مضاعفة المرونة لزيادة الاستجابة: استراتيجية التحول والتبني هي المعيار لإعادة التدرج السحابي للتمكين الفعال من حيث التكلفة لتدفقات العمل المرنة التي

إن عمليات التطوير هي بمثابة تحول ثقافي. وجدت دراسة أخرى أن عمليات التطوير إلى جانب الحوسبة السحابية هي عامل مضاعف يعمل على تحسين الأداء بنسبة تصل إلى 81% 38. وليس من المستغرب إذن أن تظهر شركة متخصصة في تحليل الصناعات، نمواً في أدوات عمليات التطوير المكونة من رقمين في عام 2019 ، حيث وصلت الإيرادات العالمية إلى 8.5 مليار دولار أمريكي.

تُعتبر التقنية بمثابة الجزء الأسهل في عمليات التطوير - البرامج النصية المؤتمتة- والتكامل المستمر والتسليم ، وتقديم الخدمة المؤتمتة. حيث تميل المؤسسات إلى خوض الصراع من أجل تحويل العمليات والهياكل الحالية لدعم الأتمتة ودفع تغيير الثقافة عبر مجموعة من العمليات. يمكن القيام بذلك من خلال إدارة التغيير والنشر واختبار قبول المستخدم والأمان والامتثال واستراتيجية المنتج المستمرة.

الشيء الذي تغير مع ظهور جائحة كوفيد- 19 هو أنه عندما يعمل الأشخاص وفرق العمل عن بُعد عبر بنية تحتية غير قياسية ، يجب أن تتغير العمليات. هذه فرصة فريدة لبناء عمليات جديدة وبنية تحتية بالنظر إلى أن الاحتياجات التنظيمية الملحة تفوق بعض العراقل المعتادة. في عالم ما بعد الجائحة ، وعندما تتعافى المؤسسات ، يجب أن تساعد القرارات المتخذة الآن على تمكين الشركات من ترشيد وتوحيد وإنشاء عمليات أكثر قابلية للتكرار. يجب أن تتطور إستراتيجيات عمليات التطوير لإدخال أساليب تواصل وتعاون جديدة ومرنة تؤثر بشكل متزايد على بيئات العمل المجزأة والبعيدة وغير المتجانسة (الشكل 6).



يمكن للفرق التواصل في الوقت الفعلي ، وتطوير قاعدة معرفية مركزية ، وإنشاء شبكة وصول موحدة وفورية يمكن الوصول إليها في أي مكان وفي أي وقت. إذا كان من الممكن فتح إمكانيات التعاون الكامل ، يمكن للفرق توفير وقت الاجتماع والمضي قدماً نحو أساليب تعاون أكثر كفاءة. يمكن لفرق المشروع إنشاء قنوات (يجب تحديثها) للوصول إلى ما وراء المجموعة إلى خبراء من خارج الفريق للحصول على ردود مُرحب بها ، والذكاء من المصادر الجماعية وضخ التحديات الموضعية إلى القنوات التي تم فرزها والوصول إليها عند الطلب. لكي يتسنى تمكين التعاون عبر التكنولوجيا والأعمال ، نجد أن أدوات التعاون في الأعمال الاجتماعية هي التي تحظى بالاهتمام لأنها تسمح بالمشاركة في الوقت الفعلي مع أصحاب المصلحة في الأعمال طوال عملية التطوير.

مثل هذه الأدوات لها أهمية خاصة ، حيث نجد استراتيجيات الأعمال والتكنولوجيا تتحول بوتيرة متسارعة للاستجابة لجائحة كوفيد-19 أخيراً وليس آخراً ، يمكن لأدوات التعاون عبر المؤسسات دعم إدارة مركز البيانات عن بُعد من خلال ربط أصحاب المصلحة عبر المؤسسات لمزيد من التواصل السلس بين فرق تقنية المعلومات والموردين والشركاء والعملاء.

الأتمتة الفائقة: يُعد التزويد المؤتمت إحدى قدرات عمليات التطوير الرئيسية التي توفر قدرة الحوسبة عند الطلب دون تدخل يدوي ، مما يوفر الأساس لبنية تحتية مرنة وتخصيص ديناميكي للموارد. يمكن أن يساعد هذا في التخلص من "الجهد المضاعف" (أي عمل مرتبط بشكل مباشر بتشغيل خدمة يدوية ومتكررة وقابلة للتشغيل الآلي ، وحيث لا توجد قيمة دائمة) ، والتي تمثل عقبة رئيسية في طريق النجاح. تُعد أتمتة تكنولوجيا المعلومات أساساً لأية استراتيجية لعمليات التطوير ، نظراً لأن الهدف هو إنشاء عمليات مؤتمتة وقابلة للتكرار. ولكن في عالم ما بعد كوفيد-19 ، من المرجح أن تكون الأتمتة أكثر أهمية من أي وقت مضى بسبب الحاجة إلى التعلم والتحسين المستمر. تدفع جائحة كوفيد-19 الحاجة إلى تبسيط العمليات وجعلها أقل اعتماداً على الإنسان ، ويبحث المؤسسات على استكشاف قيمة المستوى التالي من الذكاء الاصطناعي السحابي وخدمات التعلم الآلي.

تتسع حسب الحاجة ، مما يوفر التكلفة الأولية ويسمح لبيئة السحابة بالنمو حسب الحاجة. مع تسريع المؤسسات لبرامجها السحابية - كما هو الحال الآن - يمكن أن يعمل نهج الرفع والتحويل على دمج مراكز البيانات أو تجنب تكلفة تحديث البنية التحتية. يمكن أن تتضمن برامج تحديث السحابة عمليات التطوير لمواءمة تطوير تكنولوجيا المعلومات والعمليات التجارية وتحقيق سرعة أكبر في التسليم مع الحفاظ على المرونة في أوقات عدم اليقين.

تُعد أدوات أتمتة النشر المستمر والبناء المستمر هي السمات الرئيسية لعمليات التطوير في الوقت الراهن ، وهي مدعومة بأدوات أتمتة الاختبار. إن المؤسسات الأساسية هي تلك التي يجب أن تفكر في الترحيل السريع إلى السحابة الذي يوفر السرعة في السوق والمرونة خلال الفترات الضبابية ، مثلما هو الحال الآن. يجب أن تكون المنظمات قادرة على إظهار مدى الجاهزية والاستجابة على الفور خلال هذه الأوقات.

في ظل تفشي جائحة كوفيد-19 ، كانت هناك رغبة أقل لمبادرات الابتكار الاستراتيجية الكبيرة والمزيد من التركيز على العمل التكتيكي الذي من شأنه أن يوفر قيمة فورية ويحل مشاكل اليوم ، و الآن فمع ظهور عمليات برامج الدردشة ، عززت بيئة العمل عن بُعد اعتماد أدوات التواصل والتعاون التي تركز على فريق المشروع ، والإدارات ، والمؤسسات المختلفة. تستخدم فرق المشروع Slack و فرق مايكروسوفت وفرق أخرى داخلية تابعة لمايكروسوفت ، وركزت منصات التواصل الداخلي الأخرى على تعاون الفريق لإجراء محادثات تفاعلية وفورية ، والتي كانت بمثابة الداعم الأكبر لفرق العمل الافتراضية ، وهو توجه ساعدت جائحة كوفيد-19 على تسارعه وتيرته. على سبيل المثال ، سجلت فرق عمل مايكروسوفت 4.1 مليار دقيقة اجتماع يوميًا في أبريل مقارنة بـ 900 مليون في منتصف مارس ، بينما تضاعفت قاعدة المستخدمين النشطين يوميًا إلى 75 مليونًا من 32 مليونًا. وبالمثل ، وخلال الربع الأول من العام المالي 2020 ، أضافت Slack 90.000 مؤسسة جديدة ، منها 12.000 عميل مدفوع الأجر (زيادة بنسبة 28% سنوياً) عند العمل عن بُعد على وجه الخصوص ، تكون أدوات التعاون ذات قيمة هائلة على مستوى المشروع لأنه

في ظل جائحة كوفيد-19 هناك رغبة أقل لمبادرات الابتكار الاستراتيجية الكبيرة والمزيد من التركيز على العمل التكتيكي الذي يوفر قيمة فورية ويحل مشاكل اليوم ، الآن



المنتج. يعكس هذا التطور كيف نقلت أدوات CAD (التصاميم المنفذة بواسطة الحاسوب) الهندسة المعمارية من هندسة المواد إلى التصميم. في دراسة أجرتها Flexera ، أفادت 73% من المؤسسات بوجود فريق سحابي مركزي أو مركز امتياز سحابي، متمرساً في تقنيات السحابة والخدمات المصغرة وتقنيات واجهة برمجة التطبيقات API.

بالإضافة إلى إنشاء فرق المنصات، يتم ترقية المهندسين المعماريين داخل المؤسسة لحل تحديات الأعمال متعددة الأبعاد نظراً لانتشار التقنيات والأجهزة المترابطة، مع تفشي جائحة كوفيد-19 ، تشهد عمليات التصنيع / السلع المعبأة الاستهلاكية ، الرعاية الصحية ، التعليم ، السفر والضيافة وكذلك حكومات الولايات والحكومات المحلية، تدمير سلاسل التوريد التقليدية. يمكن أن يتيح هذا فرصة فريدة للمهندسين المعماريين للعمل مع الأعمال التجارية لطرح حلول جديدة تمكن المرونة المؤسسية لسلاسل التوريد من الجيل التالي.

العمليات المتكاملة في الأفق: تواصل المؤسسات المضي قدماً في استراتيجية عمليات التطوير و "التحول إلى اليسار"، والانتقال إلى ما وراء البنية التحتية واستخدام عمليات التطوير بنجاح لتحقيق بناء متسق وألية فحص مؤتمتة، على الرغم من البيئات المختلفة.

لقد تبنت المؤسسات -التي قطعت شوطاً طويلاً في مسيرتها - عمليات التطوير لمن أجل تحقيق الأمن المتكامل عبر عمليات التطوير ، من خلال دمج الأمن في عملية تصميم التطوير. يقول شانون ليتز ، قائد ومدير معهد عمليات التطوير "بشكل أساسي ، يصبح الأمن أحد قيود التصميم ، إن نموذج التحول إلى اليسار ... يتطلب تضمين الأمن في البرنامج بدلاً من تثبيته. وتابعت قائلة "إن التحول إلى اليسار يتطلب من الجميع معرفة كيفية التعاون وفهم ما يكفي من السياق لضمان سلامة ذلك التطبيق.

أشارت تيلسترا ، وهي شركة اتصالات أسترالية ، إلى حدوث تحسن بنسبة 20-30% في مهارات التشفير الآمن بين مطوريها. تقول آلانا براون-مدير أول في Puppet ، ومنشئ التقرير السنوي عن حالة عمليات التطوير ، "أعتقد أن هناك فكرة خاطئة

بالإضافة إلى ذلك ، بالنسبة للمبادرات الجديدة ، يجب التفكير ملياً في التطبيقات السحابية الأصلية للبنية التحتية الجديدة ، والتي تعمل على أتمتة تكنولوجيا المعلومات وتبسيطها وعمليات التطوير مع التزويد المؤتمت والنشر بدون توقف، والبنية الهيكلية للخدمات المصغرة التي تدير المخاطر والتقلبات بسهولة أكبر .

إعادة تصور الأدوار التقليدية: أجبرت السحابة أيضاً العديد من المؤسسات على إعادة تخيل الأدوار المجربة والحقيقية ، والابتعاد عن فرق المجال القائمة على الصوامع التي تتولى إنشاء الخوادم والشبكات كتركيز واحد وتوجه نحو إنشاء فريق "منصة" سحابية كاملة وشاملة يقدم خدمات سحابية يمكن للمطورين استخدامها لتقديمها لعملائهم بطريقة آمنة ومتوافقة. هناك تحول أساسي في الصورة الذهنية من نموذج مركز القيادة والتحكم في تكنولوجيا المعلومات إلى نموذج تقنية المعلومات كخدمة المرتكز على العميل حيث تدعم تقنية المعلومات نموذج تشغيل يتمركز حول العميل ويركز على المنتج. يمثل هذا تحولاً من دعم العمليات المركزية إلى قدرات العمليات المضمنة. تعمل هذه الإمكانيات على تحويل فريق المنتج إلى نموذج فريق متكامل مختلف تمامًا مع أهداف وغايات مشتركة حول منتج لتحقيق توافق أكبر.

يتحدث أنتوني إدواردز ، كبير مسؤولي التشغيل بمؤسسة (Eggplant Software)، عن نشأة عمليات التطوير هذه ، قائلاً: "إن الجمع بين التطوير المرتكز على العميل ، والخدمات المصغرة ، وقنوات المعلومات لعمليات التطوير المؤتمتة يدفع دور المطور بعيداً عن التركيز على الترميز، بل يوجه اهتمامه نحو المزيد من تصميم

لقد تبنت المؤسسات التي قطعت شوطاً طويلاً في مسيرتها، عمليات التطوير والأمن لتحقيق الأمن المتكامل عبر عمليات التطوير - من خلال دمج الأمن في عملية تصميم التطوير





تشهد البنية التحتية غير المتجانسة هذه تحولات في الاستهلاك تجعل السحابة - نظرًا لمرونتها - حلاً مناسبًا. في الوقت نفسه ، تنشئ نقاط وصول جديدة ومساحة كبيرة للهجمات الإلكترونية.

أدت التغييرات التي تم إجراؤها على الموقع إلى جعل أمان المحيط الخارجي أمرًا عفا عليه الزمن، مما يستلزم التحول إلى نماذج الأمن الموحدة التي يمكنها إدارة الأمن بشكل أفضل عبر طبقات البنية التحتية والأجهزة التقنية.

أخيرًا، تم تغيير أساليب العمل إلى طرق أكثر عمقًا، مما يدفع المؤسسات إلى مضاعفة أفضل ممارسات عمليات التطوير التي تزيد من التعاون وتقدم أساليب جديدة لعالم موزع. يمكن للمؤسسات أن تتطلع إلى مضاعفة التطوير السريع، وتبني عمليات الدردشة من أجل التعاون الافتراضي، وأتمتة إجراءات عمليات التطوير التي تستمر في التحول، والدخول في أدوار جديدة لدعم نموذج تشغيل تقنية المعلومات كخدمة. يمكن أن يساعد هذا المزيج من الحلول متعددة الوسائط السحابية، والأمن الموحد، وعمليات التطوير الموزعة في إنشاء مستقبل من البنية التحتية للأعمال التي تدعم السحابة اللازمة لإنجاح البنية التحتية للأعمال الافتراضية.



كبيرة مفادها أن عمليات التطوير تدور حول تحويل بعض اختبارات الأمن. ليس ذلك هو المقصود. يتعلق هذا الأمر بتغيير جذري في كيفية عمل كل هذه الفرق معًا وكيفية تعاونها ... التعاون حقًا أمر أساسي ، وهو يؤدي بالفعل إلى نتائج أفضل.

يتمثل التحدي التالي في كيفية نقل العمليات والحوكمة ودعم العملاء إلى اليسار، بدأت الشركات ، مثل مختبرات Concourse التي تلقت مؤخرًا 15 مليون دولار أمريكي في تمويل السلسلة أ وتقدم امتثالًا للسحابة المؤتمتة ، في الظهور لتناول هذه المجالات، تستخدم المنصة نظامًا للتسجيل (بما في ذلك سياسة المؤسسة ، والهوية ، وتاريخ استخدام السحابة) لإنشاء خطوط أساسية وتنبؤات وتمكين الكشف التلقائي عن السلوك الشاذ بالإضافة إلى اختبار إصدارات التطبيق مع المبادئ التوجيهية للأساليب العلاج المقترحة .

الخلاصة: ماذا بعد ينتظرنا من تحديات

خلفت جائحة كوفيد-19 آثاراً سلبية على الأعمال و الموظفين وأماكن العمل بطرق دراماتيكية و أجبرت المؤسسات على التفكير في احتياجات البنية التحتية المستقبلية وتسريع انتقالها إلى السحابة التي يمكنها التعامل بشكل أفضل مع احتياجات الأعمال والقوى العاملة المتغيرة باستمرار، تعد الحلول السحابية المتعددة واستراتيجيات التقنية السحابية الهجينة هي المعيار لأولئك الموجودين بالفعل في السحابة ومن المرجح أن تستمر في أن تشهد تبني لهذه المنهجية بصورة متزايدة لأنها تتيح مرونة الأعمال.

من المحتمل أن تكون الحدود التالية لإدارة التعقيد السحابي متمثلة في طرح حلول متعددة الوسائط السحابية تستخدم المجموعة الصحيحة من الأدوات والبرامج و التقنية لإدارة الخدمات السحابية وتمكين تطبيقات الأعمال - كل شيء بدءًا من تنظيم البيانات من مراكز البيانات الافتراضية إلى تنفيذ عمليات الذكاء الاصطناعي.

The future of cloud-enabled work infrastructure

Making virtual business infrastructure work

CONTACT US
Federal Authority for
Government Human Resources
United Arab Emirates
P.O.Box 2350 - Abu Dhabi
T. +971 2 4036000
P.O.Box 5002 - Dubai
T. +971 4 231 9000

The magazine is licensed by the National Media Council (License No. 306) and registered as a trademark with the Ministry of Economy of the United Arab Emirates

هيئة الاتحادية | Federal Authority



www.fahr.gov.ae
hreacho@fahr.gov.ae
@FAHR_UAE
مركز الاتصال الموحد: 600525524

NESPRESSO
PROFESSIONAL

نسبريسو
MOMENTO

صممت خصيصاً لتلبية احتياجات
القهوة في مكاتب دولة الإمارات

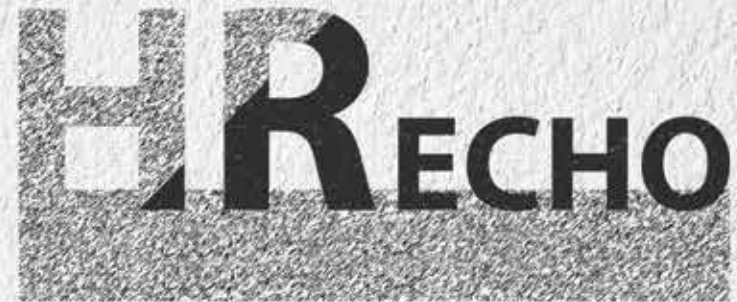


ae.buynespresso.com

what else?



800NESPRESSO
(800 637773776)



Published by the Federal Authority for
Government Human Resources

Monthly article issued bilingually by the
Federal Authority for Government human
Resources (FAHR), in partnership with leading
institutions in the field of human resources.

CONTACT US

Federal Authority for
Government Human Resources
United Arab Emirates
P.O.Box 2350 - Abu Dhabi
T. +971 2 4036000
P.O.Box 5002 - Dubai
T. +971 4 231 9000

WEBSITE

www.fahr.gov.ae

Email

hrecho@fahr.gov.ae

Twitter

@FAHR_UAE

Instagram

@FAHR_UAE

Youtube

FAHR2011

Editor in Chief

Dr. Abdul Rahman Al Awar

Editing Committee

Aisha Al Suwaidi

Ibrahim Fikri

Mahmood Al Marzooqi

Moaza Al Serkal

Asia Al Balooshi

Omar Al Balooshi

Mohammed Abu Bakr

Mohammed Al Nemer





The future of cloud-enabled work infrastructure

Making virtual business infrastructure work

Kavita Saini, Aparna Prusty, Rupesh Bhat,
and Nairita Gangopadhyay
Deloitte

COVID-19 HAS DRIVEN a fundamental shift in business-architecture assumptions. Overnight, many organizations have had to shift their cloud infrastructure strategies. In fact, in a Logic Monitor survey, 87% of global IT decision-makers agree the pandemic will Companies worldwide spent US\$34.6 billion on cloud services in the second quarter, up roughly 11% from the previous quarter.² As Satya Nadella, CEO of Microsoft, states, “We’ve seen two years’ worth of digital transformation in two months.” cause organizations to accelerate their migration to the cloud, anticipating a decline in on-premises workloads by 2025.¹ That accelerated adoption has started already (figure 1).

FIGURE - 1
Cloud strategies accelerate in response to COVID- 19

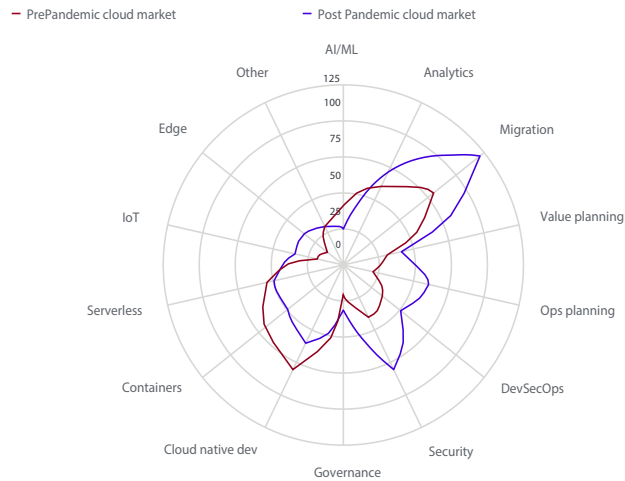
Before the COVID- 19 pandemic	During the COVID- 19 pandemic
 <p>CLOUD DEMAND 20% of enterprises expected at least half of their enterprise workload/data to be in a public cloud within 12 months.</p>	 <p>CLOUD DEMAND</p> <ul style="list-style-type: none"> • 59% enterprises expect cloud use to exceed plans due to the pandemic. • Queries for senior cloud executives in the digital realm have increased 224%. • Half a dozen global financial institutions have announced new cloud initiatives since the start of the pandemic.
<p>REMOTE WORKING 3% full-time employees reportedly worked remotely in January 2020.</p>	<p>REMOTE WORKING</p> <ul style="list-style-type: none"> • 64% full-time employees reportedly worked remotely as of April 2020. • 81% of the global workforce (2.7 billion workers) was impacted by stay-at-home orders as of May 2020.
<p>COLLABORATION TOOLS ~20 million Microsoft Teams daily active users in November 2019.</p>	<p>COLLABORATION TOOLS ~75 million (almost quadrupled) Microsoft Teams daily active users by May 2020.</p>
<p>INFRASTRUCTURE REQUIREMENT 17% desktop users and %15 mobile users accessed VPN in December 2019</p>	<p>INFRASTRUCTURE REQUIREMENT</p> <ul style="list-style-type: none"> • Microsoft Azure VPN connections grew 94%. • WAN peak traffic grew 40x since lockdowns were imposed in early March. • VPN connections grew 72% from the prepandemic levels.
<p>CLOUD REVENUES The cloud market leaders experienced considerable growth in 2019.</p> <ul style="list-style-type: none"> • 37% growth for Amazon Web Services (AWS) in Q 2019. • 22% growth in Microsoft Intelligent Cloud revenue in Q2019 3 (includes server products, cloud services and enterprise services, revenue). 	<p>CLOUD REVENUES Despite the economic recession, each major public cloud provider posted continued double-digit growth in 2020.</p> <ul style="list-style-type: none"> • 43% revenue growth for Google Cloud Platform in Q2 2020 cloud revenue. • 29% growth for Amazon Web Services in Q22020. • 27% growth in Microsoft Intelligent Cloud revenue in Q32020.

Organizations that move quickly have an opportunity to rethink how technology is enabling virtual work, workforce, and workplace and to use infrastructure as a competitive differentiator



With most of the global workforce remote, major public cloud providers witnessed a huge surge in demand for their services. Such volumes stressed traditional infrastructure (e.g., virtual private networks) and forced organizations to lift and shift to the cloud quickly, leaving room for further optimization. Stay-at-home orders made it difficult, if not impossible, to access on-premise infrastructure highlighting a key infrastructure risk.⁴ The vulnerability of tightly interlocked business and technology architectures to stress has become apparent.⁵ For these reasons, we expect to see a shift in cloud strategies toward cloud migration, security, operations, value planning, and DevSecOps (short for development, security, and operations) as well as a retraction of cloud native, container, and serverless initiatives (figure 2).

FIGURE - 2
COVID19- is a corner stone in cloud strategy and planning



Source: Deloitte perspective based on several sources.



As organizations respond to COVID-19 with a renewed cloud focus, they face IT complexity, security risk, and operational efficiency challenges. While some organizations are deprioritizing or delaying nonessential cloud migration plans,⁶ resilient leaders and organizations have an opportunity to modernize their technology backbones with scalable cloud infrastructure.⁷ When designing an approach, Deloitte’s research has shown that the “magic mix” to resolving cloud complexity is having effective tools 34%, approaches 34%, and people 32%. For many organizations, this means reigniting cloud programs and employing new strategies across development and operations (DevOps), federated security, and multicloud solutions for heterogeneous infrastructures to optimize process, mitigate risk, and manage complexity. Organizations that move quickly have an opportunity to rethink how technology is enabling virtual work, workforce, and workplace and to use infrastructure as a competitive differentiator (figure 3).

The next frontier in managing cloud complexity will likely be about building on that foundation by configuring tools, software, and technology to deliver a full-stack, multicloud solution

FIGURE - 3

Business challenges and technology infrastructure solution

 BUSINESS CHALLENGE	 TECHNOLOGY AND OPERATIONAL CHALLENGE	 TECHNOLOGY SOLUTION APPROACH
<p>Technology complexity increases with shifting consumption and access models across heterogeneous infrastructure.</p> <p>Security risks arise as tightly interlocked business and technology architectures show vulnerability to stress.</p> <p>Operational efficiency requires resilient ways of working to quickly meet shifting business needs.</p>	<ul style="list-style-type: none"> Physical data centers can no longer be accessed due to remote workplace requirements. Remote-working volumes stress traditional infrastructures, forcing lift-and-shift strategies that require greater operational efficiency. Physical infrastructure becomes inaccessible due to stay-at-home orders, expanding access points and shifting the security perimeter. Heterogeneous technology infrastructure and changes to the nature of work shift network access points and consumption. A distributed workforce that can't physically be together impacts teams and ways of working across nonstandardized infrastructure, prompting companies to implement technology infrastructure changes. 	<ul style="list-style-type: none"> Multicloud solutions (not just strategies) will support virtual work, workforce, and workplace with a focus on operational efficiency tools and platforms for a full-stack solution Virtualized data centers will enable centralized remote data access or distributed data management. Federated security manages situational awareness and access points as contexts change and encourages information-sharing for real-time threat intelligence and remediation. DevOps is a tried and true approach to achieving better value sooner, safer, and more painlessly from IT programs, and is seeing new developments in an increasingly distributed work environment.

Source: Deloitte analysis.

Multicloud solutions, not strategies, to support virtual work, workforce, and workplace

MULTICLOUD AND HYBRID cloud strategies are now the norm, with an industry study finding 93% of organizations using cloud infrastructure are employing a multicloud strategy, 87% of which are using a hybrid (public and private) cloud infrastructure model. As much as 85% of enterprises agree hybrid cloud is the “ideal”

IT operating model, with 61% efficient flow of data across the full solution architecture including storage, databases, platforms, and even security. Only then can the multicloud infrastructure efficiently and securely support business applications to drive value on an application-by-application basis.

of respondents reporting the need for application mobility across clouds and cloud types as “essential”.

As such, many organizations have moved beyond the initial challenge of selecting multiple cloud providers, determining what data to store in public or private cloud services, and managing interoperability across their multiple cloud infrastructures. The next frontier in managing cloud complexity will likely be about building on that foundation by configuring tools, software, and technology to deliver a full-stack, multicloud solution—whether that includes identity and access management, network monitoring, metadata management, or artificial intelligence for IT operations (AIOps) to manage workforce systems and platforms used to perform work.¹⁰ Multicloud solutions should consider orchestration across these tools and technologies to manage data, resources, and workflows and help ensure the most In a COVID-19 context, what can be especially challenging for multicloud solutions is finding a good application fit for those technologies, quickly. The temptation is often to leverage whatever platform or service is in a hype cycle. However, moving to an application that is not a good fit for any new platform is typically going to fail.

Organizations should first understand the application itself, understand the connected data, and the underlying architecture, and then assess if any of these new technologies is a fit. Kubernetes, an open-source project by Google to automate container deployment, management, and scaling, is an example. Flexera’s annual cloud study shows



businesses use an average of 2.2 public and 2.2 private clouds¹¹ and 20% of organizations are using Kubernetes in production or for development and testing.¹² But that doesn’t mean others should rush to use Kubernetes. Instead, companies could do well to think about what cloud management resources are needed to support the underlying business application—in this case, remote work infrastructures and collaborative working environments—and work back from there to select the right tools that bring the right services (figure 4).

FIGURE - 4
Developing IT infrastructure that powers the future of work, workforce, and workplace

NEW CHALLENGE	WHERE WE WERE	WHERE WE'RE GOING	BENEFITS
DATA CENTERS			
On-premise data centers face business continuity risk.	Virtualize data centers for long-term workload-management gains.	Build common data services with a single virtual database or by managing data in a distributed way.	Eliminate redundancy and enable data understanding, API connectivity, and enhanced governance.
IT			
Shifts in consumptionheterogeneous infrastructureincrease IT complexity.	Embrace multicloud across already and hybrid cloud strategies that are now widely accepted as the optimal strategy.	Develop multicloud solutions that focus on access, network management, operations, and end-point complexity for a full-stack solution. management, operations, and end-point.	Achieve flexible consumption models with improved cost governance.
OPS			
ITOps continues to evolve beyond CloudOps.	Implement CloudOps.	Extend CloudOps to include AIOps, which goes beyond reactive monitoring to automated response.	Enable predictive monitoring.

Source: Deloitte analysis.



A few key considerations for managing multicloud infrastructure, perhaps even more important now in a pandemic-ridden world, include building common data services, managing heterogeneous infrastructures, resolving endpoint complexity, and embracing new methodologies in IT operations (ITOps) including AIOps.

- **On-premise data centers face business continuity risk:** Organizations' inability to access the workplace, including on-premise infrastructure, during the pandemic has made virtualizing the data center a hot-button issue for business continuity risk. If it is done right, there is historical evidence of long-term gains for organizations. For example, a fintech giant saved millions by moving tens of thousands of workloads into the cloud to reduce its data center footprint.¹³ There are two paths to building common data services: one that consolidates the data into a single physical or logical database or database systems and another that manages the data in a distributed way, leveraging virtualization to look at all the data as a single database, even though they are different distributed databases, using different database models. Whichever approach the organization chooses, the idea is to have a single path to unique customer, sales, product, and other data. This approach can allow organizations to:
 - Eliminate redundancy for increased efficiency and managed infrastructure cost
 - Understand the database in great detail, along with the metadata
 - Select the right database technology to suit their needs, understanding that generally cloud-native databases are the best choice

- Enable the database service with API or web services access
- Implement governance, security, and management services
- Virtualized data warehousing has allowed large retailers, such as The Home Depot, to react faster to consumer needs across its supply chain. The Home Depot tracks more than 50,000 items across 2,000 locations, analyzes what items are sold when and where in real time with the internet of things (IoT), the edge and the cloud, and course corrects accordingly.
- **Heterogeneous infrastructure sees shifts in consumption and increased end-point complexity:** Organizations are no longer managing systems in a single data center. They're managing the mobile network, IoT devices, and the edge. Together they amplify data complexity (as in The Home Depot example). This trend toward a heterogeneous infrastructure already was underway, but COVID-19 has shifted consumption models across that network by changing where the workforce is and how work is happening. Those who already had cloud infrastructure benefited from being able to scale down workforce infrastructure costs for their unused infrastructure or increase resources in places where they saw more demand. After all, airlines, retailers, and insurance companies' business models and workforce needs were all impacted differently by the pandemic and, therefore, their data and infrastructure demands to support the workforce will all be different. For example, due to remote working, cloud consumption at Audi Business Innovation GmbH, a unit of Volkswagen AG-owned carmaker Audi, jumped 12% between March and April, with employees using more of the rented, remote computing power and software tools. Given the organization was in the cloud already, it was able to adjust consumption models and platforms with an expectation to reduce spend by 30%. COVID-19 has changed Making virtual business infrastructure work the composition of what work



organizations are sending to their off-premise data centers, how they're accessing networks via nonstandardized channels, and what volume of on-premise IoT, mobile, edge, and cloud data needs to be managed across the network with shifting access points. All of this can increase complexity.

Chances are the company's infrastructure already was a collection of many different platforms, some hosted on the cloud, and some on premises, so to manage the shift in device consumption due to the pandemic (workers at home on laptops and mobile phones, off the corporate network) organizations need to understand the interfaces, security models, and governance models and go from there. Managing heterogeneous infrastructure often starts and ends with taking an overall system inventory and then creating a management plan to implement cloud operations or cloud operations (CloudOps), which combines network, security, performance, device management, and help desk tasks, can streamline operational process design to a physical operating model inclusive of tools and technologies. Organizations can look to manage end-point complexity by reducing the number of endpoints under management, minimizing the number of system types (processor, operating systems, databases), and using management, governance, and automation tools to manage the remaining complexity.

- **Embracing new methodologies in ITOps including AIOps:** Given the need to focus on CloudOps, one evolving area within CloudOps is AIOps. In cloud infrastructure monitoring, there has been an evolution from reactive monitoring to predictive monitoring, and now we are moving on to a new era of AIOps. The use of AIOps and other modern monitoring and management tools provides the mechanism to create layers of automation that are able to react to events and launch corrective processes (such as spotting packet errors coming from a single network device and temporarily routing around

that device until it's replaced). AIOps tools as well as other operations tools are able to analyze the data coming from all systems and devices to determine when something is failing—and they can do so before humans can. If configured properly, they can detect anomalous behaviors and launch corrective processes. Prior to the pandemic, several AIOps vendors were acquired by infrastructure automation organizations as part of a growing AIOps trend which we expect to continue.

Federated security for the future of work, workforce, and workplace

WHILE COVID-19'S IMPACT on work, workforce, and workplace has forced IT to manage increasingly heterogeneous infrastructures with new tools and techniques, many infrastructures themselves are facing new security challenges, given that the where, what, and how of work has changed. As IT focus shifts to accommodate the new ways work is being done across altered workplace locations, the very context for security monitoring with an entirely new infrastructure composition—use of home internet, personal mobile devices, etc.—has changed. This has reinforced a need to focus on federated security strategies known for their success in managing distributed, heterogeneous infrastructure security across tiers, and driving situational awareness.

Federated cloud frameworks allow organizations to deploy, integrate, and manage multiple cloud computing services. They can help define and implement federated security protocols across the application, network and system layers, and the cloud security center. The focus should be on proactive defense monitoring (early warning, command, and control) and managing access point attacks against malware, advanced persistent threats and network intrusions across infrastructure tiers, data storage, trusted platforms, websites, and operating systems. All this should be done to help enable dynamic threat information sharing. The US Department of Homeland Security, for example, created a cyber defensive and intelligence-sharing ecosystem that incorporated various defensive technologies (aspects of its moving target defense and cloud systems security) into federations of enterprises across a network of organizations to enhance security against known and novel attacks. As federated security has matured, organizations are increasingly focused on web services, security-as-a-service for a cloud federation, multicloud environment, blockchain-enabled frameworks, and network ecosystems (figure 5).

FIGURE - 5

Federated security for the future of work, workforce, and workplace

NEW CHALLENGE	WHERE WE WERE	WHERE WE'RE GOING	WHY ARE WE GOING THERE
IT SECURITY			
<ul style="list-style-type: none"> A heterogeneous IT infrastructure requires a heterogeneous security model. 	<ul style="list-style-type: none"> Implement federated security to secure infrastructure across application, network, and system layers as well as the C2 security center. 	<ul style="list-style-type: none"> Manage federated computing down to the end-point level across tiers/devices (cloud, edge, mobile, IoT). 	<ul style="list-style-type: none"> Increase situational awareness, better manage access-point attacks, and enable more dynamic threat intelligence and remediation.
ACCESSMANAGEMENT			
<ul style="list-style-type: none"> Trusted access is increasingly important in a remote world. 	<ul style="list-style-type: none"> Implement role-based access controls, centralized security management, and identity access management. 	<ul style="list-style-type: none"> Use embedded zero-anonymity security features, multifactor authentication (MFA), privileged access management (PAM). Consider a trusted internet connection policy. 	<ul style="list-style-type: none"> Enhance governance of network access.
PERIMETER SECURITY			
<ul style="list-style-type: none"> Perimeter security becomes ineffective when the office perimeter is no longer relevant. 	<ul style="list-style-type: none"> Perimeter security for the physically protected data center needs to consider access points for those that need remote access, where possible, and virtual alternatives that will require new security models. 	<ul style="list-style-type: none"> Look to replace perimeter-level security with device-level security; virtualize services and desktops, and remote IoT devices; and secure every component, including object repositories, network segmentation, and web services. 	<ul style="list-style-type: none"> Manage security across a shifting threat surface area.
INFORMATION SHARING			
<ul style="list-style-type: none"> Security information-sharing and collaboration becomes increasingly challenging across distributed teams and multiple cloud solutions. 	<ul style="list-style-type: none"> Implement IM solutions across the federated network. 	<ul style="list-style-type: none"> Shift away from single-vendor IM solutions to integrated, federated IM solutions to fully leverage the cloud providers' technology. 	<ul style="list-style-type: none"> Enhance security system interoperability, collaboration, and information-sharing. Avoid vendor lock-in.

Source: Deloitte analysis.

These trends will likely continue to develop, in addition to several new ones introduced by remote working orders, triggering new work infrastructure related to trusted network access, perimeter-based security, federated instant messaging (IM), and federated computing down to the end-point level.



- Heterogeneous security for heterogenous IT infrastructure:** As organizations look to secure a multitiered architecture encompassing the cloud, the edge, mobile, and IoT, they have to secure each architecture tier against threats specific to that tier. In fact, managing heterogeneous infrastructure requires a heterogeneous security model that is federated across the technology providers for the different tiers.²⁶ At the end-point level, organizations should combine infrastructure monitoring and remediation with DevSecOps, coupled with AI for predictive and automated threat management, monitoring, and resolution, all at the desktop/mobile device level. In a federated security model, organizations are able to reach every infrastructure tier, device, or process and close security gaps with network segmentation. With COVID-19, the attack surface is now larger as the work infrastructure network is more dispersed or distributed, increasing the importance of proactive dense monitoring across all devices that extends beyond “threat detection” to “threat remediation.”
- Trusted access in a remote world:** One industry study found that 33% of enterprise security attacks on cloud infrastructure are due to a lack of proper governance and security parameters related to role-based access control. Identity access is one of the top vulnerabilities—33% of respondents to a Sophos study reported that identity access management roles were impacted by cloud security breaches and top threats (including malware, ransomware, and cryptojacking incidents). Centralized security management is a timeless concept for managing security across distributed resources. Identity management focused on access privileges remains a cornerstone of securing the network, particularly as the new remote-working conditions have increased the remote network attack surface area. As perimeters vanish, a zero trust approach to cybersecurity can help organizations preserve

the integrity and security of their data and assets outside of the perimeter across a range of devices. The approach shifts from network-based control to identity-based principles with access controls and identity management as a key focus. With zero trust, organizations take a “never trust and always verify” approach to improve their cyber posture across individuals and devices. The US Department of Defense, for example, has embedded zero-anonymity security features built onto its federated cloud infrastructure. This empowers administrators to monitor, track, and control all software, hardware, and user access to their respective clouds in real time. In response to the pandemic, the Cybersecurity and Infrastructure Security Agency announced an interim Trusted Internet Connection Policy to deal specifically with telework. Organizations are taking a “never trust, always verify, enforce least privilege” approach to securing privileged identities. Cosmo Films, a manufacturing company, has completely transformed its infrastructure from a centralized plant/office unit to a decentralization model with access layers: “We have access layers allotted based on user needs and have given availability and accessibility of our data lake and critical information to users pan-India without any geographical or time-zone challenges,” says Jagdip Kumar, the organization’s chief information officer.



Security now needs to factor in access points for those that need remote access, where possible, and virtual alternatives—all these will likely require new security models.

- **Perimeter security of the office:** COVID-19’s impact on work location (now home) has made traditional perimeter security models obsolete. The physically protected office no longer has people working inside the perimeter. So, security now needs to factor in access points for those that need remote access, where possible, and virtual alternatives—all these will likely require new security models. Organizations should replace perimeter-level security with device-level security, virtual services, virtual desktops, and remote IoT devices, and secure every component, including object repositories and web services.
- **Integrated/federated IM solutions:** An emerging trend in federated security is the shift away from single-vendor IM solutions to integrated, federated IM solutions to fully leverage the cloud providers’ technology and avoid vendor lock-in. Amazon Web Services and Google Cloud Protocol (GCP) can now be integrated with Microsoft Active Directory, making security management across multicloud infrastructure easier.³⁶ Organizations, for example, can use GCP’s federated integration to integrate with a home Active Directory solution, which enables them to streamline virtualized security communications for faster threat detection and remediation. This shift in how people are collaborating across security is being seen at a much larger scale now across all broader DevOps practices across all of the organization.



DevOps in a distributed world and altered ways of working

MANY COMPANIES SUCCEED with small cloud migrations, but when it comes to scaling the cloud, they stumble over organizational and process bottlenecks.

This is where DevOps can streamline processes. DevOps encourages great communication and collaboration (in other words, teamwork) to foster better-quality software more quickly with more reliability.

DevOps is a culture shift. Another study found that DevOps plus cloud is a multiplier that improves performance by as much as 81%. It's no surprise then that an industry analyst firm showed double-digit DevOps tools growth in 2019, with worldwide revenue reaching US\$8.5 billion.

The easiest part of DevOps is the technology— automated scripts, continuous integration and delivery, and automated provisioning. Where organizations tend to struggle is transforming existing processes and structures to support automation and drive a culture change across a range of operations. These can be done via change management, deployment, user acceptance testing, security, compliance, and ongoing product strategy.

What's changed with COVID-19 is that when people and teams are working remotely across nonstandardized infrastructure, processes should change. This is a unique opportunity to build greenfield processes and infrastructure given that pressing organizational needs are outweighing some of the usual barriers. In the postpandemic world, when organizations recover, decisions

made now should enable companies to rationalize, standardize, and create more repeatable processes. DevOps strategies should evolve to bring in new, flexible communication and collaboration techniques that factor increasingly fragmented, remote, and heterogeneous work environments (figure 6).

FIGURE - 6

DevOps strategies can enable new ways of working

NEW CHALLENGE	WHERE WE WERE	WHERE WE'RE GOING	BENEFITS
OPERATIONS			
<ul style="list-style-type: none"> Rapidly shifting business strategies require fast reaction time and resilient solutions. 	<ul style="list-style-type: none"> Follow a shift-and-adopt strategy for incremental cloud replatforming. 	<ul style="list-style-type: none"> Double down on agile to align business and technology operations and maintain flexibility needed during times of uncertainty. 	<ul style="list-style-type: none"> Enable teams to react and respond instantaneously to focus on tactical work that provides immediate value.
COLLABORATION			
<ul style="list-style-type: none"> Remote work requires more collaborative ways of working. 	<ul style="list-style-type: none"> Embrace communication and collaboration tools for virtual, distributed teams. 	<ul style="list-style-type: none"> Use ChatOps across project teams, departments, and organizations. 	<ul style="list-style-type: none"> Enable real-time knowledge-sharing, facilitate knowledge management, and generate collective intelligence.
AUTOMATION			
<ul style="list-style-type: none"> Flexible, dynamic infrastructure requires minimizing manual human intervention. 	<ul style="list-style-type: none"> Adopt DevOps tools for automated provisioning. 	<ul style="list-style-type: none"> Move toward hyper-automation by incorporating cloud AI and ML services. 	<ul style="list-style-type: none"> Create automated and repeatable processes.
TEAMS			
<ul style="list-style-type: none"> Traditional supply chains have been irrevocably disrupted. 	<ul style="list-style-type: none"> Implement a cloud center of excellence team. 	<ul style="list-style-type: none"> Reimagine traditional roles and embrace an IT-as-a-service operating model with the architect elevated in the business. 	<ul style="list-style-type: none"> Achieve shared goals and objectives as well as greater alignment across full-stack product teams.
PROCESSES			
<ul style="list-style-type: none"> DevOps continues to shift left toward end-to-end DevOps. 	<ul style="list-style-type: none"> Shift left to incorporate DevSecOps into your DevOps strategy. 	<ul style="list-style-type: none"> Continue to shift left to operations, governance, and customer support. 	<ul style="list-style-type: none"> Standardized and consistent build and development environment; enhanced governance and customer experience.

Source: Deloitte analysis.

We expect an increased focus on agile release cycles, virtual collaboration tools, hyperautomation, and continuous improvement across the entire product life cycle as organizations continue to shift left toward end-to-end DevOps.



- **Doubling down on agile for increased responsiveness:** A shift-and-adopt strategy is the standard for incremental cloud replatforming to cost-effectively enable elastic workflows that scale as needed, saving up-front cost and allowing the cloud environment to grow with need. As organizations accelerate their cloud programs—as is the communication platforms focused on team collaboration for interactive and instantaneous conversations. These support work across virtual teams, a trend accelerated by COVID-19. For example, Microsoft Teams clocked 4.1 billion meeting minutes per day in April compared to 900 million in mid-March. Its daily active user base more than doubled to 75 million from 32 million. Similarly, during the first quarter of FY20, Slack added 90,000 net new organizations, of which 12,000 were paid customers (28% increase year over year). case now—a lift-and-shift approach can work to consolidate data centers or avoid the cost of an infrastructure refresh. Cloud modernization programs can embrace DevOps to align IT development and business operations and to achieve greater delivery agility while maintaining flexibility during times of uncertainty.

Continuous build and continuous deployment automation tools are the key features of DevOps currently, supported by test automation tools. They are the baseline organizations should consider for an agile cloud migration that delivers speed to market and flexibility during uncertain times, such as now. During such times, organizations should be able to react and respond instantaneously. With COVID-19, there is less appetite for large strategic innovation initiatives and more focus on tactical work that provides immediate value and solves today's pain points, now.

- **The rise of ChatOps:** A remote working environment has fed the adoption of project team-focused, cross-departmental, and cross-organizational communication and cooperation tools. Project teams are using Slack,

Microsoft Teams, and other internal Especially when working remotely, collaboration tools are of immense value at the project level because teams can communicate in real time, develop a centralized knowledge base, and create a consolidated, instant access network that's accessible anywhere and anytime. If the full-collaboration potential can be unlocked, teams can free up meeting time and move toward more efficient collaboration methods. Project teams can set up channels (define) to reach beyond the group to experts outside of the team to gain warm responses and crowdsource intelligence and push thematic updates into filtered channels and access them on demand. To enable collaboration across technology and business, social business collaboration tools, are gaining attention as they allow for real-time engagement with business stakeholders throughout the development process. These tools are especially important as business and technology strategies shift rapidly in response to COVID-19. Last but not least, cross-organization collaboration tools can support remote data center management by connecting stakeholders across organizations for more seamless communication between IT teams and their vendors, and partners and clients.

- **Hyperautomation:** Automated provisioning is a key DevOps capability that delivers computing capacity on demand without manual intervention, providing the foundation for flexible infrastructure and dynamic resource allocation. This can help get rid of the "toil"⁴⁶ (any work that is directly tied to running a service that is manual, repetitive, and automatable, and where there's no enduring value), which is a major roadblock to success. IT automation is core to any DevOps strategy, given the goal is to create automated and repeatable processes. But in a post-COVID-19 world, automation will likely be more important than ever because of the need for continuous learning and improvement. COVID-19 is pushing the need to streamline processes and

make them less human dependent, urging organizations to explore next-level value from cloud AI and machine learning services.

Additionally, for new initiatives, think about cloud-native applications for new infrastructure, which further automates and streamlines IT and development operations with automated provisioning and zero-downtime deployment, and microservices architectures that manage risk and volatility more easily.

- **Reimagining traditional roles:** Cloud has also forced many organizations to reimagine tried-and-true roles, moving away from silo-based domain teams building servers and networks as a single focus and driving toward the creation of a full-stack cloud “platform” team delivering cloud services that developers can use to deliver to their customers in a secure and compliant manner. There is a fundamental mindset shift from an IT command-and-control center model to a customer-centric IT-as-a-service model where IT is supporting a customer-centric, product-focused operating model. This marks a shift from centralized operations support to embedded operations capabilities. These capabilities shift the product team to a very different full-stack team model with shared goals and objectives around a product for greater alignment. Antony Edwards,



Organizations that are further in their journey have embraced DevSecOps for integrated security across development operations—integrating security into the development design process.

chief operating officer, Eggplant Software, speaks to this DevOps evolution, stating, “The combination of customer-centric development, microservices, and automated DevOps pipelines pushes the role of developer further away from a coding focus and more toward product design. This evolution mirrors how CAD tools moved architecture from materials engineering to design.”⁴⁸ In a Flexera study, 73% of enterprises report having a central cloud team or cloud center of excellence⁴⁹ versed in cloud, microservices, and API technologies.

In addition to the creation of platform teams, the architect is being elevated within the organization to solve multidimensional business challenges given the prevalence of interconnected technologies and devices.⁵⁰ With COVID-19, manufacturing/consumer packaged goods, health care, education, travel and hospitality as well as state and local governments are seeing the destruction of traditional supply chains. This can provide a unique opportunity for architects to work with the business to build new solutions that enable organizational agility for next-generation supply chains.

- **End-to-end DevOps on the horizon:** Organizations continue to push forward with a “shift left” DevOps strategy, shifting beyond infrastructure and successfully using DevOps to achieve consistent build and automated testing, despite different environments. Organizations that are further in their journey have embraced DevSecOps for integrated security across development operations—integrating security into the development design process. “Essentially, security becomes a design constraint. The shift-left paradigm ... requires security to be built into software instead of being bolted on,” says Shannon Lietz, leader and director of DevSecOps, Intuit. “Shifting left requires everyone knows how to collaborate and understand enough of the context to ensure the safety of software,” she continues.⁵¹ Telstra, an Australian telecom



company, cited a 20–30% improvement in secure coding skills among its developers.⁵² Alana Brown, senior director, Puppet, and the creator of the annual State of DevOps report, states, “I think there’s a big misconception that DevSecOps is just about shifting some security tests to the left. That’s not it. This is about fundamentally changing how all of these teams work together and how they collaborate ... collaboration really is key, and it really does lead to better outcomes.”

The next frontier is how to move operations, governance, and customer support to the left. Companies, such as Concourse Labs that recently received US\$15 million in series A funding and offers automated cloud compliance, are emerging to address these areas. The platform uses a system of record (including enterprise policy, identity, and cloud usage histories) to generate baselines and predictions and enable automatic detection of anomalous behavior as well as test application releases with proposed remediation guidelines.

Conclusion: The next frontier is upon us

COVID-19 HAS AFFECTED work, workforce, and workplace in dramatic ways and forced organizations to think about their future infrastructure needs and accelerate their movement to the cloud that can better handle constantly shifting business and workforce needs. Multicloud solutions and hybrid cloud technology strategies are the norm for those already in the cloud and will likely continue to see increased adoption as they enable business flexibility.

The next frontier of managing cloud complexity will likely be developing multicloud solutions that use the right combination of tools, software, and Finally,

The next frontier of managing cloud complexity will likely be developing multicloud solutions that use the right combination of tools, software, and technology to manage cloud services and enable business applications—everything.

ways of working have been altered in technology to manage cloud services and enable business applications—everything from orchestrating data from virtual data centers to implementing AIOps. These heterogeneous IT infrastructures are seeing shifts in consumption that make cloud—given its flexibility—a favorable solution. At the same time, it creates new access points and a large surface area for cyberattacks. Changes to location have made the perimeter-in- perimeter security obsolete, necessitating a shift to federated security models that can better manage security across infrastructure tiers and devices.

profound ways, prompting organizations to double down on DevOps best practices that increase collaboration and introduce new approaches for a distributed world. Organizations can look to double down on agile development, embrace ChatOps for virtual collaboration, automate DevOps processes that continue to shift left, and step into new roles to support an IT-as-a-service operating model. This combination of multicloud solutions, federated security, and distributed DevOps can help create a future of cloud-enabled work infrastructure needed to make virtual business infrastructure work.





مستشفى كينغز كوليدج لندن
King's College Hospital London

١٧٥ عامًا من الخبرة الطبية نقدم لك أفضل رعاية صحية بمعايير بريطانية

مستشفى كينغز كوليدج لندن في دبي هيلز
مراكز الطبية متواجدة في مرسى دبي وجميرا



طب أمراض النساء و التوليد | طب العظام | طب أمراض القلب | طب الأطفال | طب الأعصاب
جراحة عامة | طب الأمراض الصدرية | طب أمراض الجهاز الهضمي | طب الأجنة | طب الأسرة