voices

CrowdStrike Customer Case Study

Virgin hyperloop

Virgin Hyperloop Plans to Revolutionize Mass Transit While Safeguarding Data

Virgin Hyperloop is a private company founded in 2014 to develop a new mode of mass transportation that moves freight and people quickly, safely, on demand, and direct from origin to destination — with no direct carbon emissions. The company has about 300 employees and offices in Los Angeles, Las Vegas and Dubai.

Because it's developing cutting-edge technology, Virgin Hyperloop faces security challenges as both a startup and a transportation company. Lean, investor-fed budgets preclude hiring a massive IT department; previously unheard-of intellectual property attracts the unwanted attention of hackers; and the company moves so fast it can be tough for security to keep pace.

Virgin Hyperloop could change the world, offering infrastructure that's faster, more scalable, less expensive and more environmentally friendly than high-speed rail. VP of IT Dawn Armstrong says Virgin Hyperloop's mission is to "reinvent public transportation as we know it. We're developing a mode of transportation that takes people in pods, and they're in a tube," she explains. "That tube can be above the ground or in a tunnel. It's an autonomous driving vehicle propelled through a vacuum."

INDUSTRY

Transportation

HEADQUARTERS

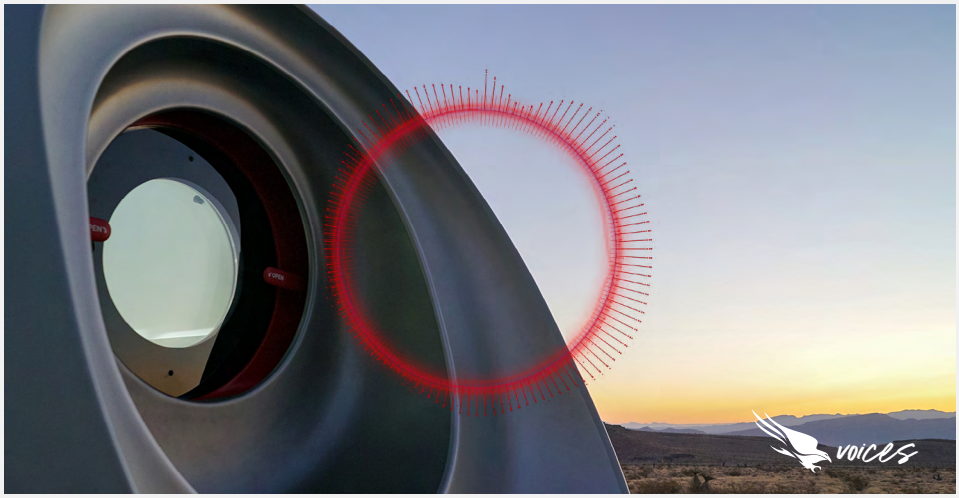
Los Angeles, CA

CHALLENGES

- Protection of revolutionary IP as a small IT team
- Fast-moving startup with a highly mobile staff
- Limited budget and the high demands of a startup

SOLUTION

Falcon Complete™ managed endpoint security



voices

CrowdStrike Customer Case Study

Virgin Hyperloop is powered by electricity, making it environmentally friendly. But the potential "change the world" benefit, Armstrong says, is speed.

"Say you could travel between Los Angeles and Las Vegas in 30 minutes," she offers as an example. "You could work in LA yet live in Las Vegas, where housing is more affordable. Consider the economic boom that would be for Las Vegas — and then consider applying that transportation model nation- and worldwide."

World-Changing Intellectual Property Attracts Worldwide Attention

Being a small company with limited resources and a big profile — and with some of the most talked-about intellectual property (IP) on the planet — puts a lot of stress on a security team.

"At all of the companies I worked for before, I never had to worry about state actors," Armstrong says. "Though we operate with a small company's resources, we have a big company's vision. That makes for a large profile for other people to be interested in." Securing Virgin Hyperloop's IP is therefore crucial, she says.

Virgin Hyperloop Wanted to Cut Costs, Streamline Security

Armstrong says when she started at Virgin Hyperloop, she was faced with a "mish-mosh of security products," including two endpoint protection products, a variety of other applications and a company under retainer to remediate malware — all of which cost "a tremendous amount of money."

Wanting to save money and streamline the company's cybersecurity, Armstrong consulted with several security companies. The CrowdStrike® Falcon Complete solution came out on top, she says.

"CrowdStrike had a Falcon Complete package that enabled me to get rid of all of the extraneous applications that were installed on our users' computers," she explains. "I canceled the professional services retainer and went with Falcon Complete. That gave us everything we needed."

Virgin Hyperloop Protects Data With CrowdStrike Technology and Services

As an investor-supported startup developing next-generation technology, Virgin Hyperloop is relatively small — staffing sits at about 300 — and without the typical budget of a large enterprise.

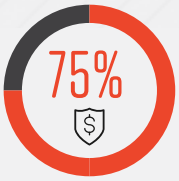
"As a result, we're not able to have a full-time security analyst on staff. That's one of the reasons why I went with CrowdStrike," she says, referring to its Falcon OverWatch™ threat hunting and Falcon Complete managed detection and response capabilities. This allows the CrowdStrike staff to augment the Virgin Hyperloop team.

One benefit of this tight partnership is that it allows Armstrong to free up Virgin Hyperloop's service desk to handle employee tickets, saving time and cost in the process.

"We remediate no malware whatsoever, and not only am I saving money, which makes me look like a hero to the finance department, but our malware instances have just plummeted. The CrowdStrike platform lets us forget about malware and move onto the stuff we need to do."

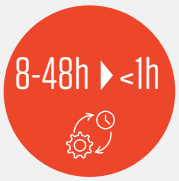
Dawn Armstrong
VP of IT
Virgin Hyperloop

RESULTS



Reduction in security costs

Malware instances plummeted from a daily occurrence to rare



Remediation went from 8-48 hours to under an hour

voices

CrowdStrike Customer Case Study

"With the company we used for malware remediation, it would take eight to 12 hours for a service desk person to remove the offending laptop from production and give the person a loaner or let them remediate," she says. "Now, we get an email from Falcon Complete that says, 'Hey, we found this. We remediated it or quarantined it and everything's fine.' That gives me total comfort and allows my team to focus on other tasks."

"We remediate no malware whatsoever," she underscores. "And not only am I saving money, which makes me look like a hero to the finance department, but our malware instances have just plummeted. The CrowdStrike platform lets us forget about malware and move onto the stuff we need to do."

Close Relationship With CrowdStrike Adds Value

Among the most important things to Armstrong are her security partner relationships. "I take them very, very seriously," she says. "Our security partners must have integrity, and the same passion for their products as everybody at Virgin Hyperloop has for our product. We also move very, very fast, and I need my vendors to do the same thing. CrowdStrike gives me that. And they give me that comfort that I know I'm secure."

Armstrong points to one example that highlights the speed at which CrowdStrike responds to real-time threats.

"Any time there's a zero-day exploit that's really, really, really critical, CrowdStrike will add a tab to its Falcon portal for just a certain period of time that tells you all the computers and servers you need to go remediate right now, because they have that vulnerability. Once the vulnerability is remediated, the tab goes away, and we can move onto something else. CrowdStrike constantly adds features, improves its dashboard and lets us know when things need to be addressed. That's why we're with CrowdStrike."

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed endpoint security
- Falcon Prevent™ next-gen AV
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed hunting
- Falcon Discover™ IT hygiene
- Falcon Device Control™ USB security

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches