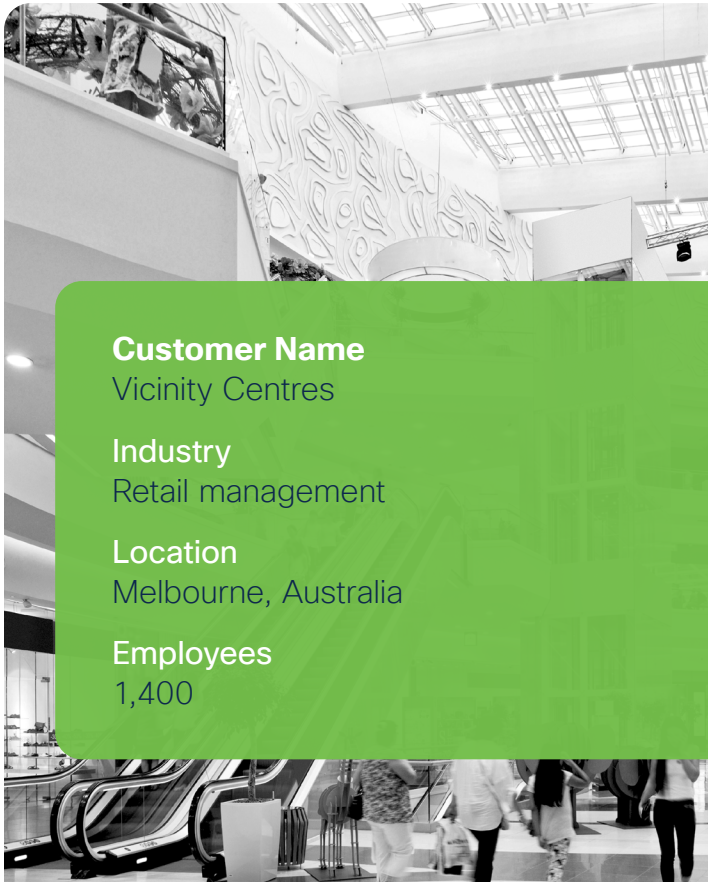
CISCO
SECURE

Case Study
Cisco Public

How Australia's Leading Retail Management Company Has Adopted A SASE Approach

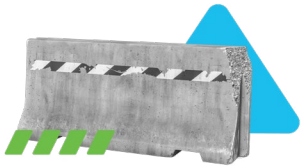


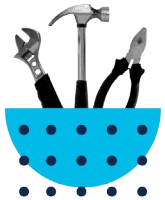
Customer Name
Vicinity Centres

Industry
Retail management

Location
Melbourne, Australia

Employees
1,400





Objective

As organisations across the world pivoted to adapt to the pandemic, Vicinity Centres needed to secure its newly remote workforce. At the same time, the pandemic became a driving force for replacing its legacy secure web gateway. The company wanted its new cybersecurity investments to not only provide robust protection for remote workers, but also support its secure access service edge (SASE) initiative.

Challenges

- A complex security environment due to remote users and different types of IoT devices connecting to the internet
- An incumbent proxy solution that lacked adequate protection for remote workers and had some reliability challenges
- The need to improve operational efficiencies and resiliency as part of a hybrid-cloud security strategy

Solution

- Cisco Umbrella
- Cisco SecureX

Impact

- Reduced internet outages and gained ability to protect users' web activity regardless of location, with full proxy for all traffic
- Secured remote workers and protected shoppers using guest wi-fi at the shopping centres
- Reduced investigation time from a day to an hour for some incidents using Cisco Umbrella Investigate

The Challenge

Fast pivot to remote work calls for enhanced cybersecurity, resiliency

One of Australia's largest retail property management companies, Vicinity Centres owns and operates 62 shopping centres. In addition to providing guest wi-fi for shoppers, these spaces rely on many digital elements that connect directly to the internet – such as digital wayfinding, digital media screens, and even counters that measure foot traffic – to fulfil the company's vision to "reimagine destinations of the future, creating places where people love to connect."

The sudden move to remote working during the pandemic and complexity of its security environment prompted Vicinity Centres to reevaluate its approach to securing the cloud edge and IT infrastructure.

The company's incumbent secure web gateway (SWG) fell short of providing adequate protection for the remote workplace. "We've had some operational challenges with the current web proxy solution, which didn't address our requirements for protecting our remote workers," David Wang, network and security engineering manager at Vicinity Centres, explains. "It also had some resiliency and performance challenges, which impacted our users. When we had a big internet outage, I realised we needed to remediate the existing on-prem web proxy solution."

The team wanted to improve performance and reliability for its users, be able to efficiently inspect and control web traffic, and better protect its remote workers. When remote employees began accessing applications directly through the internet rather than through the data centre, it further heightened the need for a new SWG.

"In an ever-evolving pandemic, we needed to improve operational efficiencies and be more resilient at the same time – and our investment in the Cisco Secure portfolio was part of that strategic IT roadmap and our move to the hybrid cloud," Glenn Ong, Head of IT Operations at Vicinity Centres says.

> "In an ever-evolving pandemic, we needed to improve operational efficiencies and be more resilient at the same time – and our investment in the Cisco Secure portfolio was part of that strategic IT roadmap and our move to the hybrid cloud."
>
> Glenn Ong,
> Head of IT Operations at Vicinity Centres

The Solution

A stepping stone towards SASE

Vicinity Centres explored a replacement SWG solution that could both secure remote workers' connections and align with the company's longer-term SASE initiative. Umbrella combines the broadest set of cybersecurity functions in a unified cloud-native service and integrates with Cisco SD-WAN, a critical element of a SASE architecture. Cisco Umbrella's capabilities supported both the current and future objectives.

Glenn says, "We introduced Cisco Umbrella during the COVID-19 crisis. Cisco Umbrella was already part of our enterprise security strategy and we fast tracked the rollout of the solution as we were able to demonstrate that Umbrella would give us many security benefits and address the security challenges imposed on us by the pandemic."

Vicinity Centres appreciates the fact they can protect both DNS and web traffic. One of the SWG capabilities that the team uses is SSL decryption, which enables them to decrypt and inspect encrypted web traffic and block hidden attacks. They also leverage Umbrella's Investigate console for a complete view of the relationships and evolution of internet domains, IPs, and files. "We had a distributed denial-of-service attack on our website. Using Umbrella Investigate, we were able to get some really good information and could clearly see a spike in DNS resolution requests. Umbrella validated that there was an attack, and we were able to provide the data as forensic evidence to law enforcement."

Currently, Vicinity Centres is exploring using Cisco SecureX to automate and aggregate threat data from Umbrella, Cisco Secure Endpoint, and Cisco Secure Email solutions. "When we looked at SecureX, we saw the benefit of having end-to-end visibility of threats from a traffic journey perspective," Glenn says. "We asked, if the platform picked up a threat, could we enforce an action over there? Could we trigger an orchestration workflow related to any threat, to protect our environment?"

"We had a distributed denial-of-service attack on our website. Using Investigate, we were able to get some really good information and could clearly see a spike in DNS resolution requests. Umbrella validated that there was an attack, and we were able to provide the data as forensic evidence to law enforcement."

Glenn Ong,
Head of IT Operations at Vicinity Centres

The Results

Improving resiliency investigation time and automation

Vicinity Centres has been able to boost resiliency and operational efficiency for the organisation, as well as tighten security for its remote employees. The migration from the legacy SWG to Umbrella was a relief for David, because he no longer worries about internet outages and disruptions to employees and customers. "No matter where our employees work, we know they're protected when they're connecting directly to the internet, and we have full visibility into all the web traffic from Umbrella's secure web gateway," he adds. "And because of the DNS-level protections in place, we gained an additional level of comfort."

For any incidents that do arise, they've been able to speed up security investigations. "For some incidents, we've cut investigation time from a day to an hour thanks to Umbrella Investigate," Glenn says. "And when we have a request to resolve an incident, we can do it 20% faster now that we have Umbrella."

As Vicinity Centres looks ahead to its upcoming cybersecurity initiatives, it plans to implement SD-WAN and use Umbrella's automated SD-WAN integration to achieve direct internet access, breakout traffic locally, and centrally manage policies for remote offices. "We're looking forward to enabling SD-WAN and to pushing Cisco Umbrella to the edge, supporting our SASE initiative. We want to allow local internet breakouts where it makes sense, and then really push the security feature to the edge level and the edge of operational technology, and segregate between IT, OT, corporate, and Wi-Fi traffic," David says. "Our ultimate goal is to continue driving business resiliency."

> "We're looking forward to enabling SD-WAN and to pushing Cisco Umbrella to the edge, supporting our SASE initiative. We want to allow local internet breakouts where it makes sense, and then really push the security feature to the edge level and the edge of operational technology, and segregate between IT, OT, corporate, and Wi-Fi traffic."
>
> David Wang,
> Network and Security Engineering Manager,
> Vicinity Centres