Going Back to Work with Cisco Network Solutions for Business Resiliency

Empower a secure remote workforce and redesign the workplace

© 2020 Cisco and/or its affiliates. All rights reserved.

Contents

From continuity to resiliency 3

The role of the network 4

Business Resiliency solutions 5

Secure Remote Workforce 6

Trusted Workplace 14

Trusted Workplace solutions 15

Conclusion 20

Resources 20

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

From continuity to resiliency

Many businesses had business continuity plans in place. Those plans were designed to address any temporary emergency imaginable. Comfortable with the knowledge that these plans would address catastrophes that include broadband connectivity outages, earthquakes, fires, regional power outages, hurricanes, and more, organizations continued on with their day-to-day business. Then the unimaginable happened.

With the onset of a global pandemic, businesses have dusted off their business continuity plans and learned they were inadequate for what they were now facing. In some cases, total company workforce relocation to home offices was needed. To reduce the impact on the business, these measures had to be acted upon literally overnight with whatever resources were available or could be procured immediately. For most businesses, their reactionary response to the pandemic has now been implemented. One thing is certain: it's imperative for organizations to reconfigure their operating models, as these changes in many cases are going to be more permanent than originally thought. To be successful in the "next normal" era, businesses must move from reactive business continuity to persistent business resiliency.



© 2020 Cisco and/or its affiliates. All rights reserved.

The role of the network

Substantial improvements and investments in digital technologies, particularly within networks, are at the core of the next normal for many organizations. Cisco's 2021 Global Networking Trends Report describes how networking is adapting to help build resilience across the workforce, workplace, workload, and IT operations. Enterprise networks were typically designed so for a majority of the workforce working from inside the corporate locations or branches. To support work-from-home users at scale, and to facilitate a safe return to the workplace for employees and guests, organizations need to rethink and redesign their network infrastructure.

Many believe that the next normal is defined by a more geographically dispersed workforce. The design of the network must support the user experience and performance that employees require to engage not only with other employees, but with customers, suppliers, and partners. All aspects of the enterprise network, including design, deployment, monitoring, analysis, and support, must consider the secure connectivity to everyone, everywhere – and to applications anywhere.

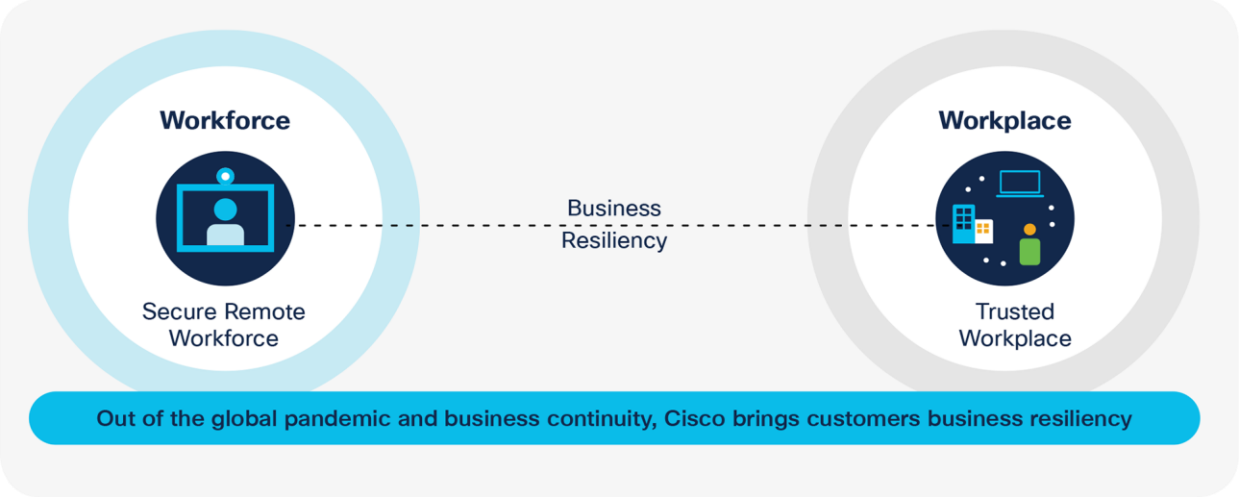


© 2020 Cisco and/or its affiliates. All rights reserved.

Business Resiliency solutions

Now more than ever, IT is being asked to design for resiliency as much as for efficiency – to accelerate digital transformation and cloud adoption while adapting to disruptions. And to not just recover in these unpredictable times but to thrive in the face of changes that are redefining work experiences. Cisco helps transform how organizations connect their people, secure their data, and automate their processes.

Cisco® Business Resiliency solutions enable you to reimagine and redesign your workforce and workplaces to provide a secure, consistent, productive, and trusted experience for your employees, customers, partners, and guests. As a part of Cisco's transformation strategy, Cisco's Business Resiliency solutions deliver on Cisco's commitment to drive the most trusted customer experience in the industry. With a breadth of portfolio offering and unmatched experience that span networking, security, cloud, and collaboration, only Cisco can deliver a complete solution that both empowers your workforce to get work done from anywhere and helps ensure safe and trusted workplace environments.

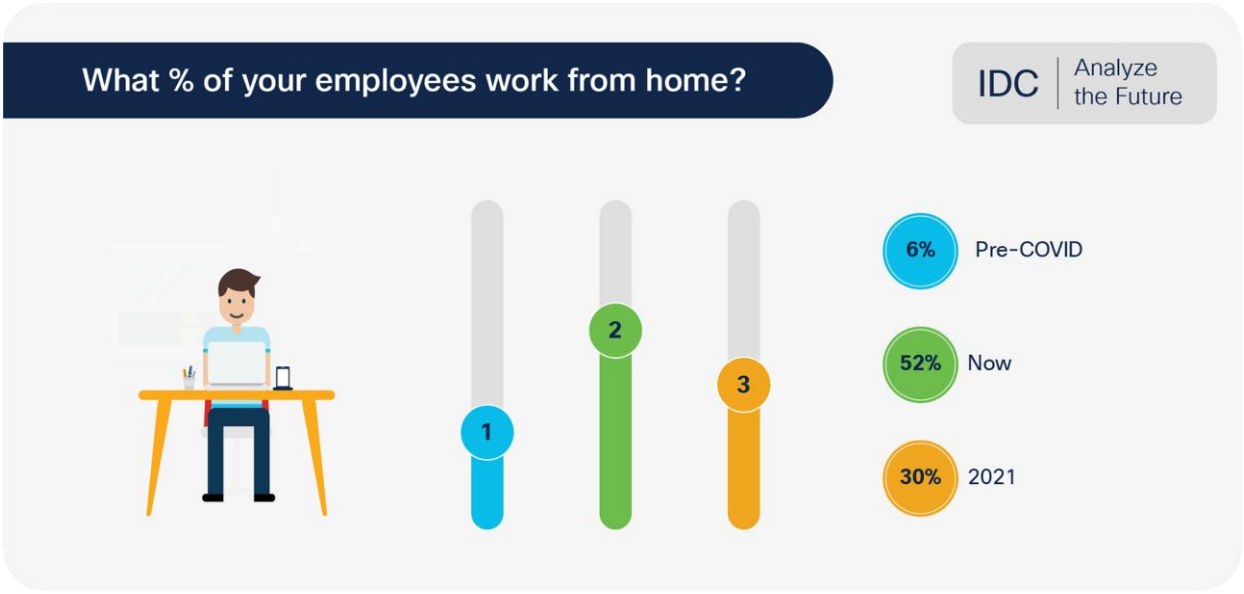


© 2020 Cisco and/or its affiliates. All rights reserved.

Secure Remote Workforce

The current pandemic has changed the way people interact and work. The idea of the workplace has transformed from office cubicles and workspaces in a commercial building to desks in sometimes makeshift offices at home.

Employees are no longer bound to a primary workplace. Over half of today's US workforce is working remotely (IDC[1]) versus 6% before the pandemic started. Many remote workers are likely to keep working from home even after COVID-19. It's estimated that 30% of the US workforce will remain remote, and it's crucial to make the network experience at home similar to that at corporate sites.



[1] IDC, COVID-19 & Enterprise Networking: Assessing the Impact, Planning for the Future, Doc # WC20200709, July 2020

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Challenges with enabling a remote workforce

Many network access solutions for remote users lack scale and critical capabilities. The provisioning and on-boarding process of some solutions can be difficult. IT administrators often manually provision new remote users one by one. And the employees' experience is also not always intuitive and simple. For instance, in many cases employees are required to configure networking devices and onboard their wired and wireless devices one at a time.

Typical challenges include:



Centralized orchestration

Lack of centralized deployment, management, and troubleshooting and not being able to monitor all distributed locations from a single pane of glass.



Application optimization

Applications are not optimized for mission-critical and cloud applications.



Zero-Trust security

Remote workers don't typically have access to enterprise-level security such as identity-based policy and segmentation.



On-demand scalability

With the growing number of remote locations – every employee's home is like a micro-office - IT is unable to scale resources easily.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Remote Workforce Network solutions

Cisco® Remote Workforce Network solutions are fundamental to achieving business resiliency. These solutions extend enterprise network connectivity to remote workers at home and at micro-offices. Going beyond traditional VPN connectivity, Remote Workforce Network solutions extend corporate policies and security to home offices for a seamless corporate experience for various needs of remote employees and IT administrators.

	Technology solution	VPN software	Wireless access point	SD-WAN router with modular LTE
	Example	Cisco AnyConnect®	Cisco Catalyst® 9105AX Series Access Points	Cisco 1000 Series ISRs
Secure connectivity to corporate data and applications		✔	✔	✔
For single user and single device		✔	✔	✔
For multiple users or devices			✔	✔
Zero-touch deployment of Remote Workforce Network solutions			✔	✔
Centralized provisioning and management			✔	✔
Corporate-level network security			✔	✔
Optimized video and voice application experience			✔	✔
Seamless onboarding of wireless and Power over Ethernet wired devices			✔	✔
Enhanced application experience via WAN optimization and SD-WAN Cloud OnRamp				✔
Advanced Secure Internet Gateway (SIG) and end-to-end segmentation				✔
Always-on connectivity via LTE				✔

With Remote Workforce Network solutions, your employees have the same level of application experience and security as they would have in a corporate office. And IT administrators can provision, manage, and automate consistent policies across all distributed home offices and micro-offices remotely and securely via a centralized management and orchestration platform. Advanced network assurance can proactively monitor remote network health and assure service quality of critical business applications as well as voice and video communications. It can also provide real-time advice with a focus on maintaining availability and suggest remediation steps when needed.

Cisco offers Remote Workforce Network solutions with wireless access points or Cisco Integrated Services Router (ISR) platforms.

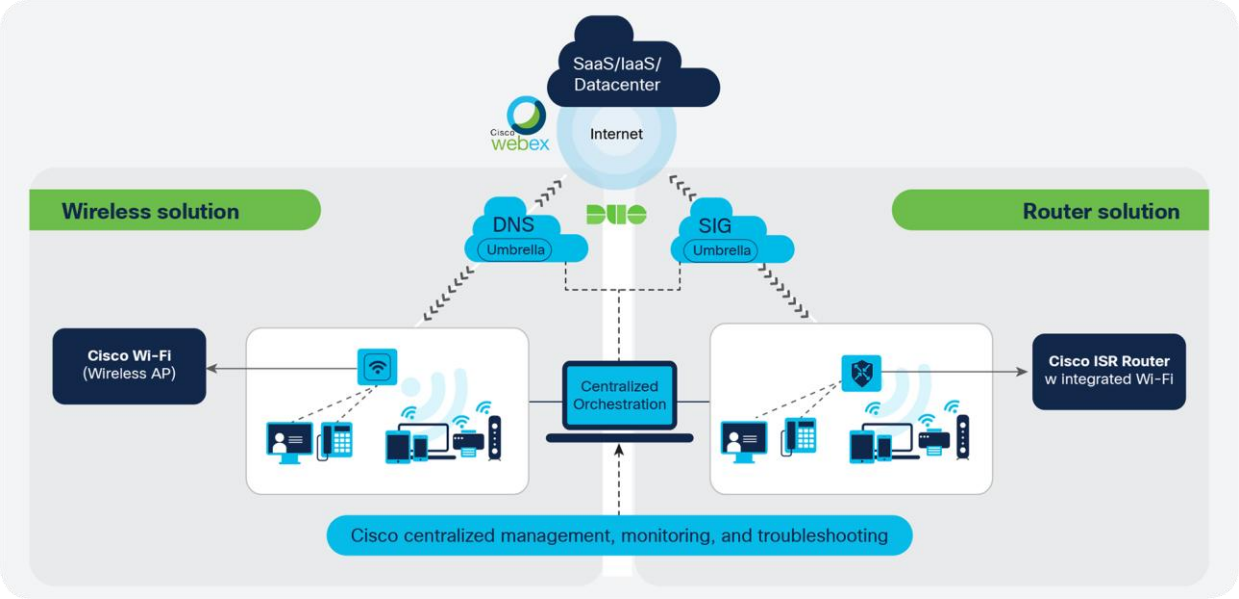
© 2020 Cisco and/or its affiliates. All rights reserved.

Wireless solution

With plug-and-play Cisco wireless access points, remote employees can connect securely to a corporate Wi-Fi or wired network and with enterprise-class identity-based policies and seamlessly onboard their wired and wireless corporate-issued and personal devices. They get an optimized cloud application experience via Cisco Application Visibility and Control (AVC), Quality of Service (QoS), and Cisco Umbrella® DNS-layer security to protect them from threats and detect compromised connections.

Routing solution

Cisco ISRs with integrated Wi-Fi deliver a zero-trust fabric with end-to-end enterprise segmentation and always-on network connectivity via its LTE (5G ready) module for remote workers. It is powered by the SD-WAN fabric and provides an enhanced application experience via WAN optimization and SDWAN Cloud OnRamp and supports advanced threat protection such as IPS, URL filtering, and Advanced Malware Protection (AMP). Optional advanced Cisco Umbrella SIG cloud security protects remote workforce direct internet access from anywhere with confidence.



© 2020 Cisco and/or its affiliates. All rights reserved.

Remote Workforce Network solutions by persona

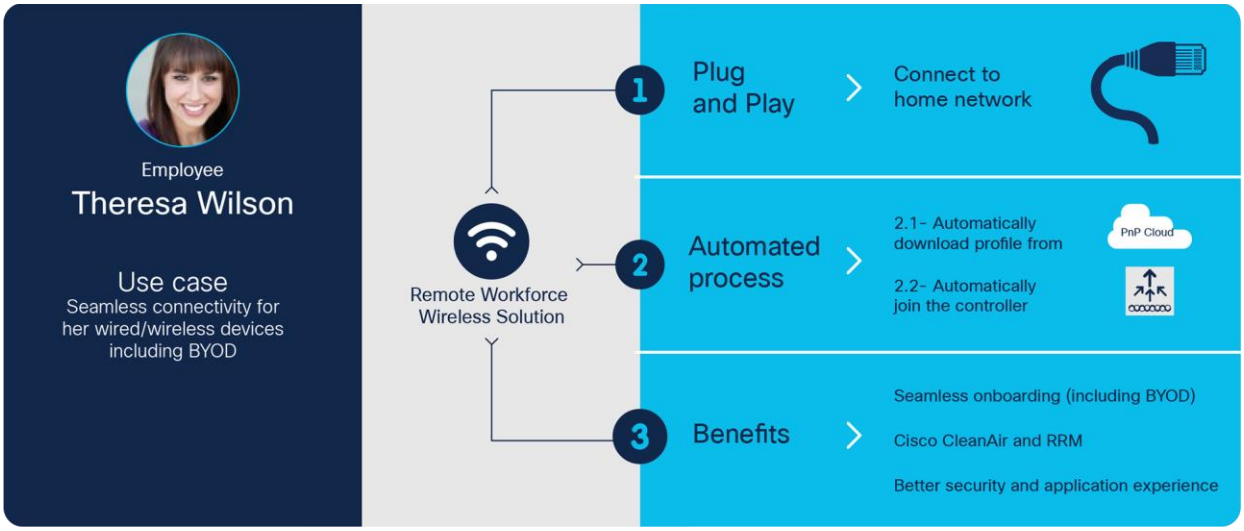
For remote employees and knowledge workers

VPNs have long been a fundamental connectivity option when working away from the office for many organizations. A VPN secures the communication channel between the employee's device and the VPN concentrator in the data center to connect to the corporate network. This means that for cloud-native applications, traffic over a VPN connection to flow through the data center, which might not be the optimal or efficient path. Also, with VPN employees can only connect their enterprise devices one by one, and many organizations prohibit them from connecting non-corporate-supplied devices.

With the mass shift to working from home, and knowing that this shift is a long-term change, enterprises have to consider that worker in a home office will require the same connectivity experience as in their company headquarters and branches. Home workers expect more than the best-effort connectivity that VPNs offer. They may need to get personal devices such as phones or tablets connected, or collaboration devices such as IP phones or video endpoints on the corporate network, as well as have the best user experience when using business applications. They also require more advanced security to protect them from cyberattacks. In short, they need seamless corporate-level connectivity and security from their home office network just as they do from the regular office network.

The Cisco Remote Workforce Wireless solution extends the corporate network into the home at scale. With plug-and-play capability, Cisco wireless access points, including Cisco Catalyst 9105AX Series Wi-Fi 6 access points, enable employees to connect securely and easily to a corporate network. And with enterprise-class identity-based policies, they can onboard their personal wired and wireless devices such as phones without the need to ever sign on to a VPN.

Cisco TrustSec® software-defined segmentation and Cisco Umbrella DNS-layer security protects remote workers from advanced threats and detects their compromised devices. Cisco CleanAir® and Radio Resource Management (RRM) technologies for Wi-Fi 6 are spectrum intelligence features designed to proactively manage the challenges of a shared wireless spectrum, which often exists in the home. They identify the source, location, and scope of radio frequency interference and can proactively guard against it.

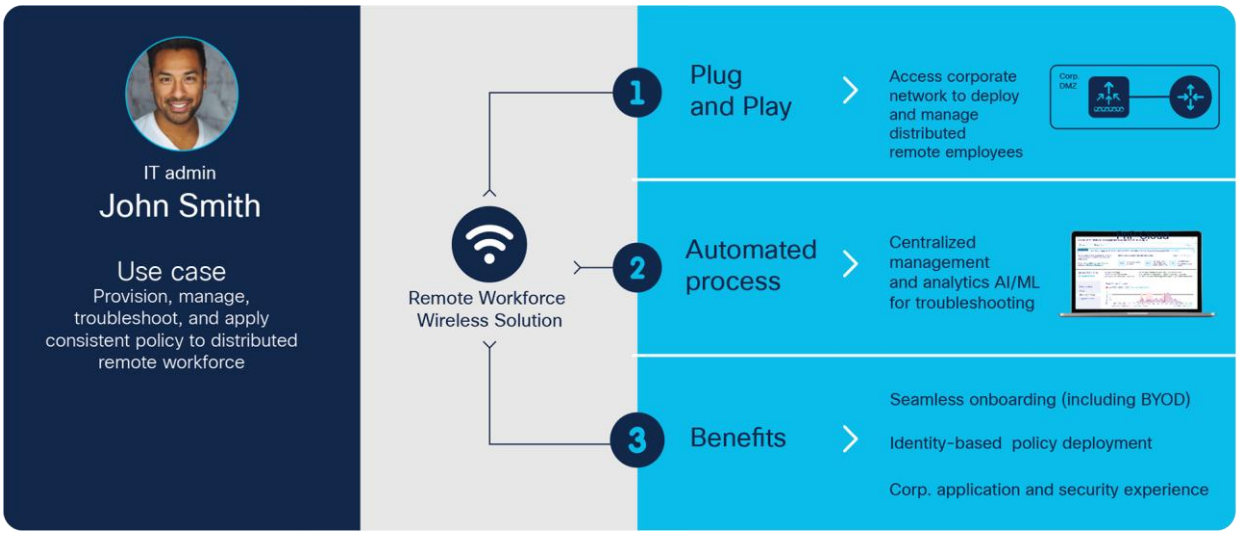


© 2020 Cisco and/or its affiliates. All rights reserved.

For remote IT administrators

With the expansion of work-from-home users at immense scale, enterprise IT teams have been grappling with the problem of how to provision, manage, and remotely monitor distributed locations. They must be able to assess end-user quality of experience, prioritize resource utilization, optimize performance, and deploy the consistent corporate policy for remote workforces. These are only possible if IT administrators have complete visibility into and control over inbound and outbound traffic of remote employees.

With Cisco DNA Center, IT administrators have full access into the corporate network from a single pane of glass. They can remotely manage, troubleshoot, and track performance and security issues. Through advanced network assurance, IT can proactively monitor remote network health and assure service quality of critical business applications as well as voice and video communications.



© 2020 Cisco and/or its affiliates. All rights reserved.

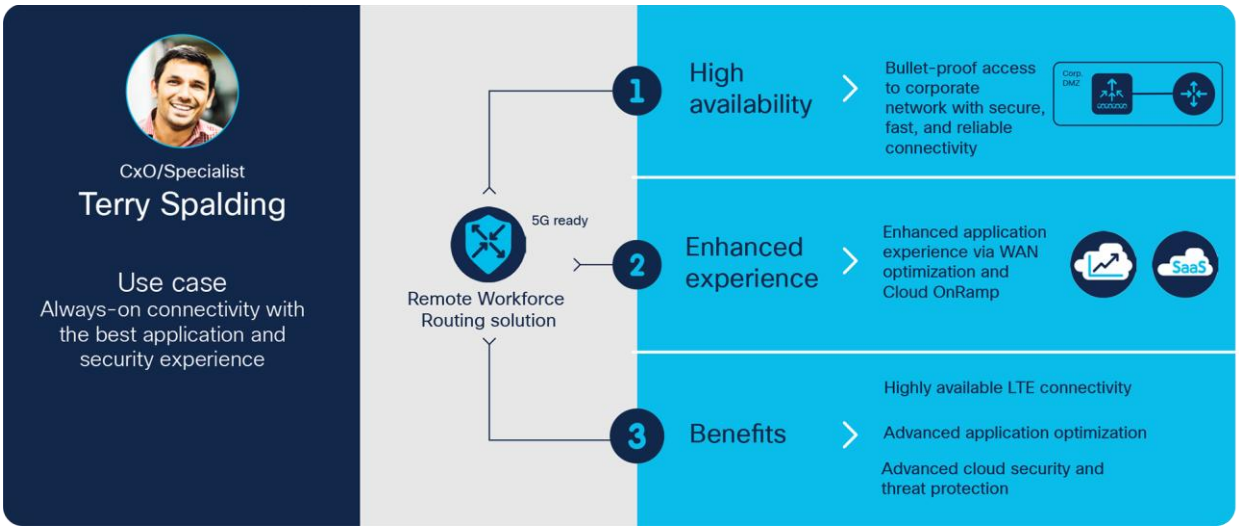
Cisco Confidential

For remote CxOs or specialists

Every employee requires a secure and reliable connection to the resources they need in order to be productive. For some, a simple VPN connection over a single broadband modem may be sufficient. However, for a growing number of people working remotely, consistent and highly available access to the corporate network with secure, fast, and reliable connectivity is critical – and running redundant broadband lines to a home is just not practical.

For a CxO hosting a conference call with company employees, a financial trader managing a multimillion dollar portfolio, or a physician providing critical telehealth care to a patient, a resilient solution with integrated unified communications is crucial. For these scenarios, a secondary cellular backup transport can help ensure always-on connectivity. Another major concern is deployment and troubleshooting when IT staff cannot perform the installation of the solution physically. Centralized management is needed to enable the SD-WAN solution and ensure that it's configured and optimized. Monitoring all distributed locations remotely, from a single pane of glass, is essential.

Cisco Remote Workforce Routing solutions provide employees with advanced application optimization for the best user experience possible, regardless of whether the application is hosted on campus, in a branch, or in the cloud. High availability with LTE connectivity helps ensure that you will always have a connection, and advanced cloud security and threat protection keeps you and your information safe.



© 2020 Cisco and/or its affiliates. All rights reserved.

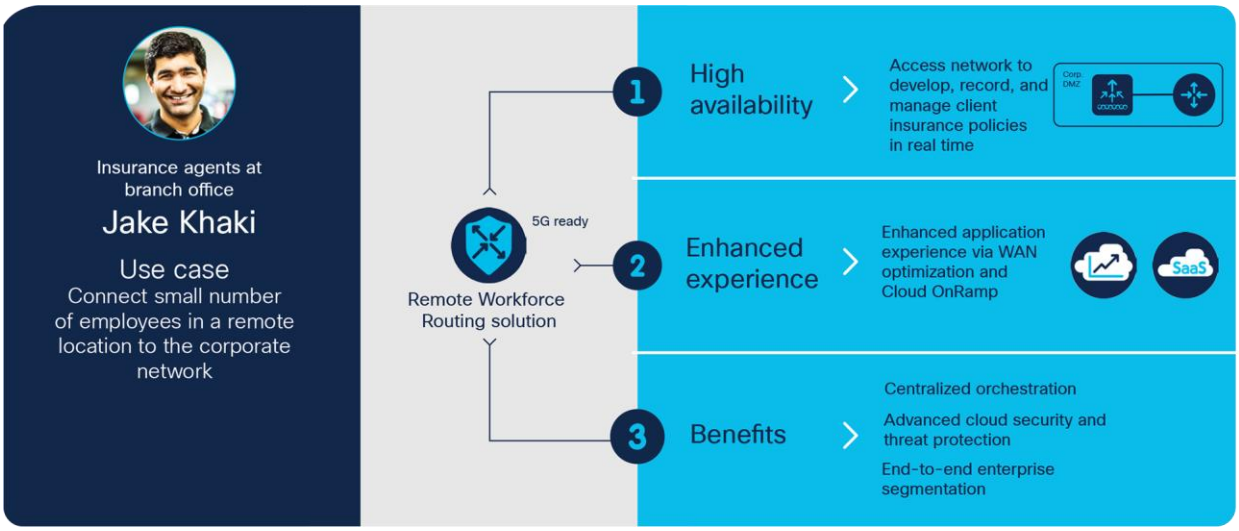
For micro-offices

A micro-office is a location that may look more like a traditional office – just smaller and maybe lacking some solutions your company centrally deploys for traditional offices.

A retirement plan advisor may work from a micro-office outside of the main corporate facility, where they can still see clients while keeping physical distancing requirements. Quite frequently, IT resources are not available at a micro-office, so equipment is shipped to the office with instructions on how to connect to power and the network, and is likely installed by a non-IT professional.

Sensitive client financial and personal information is transmitted to head offices. Cyberattacks to gain access to this information are a constant concern and could potentially put clients at risk and the advisor out of business. A Cisco Secure Access Service Edge (SASE) solution helps ensure that the right security steps are taken.

With many applications running in a SaaS environment, Cisco Remote Workforce Routing solutions provide advanced cloud security and threat protection that keeps personal information safe. End-to-end enterprise segmentation provides the ability to break networks down into smaller, more logical pieces, and organizations are able to control the access to certain segments by unauthorized users, devices, and applications – further protecting sensitive information. The traffic isolation prevents attacks from easily propagating across the entire network and turning into destructive breaches. Centralized orchestration enables central IT resources to enable the solution and manage and monitor it remotely. LTE connectivity helps ensure that financial records are always available and are up to date.



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Trusted Workplace

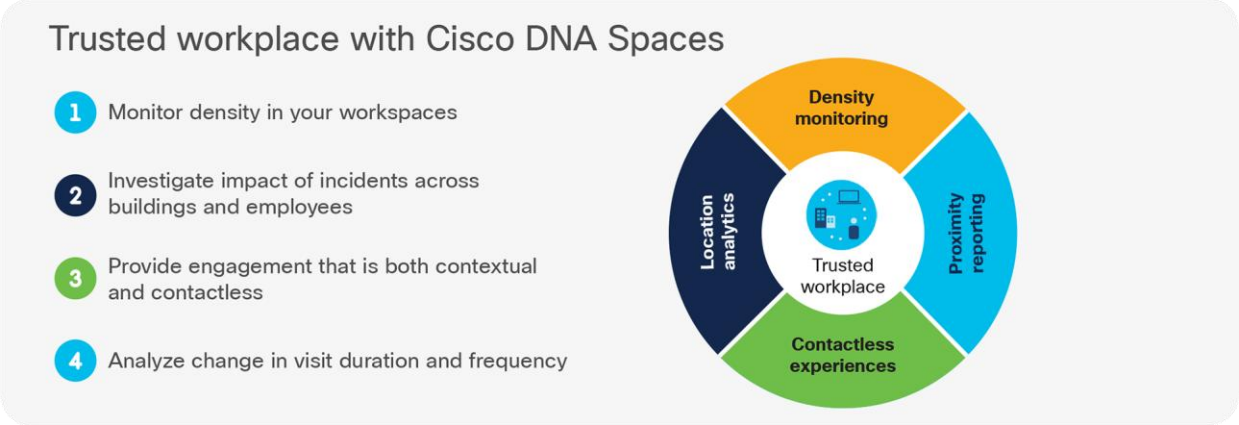
For staff that continued to be in the workplace, and for workplaces that are reopening after temporary or prolonged full or partial closure, organizations face unique challenges. Workplace resources and ops leaders must maintain a safe work environment and uphold guidelines for physical distancing. Physical space layouts may have to be reconfigured to prioritize safety and minimize unsafe behavioral patterns such as close-proximity interactions. Facilities management teams must be able to effectively communicate key safety information such as what areas to avoid, new maximum capacities, and the current number of occupants on a given floor to employees, customers, and guests.

Challenges with enabling a trusted workplace

Today, many employees are concerned and hesitant about returning to the workplace. For them to consider going back to the workplace, they are looking to their employers to have a plan in place for optimizing safety. One measure that many deem critical to safe reopening is the ability to implement reduced density in the workplace. Another is the ability to use data to respond effectively to health incidents or prevent potential transmissions. For these measures, a technology platform is needed that can provide facilities planning leaders the insights they need to monitor the situation and take the right actions to build workplace safety.

Cisco DNA Spaces

Cisco DNA Spaces can help address these challenges and requirements as organizations prepare to reopen their workplace. With a Cisco Catalyst®, Aironet®, or Meraki® Wi-Fi infrastructure, Cisco DNA Spaces, a cloud-based location services platform, can provide rich insights to improve safety and operational efficiency. In addition, with the open APIs available, customers and application developers can tailor unique apps that build upon the location services data. Many customers with existing wireless infrastructure and licenses can quickly activate and utilize these apps.



© 2020 Cisco and/or its affiliates. All rights reserved.

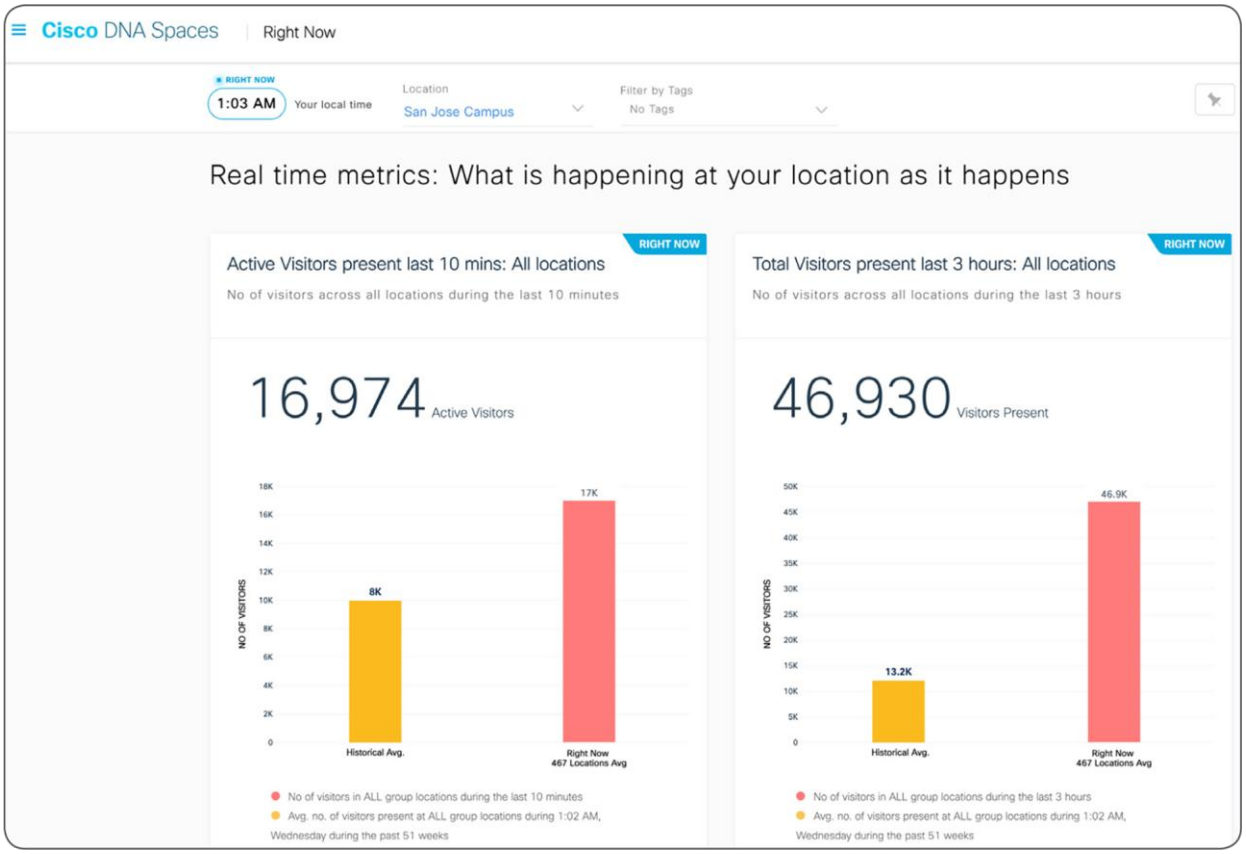
Cisco Confidential

Trusted Workplace solutions

Improve the safety of employees

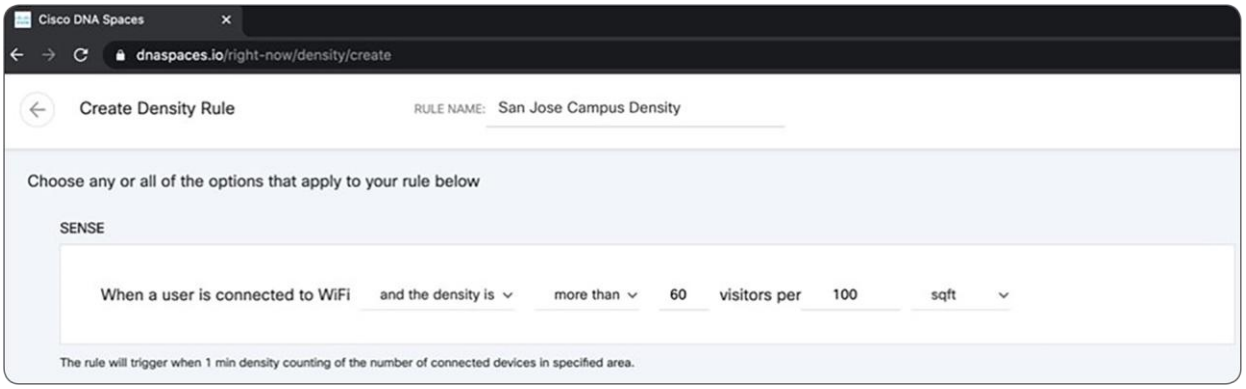
It is now increasingly common for organizations to have measures in place that allow them to effectively monitor adherence to physical distancing guidelines. Solutions that support organizations in these ways are seeing increased adoption and will continue to be relevant long after the pandemic situation has abated. Cisco DNA Spaces can provide rich insights into the location and movement of employees, visitors, and customers throughout buildings or sites. This can serve as a crucial aid in building workplace safety and well-being. Within the solution, the Right Now and Proximity Reporting apps can help monitor occupation density in premises and provide the insights needed for the organization to respond effectively when an individual self-reports as infected.

With the Right Now app it is possible to see real-time metrics into what is actively happening at locations. The number of people currently present can be monitored. To create safe capacity levels, you can set maximum density thresholds for your buildings. When those thresholds are reached or exceeded, you can trigger notifications via email, Webex Teams™, SMS, or digital signage.



© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



In the example above, note that over the last 10 minutes there were 232 active visitors and 724 active visitors in the last 3 hours. These can be filtered to specific locations through the drop-down.

Customers can set a density rule that specifies a limit on the number of devices or visitors per location, building, floor, zone, or square footage, and automatically trigger a notification via API to Webex Teams or other channel when the limit is exceeded.

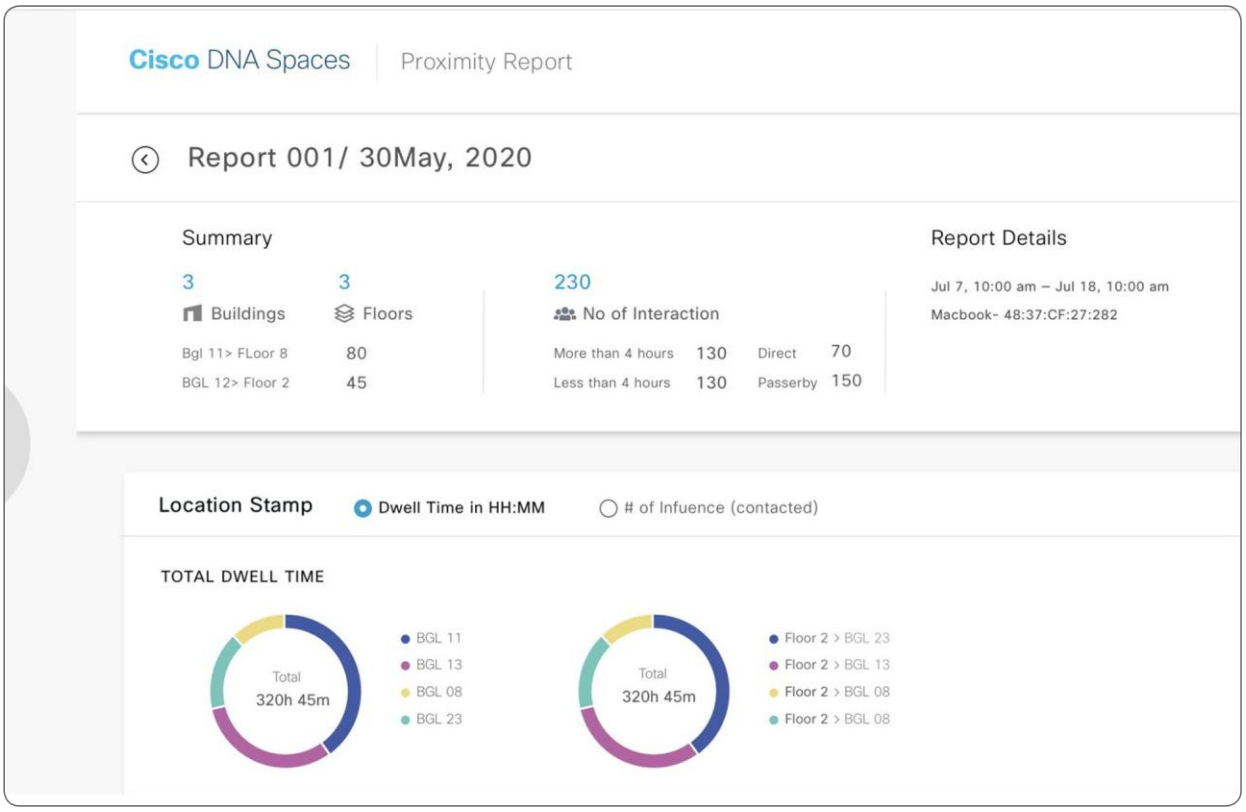
When a user self-reports testing positive for the virus, you can generate a Proximity Report of which buildings, floors, or zones that individual has visited. You can also see the potential interactions with other users or physical spaces such as meeting rooms, by location and duration. The report includes a heat map that categorizes potential risk based on proximity and duration. For example, the riskiest interactions would be those that were within 30 feet from the positively tested employee for more than 4 hours. This provides you the actionable data on how you would like to inform other people that are potentially affected. Another useful outcome would be the ability to know exactly where enhanced cleaning is needed, saving on time and cost for facilities cleaning.

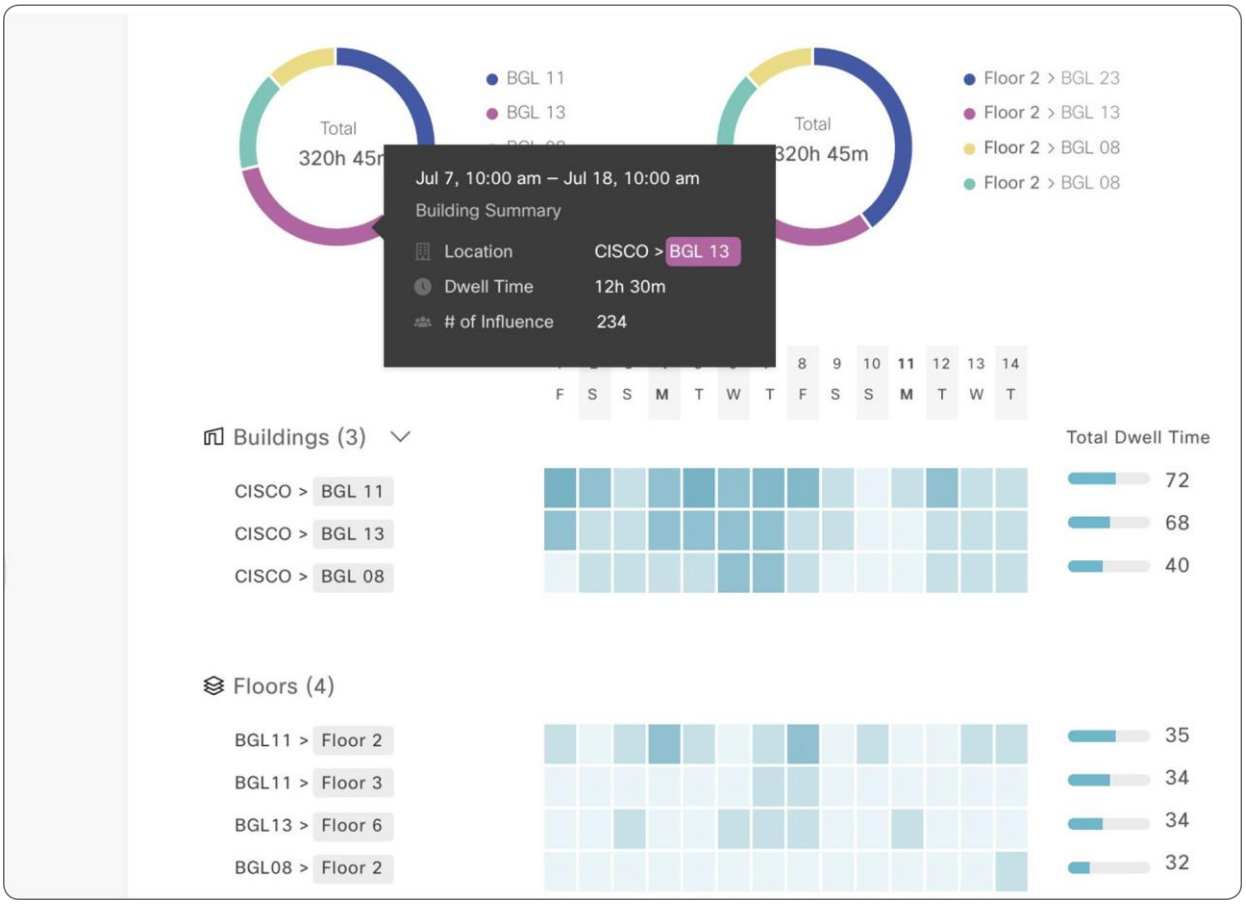
The Proximity Reporting app can be leveraged with your existing Cisco wireless access points and does not require an additional application nor hardware.

Acknowledging that location data privacy is a concern, in using Cisco DNA Spaces there is full privacy and transparency. Customers have control over the data that is stored and used. In the most privacy-sensitive model, customers can use hashed MAC addresses instead of a user ID or username. The Proximity Reporting app does not store personally identifiable details of the specific individual that self-reports. The reports generated will be auto-deleted after 30 days. Additionally, access to the reports can be limited to authorized personnel.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential





© 2020 Cisco and/or its affiliates. All rights reserved.

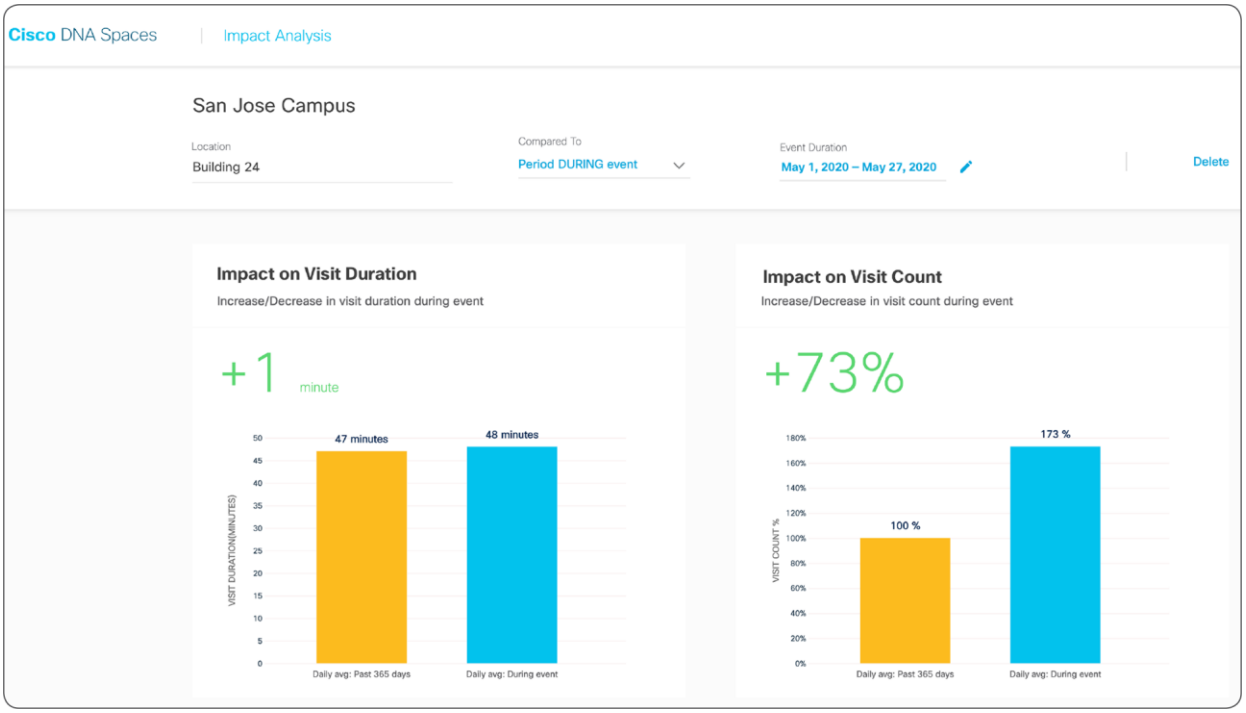
Cisco Confidential

In the example above, Proximity Reports summarizes the number of impacted buildings and floors and the number of interactions with nearby devices as well as the time spent in each. Get a daily and weekly view of which buildings were visited and the dwell time to assess the extent of impact for each building. Note that no personal details of the person nor interactions are disclosed, preserving data privacy.

Drive business decision with actionable analytics

Organizations will want to evaluate changes in how their spaces are being used. Data plays a huge role in guiding organizational decision-making and should be accessible and intuitive. Cisco DNA Spaces processes and displays the location data as robust, actionable metrics. This provides facilities and workplace resource leaders with the insight they need to make informed decisions about how employees enter the office and interact with others.

The Impact Analysis app can provide insights into how the physical spaces are currently being used, measuring the impact of an event on the behavior patterns within your location. As offices start to fill up again, you might want to assess how the visit duration and frequency have increased or decreased. The behavior patterns can be compared across locations, cities, regions, or countries for a specified time period.



At the San Jose location, the average visit duration and frequency dropped by about 3 hours and 8 visits respectively during the month of May. In comparison, at the New York location, the visit duration and frequency dropped by an average of 5 hours and 15 visits respectively during the month of May.

© 2020 Cisco and/or its affiliates. All rights reserved.

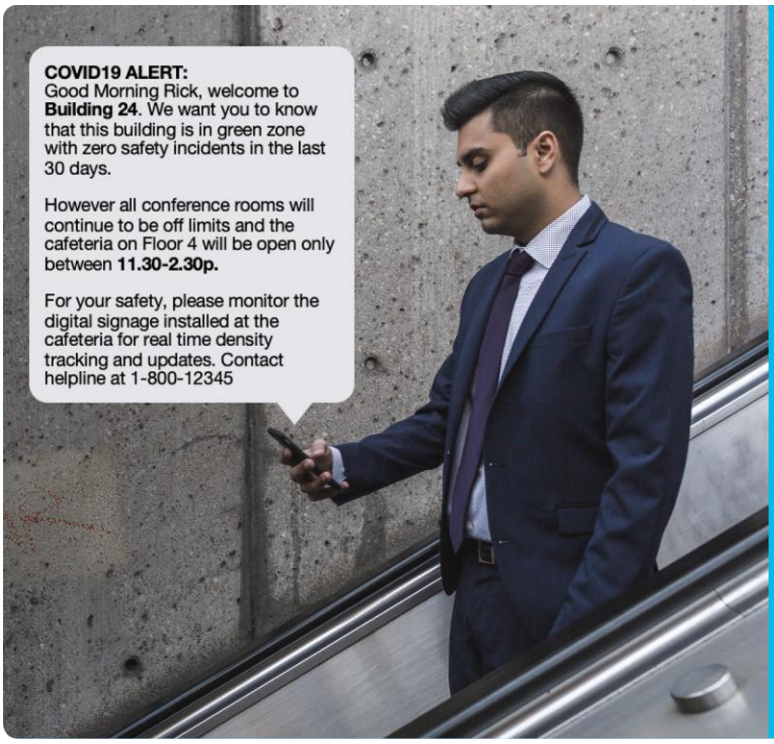
Cisco Confidential

Deliver contactless experiences

In any situation, businesses must be able to deliver valuable experiences to customers or guests in order to stay relevant and maintain customer loyalty. Contactless experiences will be a key differentiator for enterprises in the months to come. According to IDC, 45% of the Global 2000 B2B/B2C enterprises will utilize smart personalization for contextual customer engagements.

The Cisco DNA Spaces Engagements and Location Personas apps allows you to provide contactless, yet valuable customer experiences following the pandemic.

With the Engagements app, you can deliver contextual safety information based on presence at any of your buildings. Dynamic engagements are powered by a rule engine depending on building status and persona. Through the Location Personas app, you can build profiles of visitors based on their at-location behavior. This allows you to personalize engagements to make them relevant to the right audiences.



In this example, Rick can receive different SMS notifications built from the Engagements app, with the profiles created in Location Personas.

For instance, If he goes to Building 24, an SMS will display that Building 24 is a green zone with no recent safety incidents. But if he enters Building 9, he will get an SMS indicating that the building is occupied over its capacity. Lastly, in Building 17 he would receive a more alarming message that there has been a reported incident in the last 30 days, and that conference and breakrooms are closed.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Conclusion

Cisco's Remote Workforce solutions help you rethink and redesign your workplaces to provide a secure, consistent, productive, and trusted experience for your employees, customers, partners, and guests. Our solutions are designed to help you connect anyone, from anywhere, and to secure everything, with simplified remote deployment and visibility to your entire network.

The pandemic and the need to make data-driven space decisions will shape the future workplace well after the pandemic ends. Cisco's Trusted Workplace solutions provide organizations with the tools they require to rethink their spaces, whether it is being able to deliver contactless experiences or to reduce density in the buildings to allow for social distancing. When the time and situation are right, organizations must be prepared for the transition back to the workplace, and it's crucial that they do so safely. Cisco provides the technology innovation to prepare you for the next normal.

The requirements for IT to adapt to change for business continuity are nothing new. Avoiding outages has been their primary goal since the dawn of computing. However, recent global events have underscored the need to reconfigure operating models. Adapting to these significant disruptions will help your business transform and thrive in the face of change. The next normal requires solutions designed with the required flexibility and agility for persistent business resiliency.

See the solutions

Get offer

Cisco DNA Spaces 30-Day Trial

2021 Global Networking Trends Report

Business Resilience Special Edition

IDC Futurescape: Worldwide Customer Experience 2020 Predictions

Resources

- Cisco 1000 Series Integrated Services Routers Data Sheet
- Cisco SD-WAN
- SD-WAN e-book: The New Landscape of Networking
- The Road to Wi-Fi 6 eBook
- SD-WAN Security
- Cisco Cloud OnRamp

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C96-744056-00 11/20

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential