

Niki Golf Acts on Data for a Perfect Shot at Cybersecurity

Key Challenges

With a non-dedicated security team struggling to manage endpoint risk across distributed environments, the company needed to improve its incident response time and efficiency.

Key Results

By automating security management on a centralized platform, Niki Golf turns data into real-time endpoint visibility, enhancing cyber safety for its customers and responding to incidents faster.

NIKI GOLF

Industry: Retail

Solutions: Security, IT Operations

Niki Golf is an expert at cultivating calm — both on the green and online.

With a booming e-commerce shop and more than 50 brick-and-mortar stores sprinkled throughout Japan, the golf retailer places equal emphasis on enhancing the golfing experience with best-of-breed products while boosting cybersecurity to protect customers' data and ensure peace of mind.

In the past when Niki Golf experienced a problem, the company's IT team relied on tedious manual processes to extract details from disjointed endpoint protection tools before it could formulate an incident response. "We realized that security information and event management (SIEM) seemed to be a better approach for managing security in a more cost-effective way," says Shigeru Sakai from the Information Systems Division of Niki Golf.

After evaluating several options, Niki Golf believed that the combination of the Splunk Data-to-Everything™ Platform and Sysmon, Microsoft's free system monitoring tool, was a perfect replacement for any endpoint detection and response (EDR) tool. The company was eager to start a new chapter of automated security management with Splunk.

Teeing Up Shorter Investigation Times

On the Splunk platform, Niki Golf can now visualize endpoint status centrally and access server resource status in real time — ultimately helping the company to maintain customer trust and loyalty. "Prior to this, when we got an alert from the sandboxing software, we needed to access the consoles of different products one by one for troubleshooting," says Sakai, who is excited to see that everything is now automated, from anomaly detection and root cause analysis to issue resolution. Gone are the days when the IT team had to visit every endpoint for a health check. "It took two staff two hours to complete an initial incident investigation before, but now, I get it done all by myself in 30 minutes!" Sakai adds. This amounts to 75% faster incident response — and 50% manpower savings.

Data-Driven Outcomes

75%
faster incident management

50%
higher manpower efficiency

Increased
productivity for new revenue opportunities

The Splunk platform also works well with the Sysmon tool deployed across 300 endpoint PCs and servers. With more comprehensive and efficient security analysis, Niki Golf better protects its data and minimizes downtime so operations can keep running smoothly.

A Small Team Tackling Big Problems

The Splunk platform's extraordinary usability is a boon for Niki Golf. "Although we are in charge of security, this is only one of our many responsibilities," Sakai emphasizes. "We need an endpoint security system that operates reliably with minimum attention."

What makes the Data-to-Everything Platform the best fit? Simply speaking, it doesn't require Niki Golf to invest more resources or train team members in any new skills. Even a small team can operate the platform easily, boosting productivity with stress-free operation.

"Whether tech savvy or not, anyone in the company can use the system to a certain extent because of the user-friendly interface offered by Splunk," says Sakai. "It is far better than our old EDR model which required advanced security knowledge to run." Sakai also appreciates the fact that Splunk charges based on log volume, which allowed Niki Golf to "start small" at the beginning.

Scaling for a Sustainable Future

Equally impressive is the extensive collection of highly scalable apps and add-ons Splunk offers, many of which streamline data collection for better business insights. "We're considering switching to another portal, and there's already a Splunk app ready for use in the new environment," says Sakai.

Moving forward, the team is looking to raise the bar on data protection and security by automating additional processes. "We also plan to automate our security management tasks with Splunk Phantom so that we can respond to incidents even more efficiently," says Sakai.

Most encouragingly, Sakai has developed a strategy to boost revenue by deriving maximum benefits from the Splunk platform. "If this happens, the IT team will be actively contributing to the company's bottom line in addition to security management," he says. "Other plans include analyzing customer information and sales logs on the Splunk platform to turn data into actionable business insights, while separating the customer platforms for the online and offline stores."

All these are attributed to Splunk's full-stack monitoring and analytics capabilities which allow Niki Golf to visualize and correlate data in real time, bring data to every decision and action, and help the company identify and seize new opportunities.



The fact that you can use it easily without having to be an expert made Splunk a perfect solution that's second to none."

Shigeru Sakai, Information Systems
Division, Niki Golf

Download [Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com