Camuto group defends intellectual property without compromising productivity.

Organization snapshot

Company: Camuto Group
Headquarters: Greenwich, CT.
Number of users protected: 500 employees

Challenge: Protect brand-defining intellectual property on devices used by a very mobile workforce.

Solution: Cisco Umbrella

Impact:
• Detects and blocks approximately 400 potential malware threats every day
• Rapidly provision off-network security for new mobile employees
• Sees 5% – 10% improvement in internet speed; >30% improvement over alternative web filtering solutions

“There’s only a few products I’ve used in my career that actually do what they say they’ll do and Umbrella is one of them.”

Tom Olejniczak
Network Engineering Manager
Camuto Group
The challenge

Creative business must balance ease of access with protection of design assets

The Camuto Group, a footwear and lifestyle brand company with stores throughout the United States and Europe, and manufacturing facilities in Brazil, Italy and China, thrives by virtue of its unique designs. Creativity is the company’s most powerful competitive weapon, but for its IT security professionals, it’s a double-edged sword: Camuto’s 500 employees, 100 of whom work remotely, and another 250 roaming laptops must be guarded against data theft; yet its creative and sales professionals need unfettered access to a wide range of edgy websites that many web filtering solutions block incorrectly.

“Protecting Camuto Group’s products through security is one of our primary goals,” says Tom Olejniczak, Camuto Group’s network engineering manager. “Our products and designs are what drive the company; protecting these assets are a key to successfully supporting the business.”

In previous assignments, Olejniczak found that the traditional approach to securing the Web experience—proxy servers—imposed obstacles that had to be resolved manually. “Many non-malevolent websites are improperly encrypted or rely on outdated content controls such as ActiveX,” he says. “Every time someone needed to get to a problematic website, they needed hands-on help from IT.”

At Camuto, with its extensive mobile workforce, that kind of manual intervention was simply impossible. As malware rose and social media increasingly cut into productivity, Camuto Group required a network security solution that protected on and off-network devices without adding latency or hindering work activity.
The solution

Cisco Umbrella proves most effective first line of defense

Olejniczak says he “followed OpenDNS from the get-go,” even before Umbrella was an option and before OpenDNS was acquired by Cisco. As part of his research into the right solution for Camuto, IT put two alternatives to the test: Zscaler and Websense.

In the month that Olejniczak dropped Umbrella to pilot Zscaler, “malware rose by thirty percent. We were fighting up to three infections every day, spending a minimum of one to three hours each doing cleanup—more if we had to do a rebuild.” Olejniczak found that the proxy-based internet filters he’d used in the past didn’t work well with sites that required certificates. “It took a lot of manual intervention,” he says. “We would have to manage each desktop to get to the sites we wanted. It was damned near impossible to administrate every last URL that required a special client certificate.”

“The Websense product was just slow—it was like having extra software loaded on your PC,” Olejniczak says. “It increased latency by forty to fifty percent.” Ultimately, Camuto committed to Umbrella, and deployed the roaming client on laptops to extend Umbrella’s security and filtering capabilities. “We use Umbrella as the frontline of defense,” says Olejniczak, “coupling it with our antivirus protection and other proactive threat and network protections.”
The impact

Camuto Group blocks 400 malware hits each day while accelerating internet performance

“What I like about Umbrella is that it’s a cloud solution which replaces the web filtering work we used to do internally,” Olejniczak says. To protect onsite employees, Camuto deployed Umbrella virtual appliances which gives them the ability to identify internal networks or Active Directory users infected or targeted by attacks, without touching devices or re-authenticating users. Employees working off the corporate network are protected via Umbrella’s roaming client, installation of which “is as easy as adding someone to a group through Microsoft Active Directory.”

Camuto Group saw an immediate and measurable impact on security. “When I go to the Umbrella dashboard in the morning,” Olejniczak says, “I typically see as many as four hundred pieces of malware that have been redirected—that’s thousands a week.” Yet Umbrella’s power remains unobtrusive to users. “It actually improved the speed of the internet slightly,” says Olejniczak. “We see maybe a five to ten percent improvement, which makes it at least thirty percent better than other products.”

In a business that depends on creative people having access to cutting-edge fashion sites, the ability to manage white and black lists quickly is critical. “We can choose safe, HR-acceptable categories for content filtering fast,” Olejniczak says. When reports expose previously unknown sites that are inappropriate or risky—or when employees request access to legitimate sites that have been blocked—updating the lists is easy. “It’s extremely efficient: I can log in, make the changes, and log out in under three minutes.”

Olejniczak notes that Umbrella’s value increases over time. “The longer you use the product,” Olejniczak says, “the better off you are. There’s only a few products I’ve used in my career that actually do what they say they’ll do and Umbrella is one of them.”