Cisco Umbrella

CASE STUDY

How Yelp connects people with great local businesses securely.

"Cisco Umbrella gives us more confidence in our ability to proactively protect our customers and employees, and more efficiency in our incident response process."

Vivek Raman
Head of Security
Yelp

Organization snapshot

Company:
Yelp

Location:
San Francisco, CA

Employees:
4,350

Objective:
Enhance the customer experience by building automation into the security practice

Solution:
Cisco Umbrella
Cisco Umbrella Investigate

Impact:

- Decreased incident response time from days to minutes through automation, enabled by the Investigate API
- Reduction in network security incidents and infected endpoints
- Increased protection against malware, ransomware, and other threats on and off the network
- Enriched security event data and threat intelligence with Investigate

The objective

Secure data and trust of growing user base

Founded in 2004 with the mission to connect people with great local businesses, Yelp prioritizes effective user engagement so successfully that today, more than one billion unique visitors turn to Yelp every year for help finding their next favorite lunch spot or their area's highest-rated dentist—transforming the company's very name from a known brand to an essential verb in the process.

"As Yelp's customer base and the internal infrastructure to support it has expanded, protecting customers' and employees' personal, payment, and other sensitive data has become progressively more vital," says Vivek Raman, Head of Security at Yelp, "because trust is central to our customer relationships. To stay ahead of attacks, keep content trustworthy, secure our more than 4,000 employees who increasingly work out of the office and off of our network, and continue to ensure user confidence in reading reviews and transacting with local businesses, we needed to strengthen and automate our security practice."

The solution

Automated protection and integrated threat intelligence

"The entire business is built around the customer experience," says Raman. "We decided to explore automating incident response and detection processes because airtight, efficient security helps drive business and enhance the customer experience."

Cisco Umbrella's DNS-layer enforcement stood out. "People don't realize how effective protecting at that layer can be, since threats are automatically stopped before they ever reach the network or endpoints," he says. Umbrella can proactively block requests to malicious destinations before a connection is even established or a malicious file downloaded, which makes it a great first line of defense against malware and ransomware.

And while cloud-delivered Cisco Umbrella offered a close fit for Yelp's cloud-first infrastructure, Yelp saw that it could gain rich threat intelligence from Cisco Umbrella Investigate to better respond to critical incidents. "When a malware incident is detected, the Investigate API automatically gathers insight into reputations for different domains that an employee or suspected infected computer may have visited," Raman says. "We chose Umbrella and Investigate to slow down our threat traffic and speed up our response."

If an incident is detected within the network, Investigate automatically identifies domain reputation and provides the rich threat intelligence needed to contextualize the threat and determine the appropriate response. From there, security analysts can block the malicious domain with Umbrella or dive deeper into research and hunt for associated threats.

"People don't realize how effective protecting at the DNS layer can be, since threats are automatically stopped before they ever reach the network or endpoints."

Vivek Raman
Head of Security
Yelp

The results

Better security, response, and customer experience

"Almost immediately, the number of malware incidents across our network dropped; we went from seeing multiple incidents per day to a very small number per month," says Raman. "Before we used the Investigate API to build security integrations around our incident response process, it might have taken our incident responders many hours, or even days, to respond to an incident. Now we've automated much of that process, so we can get it down to a very quick and efficient few minutes."

"We've been able to evolve Yelp's security practice beyond firefighting by using Umbrella and Investigate; we're in a much better position now," says Raman. "We've reduced overall incidents, can respond quickly if we need to, and are able to protect the entire Yelp workforce even when they're working off the network. We have a new layer of security that proactively protects users and employees against malware, ransomware, and other threats. Ultimately, this gives us time for more innovative security work that will enrich customers' experience with—and deepen their trust in—Yelp."

"Before we used the Investigate API to build security integrations around our incident response process, it might have taken our incident responders many hours, or even days, to respond to an incident. Now we've automated much of that process, so we can get it down to a very quick and efficient few minutes."

Vivek Raman
Head of Security
Yelp