



CASE STUDY



# SKYLINE Enterprises

## Challenge

Skyline Enterprises is rapidly growing. Currently the core team is composed of 300 employees plus numerous outsourced contractors. Deepak Lathker, VP and head of IT, Security and Apps, leads an internal team of 12, plus additional external resources around the world. With this small team, Lathker is determined to protect Skyline's intellectual property and any client data in the most robust and complete way possible.

"Ultimately our goal is to know how strong we are, how protected we are from any sort of attack coming our way," says Lathker. "New attack vectors are constantly emerging. We strive to be more vigilant and get ahead of the known unknowns, and be completely prepared from a defense perspective."

Lathker and his team approach every end user computer as a data platform. He observed that with work-from-home, especially during and after the 2020 COVID pandemic, there are no longer any boundaries and the network must be protected from every device that touches it. For that reason, Lathker has developed an aggressive end-to-end security strategy.

## The Client

**Skyline Enterprises** is a commercial interior construction company in the San Francisco Bay Area and beyond. The company is rapidly expanding with investments in commercial real estate and construction services firms, with the vision that transparency, technology and expertise can lead to better employees, expectations, experiences and ultimately, a better end product. Skyline customers span multiple industries, including high tech, healthcare, legal services and more.

**"New attack vectors are constantly emerging. We strive to be more vigilant and get ahead of the known unknowns, and be completely prepared from a defense perspective."**



An additional challenge lies in the simple fact that Skyline was founded over 25 years ago in 1996. While most of the company's enterprise apps are in the cloud, there are some legacy systems that are standard to the long-established construction industry and are not cloud-ready. These systems are kept on-premise and need additional security consideration.

## Solution

Lathker, a long-time denizen of the Silicon Valley, was introduced to Airgap at the Black Hat computer security conference and was impressed with the team and their new developments in cyber security. Airgap's zero-trust approach to security meshed with Lathker's corporate strategy for Skyline and he invited the Airgap team to participate in a proof-of-concept. Airgap seamlessly integrates into Skyline's SSO/MFA platform and augments the TLS encryption used to secure the company's legacy RDP applications.

## Outcome

"There is no such thing as a silver bullet with it comes to cyber defense," says Lathker, "but there is such a thing as a silver lining – we look to our partners like Airgap to work in concert with all of our security tools to create this silver lining of defense, protecting our IP and other sensitive data, end-to-end."

In the future Lathker is considering leveraging Airgap's Ransomware Kill Switch™ with a privileged access model, pointing out, "Security is a journey and there's always a gap to be found. I look forward to working with Airgap further to fill more of those gaps."

"There is no such thing as a silver bullet with it comes to cyber defense, but there is such a thing as a silver lining – we look to our partners like Airgap to work in concert with all of our security tools to create this silver lining of defense, protecting our IP and other sensitive data, end-to-end."

## About Airgap Networks

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.