# SKISTAR AB

CASE STUDY

# Scandinavian Resort Giant Delivers Secure Network Experience for Guests Online and on the Ski Slopes

Scandinavian ski resort operator SkiStar provides its guests with a unique Alpine experience that extends from its interactive website and mobile apps to the mountainside. Every aspect of SkiStar's business relies on its network. However, the company's legacy cybersecurity infrastructure allowed malware and other exploits to slip through, in some cases disrupting business operations. To combat this threat, SkiStar replaced its old Cisco® ASA firewall, IPS and web proxies with Palo Alto Networks® Next-Generation Security Platform.

The Palo Alto Networks platform provides SkiStar with more complete, effective network security with much less complexity than its previous solutions. It eliminates problems with ransomware that previously affected the business, and it successfully detects and blocks known and unknown cyberthreats daily, keeping all network activity by guests and employees safe and secure. Moreover, the Palo Alto Networks platform enables SkiStar to extend security to the endpoint devices of all employees, including remote users. And with its single, intuitive user interface, the Palo Alto Networks platform simplifies administration, saving IT hundreds of hours per year.

"We wanted end-to-end security on a single platform. This was important to keep our security infrastructure simple and easy to manage. Those were our goals, and the Palo Alto Networks platform met them perfectly."

**Peter Larsson** | CIO/IT chief | *SkiStar*

**INDUSTRY:**
Hospitality

**CHALLENGE:**
Improve network security to deliver a reliable, efficient web experience and safe, interactive mobile apps for guests.

**SOLUTION:**
Palo Alto Networks Next-Generation Security Platform to defend critical network services against cyberthreats, extending protection to the network perimeter, web and all endpoints in the business.

**SUBSCRIPTIONS:**
Threat Prevention, URL Filtering (PAN-DB), WildFire, Traps, GlobalProtect

**APPLIANCES:**
PA-3050 (2), PA-500 (1), PA-200 (1)

**RESULTS:**

- Automatically detects and stops cyberthreats from infiltrating or exfiltrating the network
- Blocks ransomware from disrupting employee productivity
- Saves hundreds of hours per year on security administration
- Brings more complete security with less complexity

## Customer Overview

SkiStar is a leading Scandinavian resort company that owns and operates six major Alpine destinations in Sweden, Norway and Austria. SkiStar's core business is Alpine skiing, with a focus on the guests' overall skiing experience. The business spans ski operations infrastructure, such as lifts, as well as an extensive online and app-based digital infrastructure to engage guests. The company also operates hotels and restaurants, along with retail properties associated with resort operations.

## Transforming Ski Holidays Into Interactive Digital Experiences

The Alpine skiing business has completely transformed in the wake of the digital age. It's no longer just a matter of strapping on some skis and riding to the top of a mountain for an exhilarating run. For guests at any of SkiStar's resorts, the Alpine experience is now an expansive digital experience that can start with a web inquiry from thousands of miles away and culminate in slope-side competitive skiing games on a mobile app.

A leading Alpine resort operator in Scandinavia and the Alps, Stockholm-based SkiStar is focused on creating a memorable mountain experience for every guest. From finding the ideal holiday package to buying digital lift tickets and sports gear, nearly every aspect of SkiStar's business relies on its network. SkiStar even uses network data to create popular mobile apps, including a gamification platform. This unique game offering has nearly 700,000 players who use the app to find friends on the slopes and compete to see who skis the most runs. Naturally, protecting the network from disruptive malware – or worse, breaches that compromise guest payment or personal information – is paramount.

Peter Larsson, SkiStar's CIO/IT chief, remarks, "Our entire business depends on the network. It handles payments on the e-commerce side as well as payments from on-site ticket sales, hotels and retail transactions. We also issue our ski tickets with an RFID tag that must be validated at all points of entry and at the lifts in our resorts. If our network is corrupted by a cyberattack, it would disrupt revenue streams and create a very bad impression on our guests."

"The Palo Alto Networks platform has given us a more capable security infrastructure with much less complexity. Most importantly, it ensures our guests can enjoy everything SkiStar brings them online and on the slopes with complete confidence in the security of our network."

**Peter Larsson** | CIO/IT chief | *SkiStar*

## More Advanced Cyberthreats Require More Advanced Security

As its network became ever more critical to the business, SkiStar recognized that the traditional Cisco ASA firewall at its network perimeter was no longer adequate. Further, SkiStar wanted to simplify its complex array of security solutions, which included a separate intrusion prevention system (IPS) and web proxies in addition to the Cisco firewall.

Despite all this hardware, sophisticated cyber exploits could still slip through and wreak havoc. In fact, the company suffered a ransomware attack that locked up several employee computers for a day until the IT team could clean things up. The business impact was minimal, but the attack provided a wake-up call that prompted SkiStar to modernize its network security infrastructure.

Larsson and his team considered a newer offering from Cisco, but the technology was not well-integrated, which made administration difficult. After a thorough evaluation, SkiStar decided to replace its legacy Cisco firewall with Palo Alto Networks Next-Generation Security Platform. "We wanted end-to-end security on a single platform," says Larsson. "This was important to keep our security infrastructure simple and easy to manage. Those were our goals, and the Palo Alto Networks platform met them perfectly."

With the Palo Alto Networks platform, which comprises the Next-Generation Firewall, Threat Intelligence Cloud and Advanced Endpoint Protection, SkiStar can safely enable applications, users and content, protecting against known and unknown cyberthreats across its multinational resorts.

To protect its main data center in Sweden, SkiStar deployed a pair of PA-3050 next-generation firewalls in high availability mode with subscriptions for Threat Prevention, URL Filtering, Traps™ advanced endpoint protection, GlobalProtect™ network security for endpoints and WildFire® cloud-based threat analysis service. This deployment safeguards all traffic for SkiStar's Scandinavian operations, including its flagship website, mobile apps and payment infrastructure. No traffic can traverse SkiStar's network without first passing through the security controls of the Palo Alto Networks platform.

Similarly, SkiStar deployed a PA-500 next-generation firewall for its Austrian resort, along with a PA-200 for testing and development. Larsson points out, "One of the strengths of the Palo Alto Networks platform is that we can test our software and apps using the same security policies on a small firewall as we do on the larger ones in our data centers. This allows us to validate that our applications will function properly and securely in production."

## GlobalProtect Helps Stop Cyberthreats at Every Point in the Network

With the in-line intrusion prevention capabilities of the Palo Alto Networks platform, SkiStar has advanced the security at its network perimeter well beyond its previous solution. Instead of controlling traffic based solely on port and protocol, as in the past, the Palo Alto Networks platform enables SkiStar to automatically inspect all traffic and stop known threats, encrypted or not, regardless of port and protocol. It also blocks any attempts by command-and-control exploits to exfiltrate data.

By adding URL Filtering, SkiStar shrinks the threat landscape further by preventing employees from accessing unknown sites. Yet the company still has flexibility to whitelist a URL if someone on the staff requests access. Larsson comments, "When we first enabled URL Filtering, we didn't know what to expect. But almost immediately, we recognized that it's one of the features we've benefited from most. With so many suspicious websites, there's no reason for anyone on our staff to visit a site that's not categorized in the Palo Alto Networks platform."

SkiStar extends the same protections to its mobile workforce through GlobalProtect. Now, as soon as a remote user connects to the internet, GlobalProtect automatically establishes a secure VPN tunnel on the device so all traffic flows through the Palo Alto Networks platform. "We wanted to be sure people working from home or on the road still had the full protection of the Palo Alto Networks platform as those on site," notes Larsson. "With GlobalProtect, we're not dependent on the user to establish the VPN, which gives us greater assurance that all their online activity will be secure behind the firewall."

> "Most people in IT today know that signature-based antivirus and antimalware solutions won't work on advanced threats like ransomware. Traps was the perfect choice to run alongside our other solution and gain the advanced endpoint protection we need. In fact, since installing Traps, we have had no more problems with ransomware."
>
> **Peter Larsson** | CIO/IT chief | *SkiStar*

### Advanced Endpoint Protection Puts an End to the Ransomware Problem

SkiStar also secures all its endpoint client devices with Traps. This includes approximately 800 PCs and laptops used by resort managers and staff, as well as hotel personnel and retailers. While SkiStar still runs traditional antivirus software, Traps complements those basic capabilities by preventing more sophisticated cyberthreats, such as ransomware and spear phishing, from getting through.

"Most people in IT today know that signature-based antivirus and antimalware solutions won't work on advanced threats like ransomware," Larsson asserts. "Traps was the perfect choice to run alongside our other solution and gain the advanced endpoint protection we need. In fact, since installing Traps, we have had no more problems with ransomware." He adds, "Traps was very easy to deploy, and took only a half day to implement for all our end users. It's also very easy to manage. Out of the box, the default policies covered our needs, so there's very little administration needed from my team."

With WildFire, SkiStar gets added protection from unknown threats and zero-day exploits for both its network and endpoints. "We think the WildFire service is great," says Larsson. "It provides us with extra detection capabilities that minimize the threat of zero-days hitting us. WildFire catches suspicious files every week that might otherwise cause trouble in our business. There's no doubt we're better protected because of WildFire."

### Stronger Security With Less Complexity

One of SkiStar's most important objectives was reducing complexity compared to its previous security infrastructure. By consolidating on the Palo Alto Networks platform, the company eliminated the need for web proxies and a separate IPS. Instead, it now has one platform and one set of policies to manage for the whole enterprise. "With the ease of managing the Palo Alto Networks platform through a single user interface, we save hundreds of hours of administration time each year compared to our previous infrastructure," reports Larsson.

He concludes, "The Palo Alto Networks platform has given us a more capable security infrastructure with much less complexity. Most importantly, it ensures our guests can enjoy everything SkiStar brings them online and on the slopes with complete confidence in the security of our network."