# Securing Agility During Crisis

## Covid-19, firewalling, and remote work




## Customer summary

**Name**
New Castle Hotels and Resorts

**Industry**
Travel and Hospitality

**Location**
U.S. and Canada

## Business challenge

- Securely supporting remote work to continue operations during a disaster
- Bringing security operations in-house to better mitigate risk and secure the enterprise

## Security drivers

- Refreshed security stack to support business continuity and remote work
- Replaced outsourced Managed Service Security Provider (MSSP) with a more effective in-house program

## Business results

- Enabled secure and fully supported transition to remote work in less than a day
- Reduced time-to-detection and remediation of systems from days to hours

### Securely enabling a remote workforce

During a disaster, how does a "Lean IT" organization, in a matter of hours, securely enable remote work for an entire staff? New Castle Hotels and Resorts operates over twenty award-winning upscale hotels in the U.S. and Canada, both franchised global brands and independent properties. Day-to-day, a single person performs all hands-on management of New Castle's in-house IT and Security functions.

Central to New Castle's business success has been turnarounds of properties requiring fresh, vibrant identities, strategic leadership, and operational efficiency. Alan Zaccario, VP of IT and Cybersecurity, is charged with aligning New Castle's business strategy with technology. For New Castle's security refresh, Zaccario focused on effective and manageable security tooling that could accommodate rapidly changing business needs and security threats.

When asked how New Castle was ready to support employee productivity during a secure work-from-home program stemming from the Covid-19 pandemic, Zaccario replied:

"Planning. We had disaster response and business continuity in mind when we recently did a security refresh.

"You must have confidence that your security posture isn't degraded with remote work. And security at the endpoint has to be transparent. It's critical, because our executive team — and every department — we're all working from home now. Our hotels are up and running with reduced staffing, and much of the daily administration is being done from home by the hotel staff. We're managing the business, and it's been non-stop. As soon as restrictions are lifted, we'll be primed to get the business back on track.

"We're an agile organization, and ahead of most of our hospitality industry peers in embracing SaaS services and applications, which has definitely helped. When the scope of the recent pandemic became evident, we were able to move corporate operations offsite to home offices within hours.

"We take pride in running a capital-efficient IT shop. We talk about security not only from cost — capex and opex perspectives — but also how security is about business enablement. Cisco gets that, and that tracks with how we think. We really can't afford a misfire with our security spend. We understand the Cisco security integrations, and how Cisco's platform approach protects our investment."

> "We had disaster response and business continuity in mind last year when we did a security refresh. We deployed AMP and Umbrella. Then, I decided to leverage that investment with Cisco firewalls."

**Alan Zaccario**
VP, IT and Cybersecurity, New Castle Hotels and Resorts

## A platform approach

Cisco's security vision is a platform approach that enables visibility and what we call the *future of firewalling* – intelligent, tightly-integrated control points everywhere they're needed, on prem, in the cloud, and on endpoints. Cisco's vision was aligned with New Castle's security strategy.

"Other companies just tout firewall appliances," Zaccario said. "Cisco isn't like other security companies that are primarily hardware or primarily software. Cisco is both. That was really important to us, because we knew we needed control on endpoints, in the cloud, and on-prem at our properties. Of all the vendors we evaluated, Cisco had the most mature integrations to bring security visibility together. But it's not just about the platform – it has to be manageable by a small shop like ours if we're going to use it.

"We deployed AMP and Umbrella on most of the laptop and company-owned PCs about two years ago. Then, I decided to leverage that investment with Cisco firewalls. And having AMP and Umbrella working, even when our people are off VPN and things like that, it's just critically important. Cisco security has definitely proven to be the correct choice, because Cisco enables a strong security posture for remote work. When the rapid move to remote work happened, my biggest concern was helping people configure local printers and scanners, not scrambling to secure the enterprise."

Another driver for New Castle's security refresh, beyond Cisco's firewalling vision and remote-work readiness, was a transition from using a Managed Service Security Provider (MSSP) to managing security in house.

"We used to use a traditional MSSP, and they were very helpful for firewall logging and some of our compliance needs, but less useful on the threat side," Zaccario explained. "We'd get lots of alerts but, frankly, most of it was just noise. In contrast, I'd say that Cisco provides answers, not alerts. That's important because we're a small shop and don't always have time to dig into the minutiae of each incident. When Cisco tells us there's a compromised endpoint, that's a high-fidelity data point. And when we do have time to drill into the threats we're seeing, we discover patterns and get a better understanding of the threat landscape and what we're up against. Even a false positive from Cisco is helpful to me, as it helps us understand more about the user and potential for future threats based on behavior."

In the transition from using a MSSP to bringing security in-house, firewall management is particularly important. Cisco offers a variety of cloud and on-premises firewall management solutions to suit different types of organizations and their needs. For smaller organizations like New Castle, ease of management is essential.

"Other companies just tout firewall appliances. Cisco isn't like other security companies that are *primarily hardware* or *primarily software*. Cisco is both. That was really important to us, because we knew we needed control on endpoints, in the cloud, and on-prem at our properties.

**Alan Zaccario**
VP, IT and Cybersecurity, New Castle Hotels and Resorts

"I've managed firewalls from quite a few vendors. And I'm comfortable with command line, but I really like the new GUI and ease of management for Cisco firewalls," Zaccario said. "For instance, we run lots of VLANS to segment our network, and setting that up has been very straight-forward. The next-gen IPS has been an important part of our defense too. On our properties with global hotel brands, the brands have their own infrastructure and handle all the PCI-related functions. But we have our own employee PII [personally identifiable information] and protecting that PII is really important. And, obviously, we have PCI requirements to manage on our independent properties. When an auditor looks at us, they see we're doing what we're required to do. And also, the Firepower IPS in our firewalls not only protects our production network, it gives us lead-time when we can't immediately patch systems because we're putting out fires elsewhere."

"Firewall performance is important too–I have good visibility into the load on each firewall, and we've not had any issues with threat inspection compromising our network performance. People often forget that a key part of security is availability. If the network goes down, that means we're losing revenue at a property. We can't have that. We've had excellent uptime with Cisco firewalls, and they've enabled our threat protection and regulatory compliance without impacting our business operations."

New Castle also chose Cisco because of Cisco's leading threat intelligence organization, Talos. "The reputation of the Cisco Talos organization mattered. The firewalls get daily threat intelligence updates from Talos, that's a big deal."

## Security that drives business outcomes

A strong security posture is essential for driving business. "Cisco security has helped enable secure remote work for our sales teams during the crisis," stated Don Urbahn, VP Revenue Management at New Castle. "As our teams have been extraordinarily dedicated and creative while working from home, we have been able to meet the needs of current travelers, including many first responders, healthcare workers, government employees, national guard and military members, and other essential employees, as well as those requiring 14-day quarantines."

Zaccario detailed the top three business results that New Castle has seen with Cisco: "First, Cisco Security rapidly enabled a secure transition to work-from-home for our workforce. Second, we've reduced the time that compromised systems are on our production network from days to, now, in most cases, just hours. That's huge. As well, Cisco's platform approach protects our investment. We get more from the tight integration of Cisco network and endpoint security together."

"Third, Cisco SmartNET support – very important – because if I have an issue, or just a question, I can go straight to Cisco."

"Cisco security has helped enable secure remote work for our sales teams during the crisis."

**Don Urbahn**
VP, Revenue Management, New Castle Hotels and Resorts

### The way forward

As New Castle continues its security journey, continuing to reduce staff time on day-to-day management remains important. When asked what he expected things to look like in a post-Covid-19 world, Zaccario said "I don't have a crystal ball. But there's obviously going to be cost control pressure on everyone. And a lot of the threat actors now have extra time to develop new exploits, so life's not going to get easier. When we come up for air, and Corona's in our rear-view mirror, I'll be taking a look at CDO [Cisco Defense Orchestrator]. If CDO could make my firewall administration that much easier, and manage Firepower, ASA, and Meraki together, I want to check that out."

"We've reduced the time that compromised systems are on our production network from days to, now, in most cases, just hours."

**Alan Zaccario**
VP, Information Technology and Security, New Castle Hotels and Resorts

## Learn more

Learn more about how Cisco firewalling can help you by visiting https://cisco.com/go/ngfw

## Security products

- Cisco Firepower 1000 Series firewalls
- Cisco Meraki MX firewalls
- Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco Umbrella

CISCO DESIGNED



2091601 05/20