

CASE STUDY

EQT Corporation

The largest producer of natural gas in the United States improved its cybersecurity defenses by adding Airlock Digital application control and allowlisting to its security stack.



About EQT Corporation

EQT Corporation is a premier, vertically integrated American natural gas company with production and midstream operations focused in the Appalachian Basin.

Learn more about EQT by visiting www.eqt.com.



Challenge

The cybersecurity team needed to eliminate risks to the business and its operations from unknown and **Living off the Land (LOTL) attacks**, where existing detection and response capability was ineffective.



Approach

Airlock Digital application control and allowlisting provided flexible, cost effective, and easy to manage **Deny by Default security** capabilities, which enabled EQT to bring 1,500 endpoints under management without hiring additional team members.



Result

EQT is able to keep its servers, people, and reputation safe from cyberthreats. The cybersecurity team spends just 10–15% of their time managing Airlock Digital, freeing up resource to manage other cybersecurity applications.

Benefits to EQT

With Airlock Digital application control and allowlisting, EQT has:

- Reduced risk on machines where local administration rights are necessary while minimizing friction by allowing users to self-service when installing new applications
- Implemented allowlisting with minimal operational impact
- Managed the solution effectively with < 0.15 FTE after implementation
- Eliminated the risk of a supply chain attack in <15 minutes

“Airlock’s Digital’s brilliance is through its simplicity. The product demonstration consisted of one salesperson who knew the product front and back.”

EQT Cybersecurity Manager

About Airlock Digital

Founded in 2013 in Adelaide, South Australia, pure play allowlisting and application control solution provider Airlock Digital helps organizations keep ransomware and other malware out of their environments.



The Customer

EQT Corporation is the largest natural gas producer in the United States with operations in Pennsylvania, West Virginia and Ohio. The company produces two trillion cubic feet of natural gas a year and is committed to becoming the operator of choice for all stakeholders. EQT has close to 1,000 well pads, and the capability to drill vertically up to 3,000 meters and laterally up to 5,000 meters to access natural gas deposits.

A three-person team headed by the Cybersecurity Manager manages cybersecurity across all on-premises, remote, and cloud computing resources used by EQT Corporation and its 800 employees.

The Challenge

Today's cyberthreat landscape presents ongoing challenges to the EQT cybersecurity team. When the Cybersecurity Manager joined the business in 2019, he and his team discussed application allowlisting as a way of reducing the risk posed by malware to its systems and data.

The Approach

After initially dismissing allowlisting as "pie in the sky," EQT in 2021 evaluated products from a range of vendors, including Airlock Digital.

"Airlock Digital's brilliance is through its simplicity. The product demonstration consisted of one salesperson who knew the product front and back," said EQT Cybersecurity Manager.

Other important factors included the fact that Airlock Digital was a pure play allowlisting solution, rather than a product that bundled allowlisting with other functionality extraneous to EQT Corporation's needs. In addition, the solution was flexible enough to enable a staged deployment so EQT Corporation's cybersecurity team could undertake an orderly implementation and change management process.

EQT moved to a 45-day proof of concept "which demonstrated that Airlock Digital allowlisting does exactly what it is supposed to do!" said EQT Director of Infrastructure.

The Result

Ease of management proved to be a key benefit of Airlock Digital. The EQT cybersecurity team found they were able to spend just 10–15% of their time managing the solution, freeing up resource to manage the 20 plus cybersecurity applications deployed at the natural gas producer.

The built-in data analysis and wizard-driven workflows enabled EQT to identify patterns and make data-driven decisions quickly and easily.

EQT's Cybersecurity Manager said, "we should not be making changes on production servers without change control, and Airlock Digital helps keep our servers, our people and our reputation safe."

The EQT cybersecurity team found the product added greatly to their existing security product set. "Airlock Digital is an excellent complement to our endpoint detection and response solution," said EQT's Cybersecurity Manager.

Airlock Digital gives the organization an easy way to audit and block Living off the Land binaries and scripts (LOLBAS).

"We evaluated another tool from a globally recognized vendor for this purpose, but its auditing functionality and user-friendliness could not match that provided by Airlock Digital," said EQT's Cybersecurity Manager. "At the moment, 50% of Airlock Digital's value is in allowlisting and the other 50% is in preventing LOLBAS."

The solution's blocklisting feature has played a critical role in keeping the EQT environment secure. "When one of our vendors was compromised, we quickly audited our own systems for the wscript.exe LOLBin that was used to infect the vendor. We then confirmed limited usage in our environment and implemented additional blocking rules within 15 minutes," said EQT's Cybersecurity Manager.

Learn more about how Airlock Digital provides secure application control for energy and utilities companies.