

Energy Company Powers Up Defences with Proofpoint

The Challenge

- Increase security threat visibility into mission-critical infrastructure and assets
- Accelerate identification of threat and improve incident response
- Enhance ability to gather forensic data

The Solution

- Proofpoint Identity Threat Defense
- Proofpoint Shadow

The Results

- Received only positive alerts of attack activity
- Viewed attacker activity in real time
- Reduced investigation time by two-thirds
- Gained instant, detailed forensic data, supporting action with incontrovertible evidence
- Developed a true partnership with Proofpoint through the deployment lifecycle

The Organisation

This organisation provides energy and related services to millions of consumers and partners worldwide. This multinational company also conducts exploration and energy production operations. Because energy is critical to life and national security, the company relies on technology innovation – developing cutting-edge products, applications and services. With security always top of mind, the company reached out to Proofpoint to add unique capabilities for detecting malicious activity and delivering instant forensic insight.

The Challenge

For an energy company, a major security challenge is securing its complex attack surface. This company has both on-premises and cloud infrastructure, as well as a critical Supervisory Control and Data Acquisition (SCADA) network and devices. Having multiple external partners requires numerous network ingress and egress connections. The focus on DevOps also requires securing endpoints for a large developer community, as well as application code and testing systems. As an energy provider, compliance with industry regulations, General Data Protection Regulation (GDPR), and other security requirements requires clear visibility into the security infrastructure and an ability to capture telemetry in the event of a detected threat.

The company already had a defence-in-depth approach to security and continuously works to implement and improve best practices. Prior to Proofpoint, in several instances, insiders had triggered alerts from the company's security systems. When the SOC team experienced an alert, they had to obtain the user's laptop and investigate manually – scraping system registries and painstakingly piecing together enough forensics to reconstruct what happened. Assuming the SOC could quickly obtain the laptop, the investigation could take hours. To improve responsiveness, the company launched a security initiative focused on securing laptops and workstations.

The Solution

The company initially looked at traditional honeypot technologies but learned about Proofpoint Identity Threat Defense's endpoint-based deception technology as part of their solution research process. They chose Proofpoint Shadow as their solution.

"At first I thought Proofpoint Shadow was just a honeypot," said the information security manager. "It quickly became clear that the Proofpoint approach was much more sophisticated."

Shadow's agentless, intelligence-driven deceptions on every endpoint are tailored to mimic real data, credentials and connections. Now, when a malicious actor – or insider with legitimate network access – attempts to traverse systems, he is confronted with a large number of fake resources that look real. Choosing a safe, undetectable path forward becomes almost impossible, and one misstep alerts the SOC to his presence. Once a deception is tripped, the system begins collecting rich forensic data from systems where the attacker is operating to deliver precise, real-time data for informed and rapid response.

"Proofpoint cut investigation time by two-thirds. The graphical dashboard shows us where the attacker is in relation to crown jewels. We can quickly drill down to specific details, and the system automatically gives us a timeline of what has happened on the endpoint. It's invaluable."

Information Security Manager, Energy Company

The energy company deployed Identity Threat Defense across its estate with help from its MSP and Proofpoint Professional Services. Immediately, the solution identified critical paths to crown jewels and several legacy system misconfigurations that represented vulnerabilities.

"Identity Threat Defense is tremendously helpful," said the information security manager. "It gathers intelligence from endpoints and suggests a pool of the most appropriate deceptions, which saves time and significantly improves our defences. We're also impressed with the Proofpoint team. They listen to our needs with patience, help us tailor defences to our environment and are really responsive."

The Results

After Proofpoint was deployed, it immediately detected instances when an unknown adversary attempted to traverse systems and tripped a deception. Now, the SOC team can see and monitor attacker activity in real time. At the same time, real-time forensics puts attack intelligence at the SOC team's fingertips, enabling them to quickly drill down to specific details – without the adversary knowing he is being investigated. Now the incident response team can quickly determine where to focus their investigation, armed with knowledge of which tools the attacker is using. Proofpoint alerts are simultaneously sent to the company's ServiceNow system, streamlining analyst assignment, response prioritisation and ticket management.

“In the past, we would not have known this activity was happening,” said the information security manager. “We would have needed alerts from multiple security layers and time to ascertain that the alert was positive. Then we would need to quarantine and confiscate the laptop before being able to investigate and collect evidence.”

A real game-changer

“The telemetry has been a game-changer,” he continued. “Identity Threat Defense cut investigation time by two-thirds. The graphical dashboard shows us where the attacker is in relation to crown jewels. We can quickly drill down to details, and the product automatically gives us a timeline of what has happened on the endpoint. It’s invaluable.”

The product’s telemetry also provides incontrovertible evidence. If the attacker is a malicious insider, the company can state unequivocally what occurred and take the necessary action. With more common external attack attempts, the company now has detailed data about the attacker’s goals and techniques so it can strengthen defences where needed.

Foundational to the future

With remote plants, a SCADA environment and IoT devices to defend, the energy company plans to use Identity Threat Defense to extend its defence-in-depth security approach to these assets.

“Identity Threat Defense is a foundational tool,” said the information security manager. “It has been very effective for us. If, for some reason, we had to rationalise our security tools, it would be the last to go.”

LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trade mark of Proofpoint, Inc. in the United States and other countries. All other trade marks contained herein are property of their respective owners.