

*How did the recent Colonial Pipeline cyber attack happen? What could have been done to prevent it?  
A closer look at the most recent—and potentially most devastating—cyberattack.*



It happened again. Yet unlike the recent SolarWinds (<https://blog.ariacybersecurity.com/blog/what-does-the-solarwinds-orion-attack-say-about-the-state-of-cybersecurity>), Microsoft Exchange (<https://blog.ariacybersecurity.com/blog/what-we-can-learn-from-the-2021-microsoft-data-breach>) cyberattacks and even many of the ten worst attacks in 2020 (<https://blog.ariacybersecurity.com/blog/the-top-10-most-significant-data-breaches-of-2020>), the ransomware attack against Colonial Pipeline led to immediate, painful, and costly effects for millions of American consumers.

## **What happened to Colonial Pipeline?**

On Friday, May 7, Colonial Pipeline reported that a cyberattack forced it to proactively close down operations and freeze IT systems after becoming the victim of a cyberattack, specifically a ransomware attack from a group identified as DarkSide.

It's a significant event and one that could affect gas availability and prices on the entire east coast of the U.S., if not larger parts of America. The Colonial Pipeline is the largest pipeline system for refined oil products in the U.S. and consists of two massive pipelines that are 5,500 miles long. Colonial Pipeline is capable of transporting three million barrels of fuel per day between Texas and New York and supplies nearly half of the East Coast's fuel.

The shutdown caused millions of people to scramble to quickly fill their tanks. In some places gas prices experienced a significant increase, in many locations well over the \$3 threshold, and many stations were running low, or ran completely out of gas. As we've seen before, this type of incident could be the first domino to fall and could potentially impact consumer confidence and even the entire U.S. economy.

There are few concrete details on how the cyberattack took place, and it is likely that this will not change until Colonial Pipeline and its investigative partners and experts have concluded their analysis.

However, what did occur was a ransomware outbreak (<https://blog.ariacybersecurity.com/blog/just-what-is-a-ransomware-attack-and-can-you-prevent-one>), linked to the DarkSide group, that struck Colonial Pipeline's networks. Apparently DarkSide operators targeted the business side rather than operational systems, which implies the intent was focused on securing a ransom, and not to send the pipeline crashing down.

The initial attack vector (<https://blog.ariacybersecurity.com/blog/what-is-a-threat-attack-surface-blog>) isn't known, but it may have been an old, unpatched security vulnerability in a system; a phishing email that successfully fooled an employee; the use of access credentials purchased or obtained elsewhere that were leaked previously, or any other number of tactics employed by cybercriminals to infiltrate a company's network. We've written about these types of attacks in the past (<https://blog.ariacybersecurity.com/blog/9-types-of-cyber-attacks-organizations-must-prepare-for>), especially those targeting industrial companies and utilities ([https://www.ariacybersecurity.com/wp-content/uploads/2019/12/ARIACS-IIoT-Industrial-use\\_case.pdf](https://www.ariacybersecurity.com/wp-content/uploads/2019/12/ARIACS-IIoT-Industrial-use_case.pdf)).



But new details are emerging now, such as the fact that the Colonial Pipeline CEO Joseph Blount revealed he authorized a \$4.4M ransom payment. Despite his own personal misgivings, he realized there were larger issues at play, including national implications. “It was the right thing to do for the country,” he said, “I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this.”

## Traditional tools fall short

Utilities and industrial companies such as Colonial Pipeline tend to operate infrastructure, systems, and environments where harmful network-borne threats, such as ransomware, DDoS, instructions, and so many other types of cyberattacks (<https://blog.ariacybersecurity.com/blog/9-types-of-cyber-attacks-organizations-must-prepare-for>) are typically missed by existing cyber security solutions.

For example, the traditional current approach to threat detection and response (<https://www.ariacybersecurity.com/cybersecurity-products/threat-detection-response/>) is a suite of individual security tools that organizations need to manually monitor, correlate, interpret data, and take action on it. Often the heart of these systems are SIEMs (<https://blog.ariacybersecurity.com/blog/siem-security-solutions-blog>) and/or IDS/IPS tools (<https://blog.ariacybersecurity.com/blog/understanding-the-strengths-and-limitations-of-your-intrusion-detection-system>), and unfortunately they just aren't effective at finding zero-day attacks or APTs (<https://blog.ariacybersecurity.com/blog/top-security-trends-for-2021-and-what-they-mean-for-you>) like this one.

They use a log-based approach that requires a sizable amount of analyst time to create query strings and develop other code in the hopes of increasing threat coverage and finding cyber threats (<https://blog.ariacybersecurity.com/blog/enterprise-wide-threat-detection-and-response-becomes-easy>), as well as make sense of the thousands of intrusion alerts that are generated daily. Because this approach is based on human knowledge, the security tools can only look for what is known— not new threat behaviors found in zero-day attacks and other types of attacks against utilities and pipeline operators (<https://blog.ariacybersecurity.com/blog/five-examples-of-iiot-iiot-security-threats-blog>) such as Colonial Pipeline.

As we've discussed before oil and gas, utilities, and other industrial companies are highly attractive targets (<https://www.ariacybersecurity.com/cybersecurity-products/industry-use-cases/cybersecurity-for-industrial-and-utility-networks/>), both because of the vital service they provide, but also because their cybersecurity is usually a step behind. For example, many industrial companies still rely on infrastructure, systems, and proprietary applications that can't be patched or upgraded or work with modern security tools. Additionally, this industry relies on a growing number of IIoT and IoT devices (<https://blog.ariacybersecurity.com/blog/industrial-iiot-security-challenges-blog>), which are highly vulnerable and expand the company's overall threat surface.

**How could this attack have been prevented?**



At ARIA Cybersecurity Solutions, we have always recommended a new focus in the industrial sector (<https://www.ariacybersecurity.com/cybersecurity-products/industry-use-cases/cybersecurity-for-industrial-and-utility-networks/>), especially since these companies tend to rely on IoT and aging infrastructure that is hard to secure. There needs to be a cyber security solution that solves the tough problems and isn't focused on stemming the wound.

Specifically oil and gas and utility companies need to address the following challenges:

- Lack of visibility into the network to identify potential threats
- Over-burdened security analysts who must respond to too many alerts
- The need to take critical systems offline in order to stop an attack
- Relying on log-based approach that requires time-consuming and complex scripts, tuning, and management
- Security tools that can't evolve with cyberattacks

Our ARIA ADR solution (<https://www.ariacybersecurity.com/cybersecurity-products/aria-sds-advanced-detection-and-response/>) was purpose-built to overcome these challenges and more. It's a fully automated, AI-SOC that uses behavior-based ML threat models to detect, stop, and contain all types of threats as they move through the network. With ARIA ADR, organizations can stop 99% of the most harmful network-borne threats including ransomware, malware, DDoS, intrusions, brute force attacks, insider threats, compromised credentials, policy violations and data exfiltrations.

ARIA ADR automatically stops the hackers and attackers by detecting any abnormal communications from within the network's network and movements. It can stop those communications and lateral movements so attackers can't hide, and the attackers' obfuscation techniques don't work. Nothing gets lost in the noise.

How does it do this? ARIA ADR provides complete visibility into the network, generating enhanced analytics for every packet traversing (even laterally) the network. With this information, in addition to the 70+ threat models, it detects threats in real time and before harm is done.

The ARIA ADR solution is not only unique, but powerful as in a single platform, it has the capabilities of seven security tools, including SIEMs, UEBA's, NTAs, EDR systems, threat intel platforms, IDS/IPS tools, and SOARs.

No longer will organizations have to manage and correlate information from disparate tools. Unlike other threat detection solutions, it delivers the benefits of "a single pane of glass solution," with insightful dashboards and actionable information—think of it as a one monitor SOC. It can be operated remotely, from anywhere, and because it's fully automated, it does not rely upon or require a highly-trained analyst and operates around the clock for complete coverage.

We believe that with ARIA ADR, the Colonial Pipeline attack would never have happened, which would have saved many of us from the long-term effects related to expensive gas and lower supplies.

If you're interested in learning more about ARIA ADR, and how it can present a new approach to cybersecurity, please review our ARIA ADR Advantages solutions guide (<https://www.ariacybersecurity.com/wp-content/uploads/2020/03/ARIACS-ARIAADR-Advantages.pdf>)

today.

## About ARIA Cybersecurity Solutions

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

Tags: cyber attack (<https://blog.ariacybersecurity.com/blog/tag/cyber-attack>), cybersecurity (<https://blog.ariacybersecurity.com/blog/tag/cybersecurity>), ransomware (<https://blog.ariacybersecurity.com/blog/tag/ransomware>)

---

## Related Articles



(<https://blog.ariacybersecurity.com/blog/ransomware-attacks-what-you-need-to-know-aria>)

### Ransomware Attacks: What You Need to Know

(<https://blog.ariacybersecurity.com/blog/ransomware-attacks-what-you-need-to-know-aria>)

(9 min read)



Topics: Cyber Attack (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cyber-Attack>), Cybersecurity (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cybersecurity>), Ransomware (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Ransomware>)

(<https://blog.ariacybersecurity.com/blog/machine-learning-ai-in-cybersecurity-solutions>)

## **Top 5 Reasons Companies Are Denied Cybersecurity Insurance (<https://blog.ariacybersecurity.com/blog/machine-learning-ai-in-cybersecurity-solutions>)**

*(3 min read )*

---

Topics: Cyber Attack (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cyber-Attack>), Cybersecurity (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cybersecurity>), Ransomware (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Ransomware>)

(<https://blog.ariacybersecurity.com/blog/mitre-attck-framework-aria-adr-is-the-first-fully-automated-solution-built-around-the-industries-only-proven-framework-to-find-and-stop-todays-cyber-attacks>)

## **ARIA ADR Stops Cyber Attacks With the MITRE ATT&CK Framework (<https://blog.ariacybersecurity.com/blog/mitre-attck-framework-aria-adr-is-the-first-fully-automated-solution-built-around-the-industries-only-proven-framework-to-find-and-stop-todays-cyber-attacks>)**

*(2 min read )*

---

Topics: Cyber Attack (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cyber-Attack>), Cybersecurity (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Cybersecurity>), Ransomware (<https://Blog.Ariacybersecurity.Com/Blog/Tag/Ransomware>)



## CYBERSECURITY PRODUCTS ([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/](https://www.ariacybersecurity.com/cybersecurity-products/))

ALL CYBERSECURITY PRODUCTS

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/ALL-PRODUCTS/](https://www.ariacybersecurity.com/cybersecurity-products/all-products/))

ARIA SDS APPLICATIONS

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/ARIA-SDS-SECURITY-SERVICES/](https://www.ariacybersecurity.com/cybersecurity-products/aria-sds-security-services/))

ARIA SDS AIR

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/ARIA-AIR/](https://www.ariacybersecurity.com/cybersecurity-products/aria-air/))

ARIA SDS KMS

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/ARIA-KMS/](https://www.ariacybersecurity.com/cybersecurity-products/aria-kms/))

ARIA MICROHSM

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/ARIA-HSM/](https://www.ariacybersecurity.com/cybersecurity-products/aria-hsm/))

ARIA SECURITY APPLIANCES

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/SECURITY-APPLIANCES/](https://www.ariacybersecurity.com/cybersecurity-products/security-appliances/))

NVOY SERIES

NVOY PACKET BROKER

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/NVOY-PACKET-BROKER/](https://www.ariacybersecurity.com/cybersecurity-products/nvoy-packet-broker/))

NVOY PACKET RECORDER

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/NVOY-PACKET-RECORDER/](https://www.ariacybersecurity.com/cybersecurity-products/nvoy-packet-recorder/))

## SOLUTIONS

THREAT DETECTION AND RESPONSE

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/THREAT-DETECTION-RESPONSE/](https://www.ariacybersecurity.com/cybersecurity-products/threat-detection-response/))

DATA PROTECTION

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/DATA-PROTECTION/](https://www.ariacybersecurity.com/cybersecurity-products/data-protection/))

INDUSTRY COMPLIANCE

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/INDUSTRY-COMPLIANCE/](https://www.ariacybersecurity.com/cybersecurity-products/industry-compliance/))

PROTECTING COMMERCIAL IOT

([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-PRODUCTS/PROTECTING-COMMERCIAL-IOT/](https://www.ariacybersecurity.com/cybersecurity-products/protecting-commercial-iot/))

## MYRICOM SMARTNICS ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/](https://www.ariacybersecurity.com/network-adapters/))

SOFTWARE ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/SOFTWARE/](https://www.ariacybersecurity.com/network-adapters/software/))

MYRICOM DBL ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/SOFTWARE/DBL/](https://www.ariacybersecurity.com/network-adapters/software/dbl/))

MVA ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/MVA-SOFTWARE/](https://www.ariacybersecurity.com/network-adapters/mva-software/))

MYRICOM SNIFFER 10G ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/SOFTWARE/SNIFFER10G/](https://www.ariacybersecurity.com/network-adapters/software/sniffer10g/))

MYRICOM ARC

C-CLASS ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/C-CLASS/](https://www.ariacybersecurity.com/network-adapters/c-class/))

D-CLASS ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/D-CLASS/](https://www.ariacybersecurity.com/network-adapters/d-class/))

E-CLASS ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/E-CLASS/](https://www.ariacybersecurity.com/network-adapters/e-class/))

MYRICOM SIA SMARTNIC ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/MYRICOM-SIA/](https://www.ariacybersecurity.com/network-adapters/myricom-sia/))

RESELLERS & DISTRIBUTORS ([HTTPS://WWW.ARIACYBERSECURITY.COM/NETWORK-ADAPTERS/RESELLERS-DISTRIBUTORS/](https://www.ariacybersecurity.com/network-adapters/resellers-distributors/))



## MSSP AND OEM SOLUTIONS

MSSP SOLUTIONS ([HTTPS://WWW.ARIACYBERSECURITY.COM/MSSP-SOLUTIONS/](https://www.ariacybersecurity.com/mssp-solutions/))

OEM SOLUTIONS ([HTTPS://WWW.ARIACYBERSECURITY.COM/OEM-SOLUTIONS/](https://www.ariacybersecurity.com/oem-solutions/))

## ABOUT US ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/](https://www.ariacybersecurity.com/about-us/))

CAREERS ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/CAREERS/](https://www.ariacybersecurity.com/about-us/careers/))

AWARDS ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/INDUSTRY-AWARDS-AND-RECOGNITION/](https://www.ariacybersecurity.com/about-us/industry-awards-and-recognition/))

NEWS ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/NEWS/](https://www.ariacybersecurity.com/about-us/news/))

RESOURCES ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/RESOURCES/](https://www.ariacybersecurity.com/about-us/resources/))

## BLOG ([HTTPS://BLOG.ARIACYBERSECURITY.COM/BLOG/](https://blog.ariacybersecurity.com/blog/))

## SUPPORT ([HTTPS://WWW.ARIACYBERSECURITY.COM/SUPPORT/](https://www.ariacybersecurity.com/support/))

---




CONTACT US ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/CONTACT-US/](https://www.ariacybersecurity.com/about-us/contact-us/))

CAREERS ([HTTPS://WWW.ARIACYBERSECURITY.COM/ABOUT-US/CAREERS/](https://www.ariacybersecurity.com/about-us/careers/))

PRIVACY POLICY ([HTTP://WWW.ARIACYBERSECURITY.COM/PRIVACY-POLICY/](http://www.ariacybersecurity.com/privacy-policy/))

CYBERSECURITY TERMS AND CONDITIONS ([HTTPS://WWW.ARIACYBERSECURITY.COM/CYBERSECURITY-TERMS-AND-CONDITIONS/](https://www.ariacybersecurity.com/cybersecurity-terms-and-conditions/))

ADR AND SAAS SOLUTIONS TERMS AND CONDITIONS ([HTTPS://WWW.ARIACYBERSECURITY.COM/ARIA-CYBERSECURITY-TERMS-AND-CONDITIONS-ARIA-ADR-AND-SAAS-SOLUTIONS/](https://www.ariacybersecurity.com/aria-cybersecurity-terms-and-conditions-aria-adr-and-saas-solutions/))

 (/about-us/careers)  (/support) 

(<https://twitter.com/ARIACyberSec>) 

(<https://www.linkedin.com/company/aria-cybersecurity-solutions>)

 (<https://www.facebook.com/ARIACyberSec/>)

© Copyright 2021 CSP Inc. All rights reserved.

ARIA Cybersecurity Solutions, which includes ARIA SDS, Myricom network adapters and nVoy security appliances are designed and manufactured by the High Performance Products Division of CSP Inc.





