CompTIA®

SKOUT
CYBERSECURITY

How to Prepare Partners to Move Quickly, Responsibly:
Creating New Packages to Protect Customers' New Remote Workforces

In this edition, learn how a cybersecurity vendor packaged its solutions
to help solution providers, MSPs, and their customers pivot to protect
remote workforces from the latest threats amid the COVID-19 pandemic.

OVERVIEW
When COVID-19 started to spread globally, SKOUT Cybersecurity recognized quickly that many MSPs and
their end users were ill-prepared to transition their businesses to a largely remote workforce, let alone in a
hastened manner. So, the Melville, N.Y.-based company jumped into motion, creating a special bundle and
corresponding marketing strategy that helped channel partners ensure that their small-business customers
were adequately protected against the latest threats.

"Our first thought, top of mind, was to protect our co-workers, their families and support our partners,"
said Jeff Benedetti, vice president of sales and marketing at SKOUT. "We built our entire internal stack to
be cloud-based and foster secure remote working environments. We were ready for this."

CHALLENGE
Like many companies, SKOUT Cybersecurity had to quickly transition its business once states started
mandating stay-at-home measures for non-essential businesses due to the COVID-19 pandemic. Employees
packed up their computers, monitors, phones and headed home to work—a relatively smooth transition
because SKOUT hosted much of its IT infrastructure in the cloud. But many of its managed service provider
partners and their customers were not in the same boat.

"What we heard from partners right off the bat was that they needed help. VPN connections were critical
and they're reading the news from the threat landscape," said Jimmy Hatzell, director of marketing at

CompTIA®

SKOUT. "There are multiple ways in which home environments can be breached and we had a lot of partners trying to figure out the best approach to deal with it. We knew we had to help."

SKOUT Cybersecurity responded by repackaging solutions for MSPs setting up new remote employees and providing training and marketing support to ensure those MSPs had everything they needed to help customers through the process.

"Businesses of all sizes struggled to make the transition to a remote world, creating a huge spike in demand for remote access, VPN, security, and remote office applications," Hatzell said. "With that, came an equally important need to secure these new access points—especially as reports of cybercriminals targeting new work-from-home users accelerated. Our solution could do that, but a lot of MSPs weren't as experienced setting up home users as they were office users."

SOLUTION
SKOUT created Remote Worker Security Guidelines for MSPs and their customers, a checklist for IT resources and employees to follow to ensure that they've created a secure workspace away from the office—and steps to follow to ensure it remains that way.

Next, SKOUT assembled a package that address two pressing threats to new remote workers: business email compromise and ransomware. SKOUT designed a package that included SKOUT Email Protection, Endpoint Protection, Office 365 Log Monitoring, along with technical and go-to-market support. The solution was designed to help MSPs expedite corporate network access for newly remote workers. All the pieces were already available, but the package allowed MSPs to respond more quickly to customer requests, according to Benedetti.

"Our MSPs said they got a lot of value out of that. Because we're based in the cloud, we're able to be nimble and react to our partners' needs. From integration to tools to pull logs, we were able to accommodate requests pretty quickly," he said. "It was all hands on deck to get that done."

While the bundle was being finalized, SKOUT's marketing team was creating the collateral to get the word out, both from the company to MSPs, and for MSPs to send to their customers. "Our partner portal played a big part of that. It allowed us to outreach to partners in an organized, cohesive manner to let them know what we were doing, and also for them to provide feedback and ask questions of us," Hatzell said.

OUTCOME
All told, SKOUT estimates it has spent about 500 hours between technical, marketing, and sales teams to develop new messaging for MSPs to support new remote workers. Feedback from the market has been positive and led to an increase in monthly new partners who are, in turn, able to expand their own services through SKOUT. But the benefits will also be long term, Benedetti believes, because of tighter relationships and increased good will with MSPs.

> "We had a lot of partners trying to figure out the best approach to deal with it. We knew we had to help."

> "These are demanding times for MSPs. Our mission is to be part of their solution, not part of their problem."

"Honestly, nobody was thinking about sales at the time. It was all about supporting people that were going through a lot of turmoil. Businesses are experiencing unprecedented change at a very fast rate. It's critical to support partners and for partners to support customers."

MSP teams saw a flurry of demand after stay-at-home orders were instituted and often worked days of 12+ hours to help small businesses. With so much of the economy thrown into chaos, the ability to provide online access, securely, helped many MSPs gain more loyal customers, Hatzell said.

"These are demanding times for MSPs. Our mission is to be part of their solution, not part of their problem," he said.

SUMMARY

COVID-19 has been the most disruptive force to impact business in generations. It's caused businesses to adjust on the fly and make major changes in order to survive. Companies adapting to a "new normal" (even if that "normal" changes every day) stand a better chance of success, and those adapting in a secure infrastructure even more so, according to Benedetti. It's critical for MSPs and their customers to embrace cloud-based security technologies to withstand all these changes.
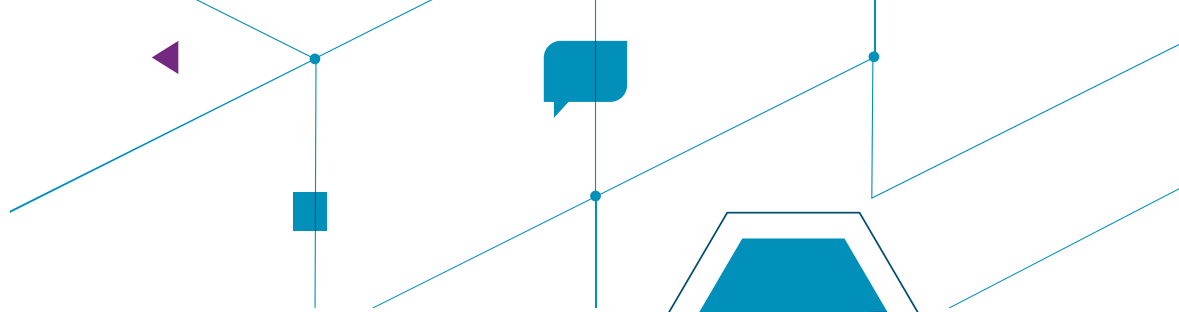
"Security now is more critical than ever," said Benedetti. "As the economics of the world change, and as people and businesses and governments become more vulnerable, it's critical that security stays top of mind. Our infrastructure allowed us to pivot quickly and provide our partners with the right solution, the right messaging, and the right support to make them more successful."

WHAT'S NEXT

About 85% of CompTIA members surveyed in March had transitioned at least a portion of their staff to work remotely and a June survey of CompTIA members revealed that 65% of respondents plan to let more employees stay working remotely, even after the pandemic recedes. So, while there was an initial rush to get customers up and running remotely, long-term support for those customers will also be necessary.

SKOUT worked diligently to release its work-from-home bundle in early April, and has been monitoring the flow of demand since. The need for remote security solutions has remained steady because many MSPs are choosing to continue working from home even as COVID-19 pandemic restrictions are being lifted, according to Hatzell. The convenience of a home office in conjunction with SKOUT's services has created sustainable work environments for employees.

"We see work from home as a relatively new normal moving forward," says Benedetti, "And SKOUT is proud to provide the solutions to make that safely possible for our partners."

NOW IT'S *YOUR TURN*

Conducting business changed dramatically anywhere and everywhere during the COVID-19 pandemic. SKOUT Cybersecurity made sure its MSP partners were prepared to help customers respond accordingly, creating a packaged security and monitoring solution for customers with new remote workers. Here's their advice for what to do in a similar situation requiring fast, decisive action:

▼

Prior to any time-sensitive response, evaluate your existing tools and solutions to determine if you're capable of meeting quickly changing customer needs in real-time.

▼

Treat the situation as if you're fixing a critical business problem, not as an upsell opportunity for your specific product/solution.

▼

Create content such as a checklist or guidelines that partners and customers can use to identify problems/gaps and remedy them on their own.

▼

Coordinate your efforts across all internal teams to ensure that the solution or service is complemented by the messaging and support necessary to be successful.