VARS

Whitepaper

BREACH PROTECTION FOR ENERGY COMPANIES

Powered by Cynet

Business Challenge

Widely classified as critical infrastructure, energy companies traditionally relied on the inaccessibility of their core technology environment to protect against threats. Today, energy companies are focusing on grid modernization, increasing connectivity between information technology (IT) and operational technology (OT) to provide myriad operational benefits and efficiencies. The environment has expanded to remote endpoints and networked devices used across the entire supply chain to improve collaboration, access and control. This interconnectedness, however, opens energy companies to considerable risk.

Interconnected, automated networks increase attack surface for both internal and external threats. Legacy industrial control systems (ICS) that sometimes cannot be updated or patched are particularly vulnerable to threats. Energy environments are built to maximize productivity and often lack the security controls required for protection.

Compounding the challenges of protecting the energy environment is the requirement for services to be "always on." Security controls must be highly accurate and increasingly automated to instantly identify and respond to real risks. This requires complete visibility across the entire infrastructure to ensure fast and effective threat detection and response. Threats that can quickly hobble or completely shut down operations, like ransomware, must be discovered and dealt with as fast as possible.

Energy sector companies are also under increased pressure by government regulators to implement advanced threat protection solutions. The National Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) require operators to significantly improve their ability to protect against cyber threats, including real-time visibility across the environment to rapidly detect of and respond to advanced attacks.

Top Security Challenges

Legacy application and system often can't be updated, patched and adequately protected

Reliance on traditional antivirus and anti-malware software provides limited protection against newer threats like ransomware and cryptolocking

> "Without Cynet we would have needed at least five different solutions to accomplish the same goal, not to mention the time and cost to get the different solutions to work together, if we even could."
>
> CISO, Energy Company

> "We were overwhelmed with alerts from our previous EDR provider. The Cynet XDR platform is far more accurate and automates most of what needs to be done."
>
> Security Director, Energy Company

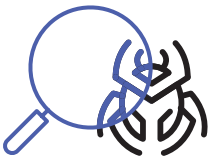
Key Cyber Security Challenges

Protecting an energy environment is highly challenging, especially considering the mix of legacy and modern technologies accessible to a variety of internal participants and third party providers throughout the supply chain. Energy providers, especially those considered small to mid-sized enterprises, have similar issues surrounding threat protecting.

Increased Cyber Attacks

Government intelligence agencies have issued multiple alerts to operators of critical infrastructure regarding cyber threats. All companies in this sector are being increasingly targeted by highly capable nation-state actors and organized crime groups. Attacks on energy providers have increased both in volume and sophistication. Cyber attacks can not only result in stolen intellectual property and service disruptions, but can also lead to more dire consequences if critical safety controllers are altered.

Digitization and interconnectedness mean that criminals can attack the perimeter and ultimately find their way into valuable infrastructure assets. Simple phishing or Trojan attacks on employee or contractor endpoints can provide access to the company network. Using stealthy lateral movement and privilege escalation techniques can ultimately provide unfettered access across the environment.



Limited visibility across environment

Energy companies continue to rely on antivirus and anti-malware software, which only detects a fraction of advanced attacks. These solutions often do not operate or provide very limited protection on older operating system versions that cannot be updated or patched. The bottom line is that even the best heuristic or behavior-based malware detection techniques cannot detect and prevent 100% of threats.

Many energy companies operate over multiple remote locations with different systems and applications used across different sites. This lack of uniformity introduces additional challenges as security protections and risks may differ from one site to the next. To extend protection beyond antivirus solutions, energy companies incorporate additional tools such as endpoint detection and response (EDR) and network detection and response (NDR).

EDR solutions were borne out of the premise that because all endpoint threats cannot be prevented with antivirus software, these threats still need to be detected after they successfully infect an endpoint. EDR solutions continuously monitor endpoints to detect malicious activity and system behaviors that are indicative of compromise.

NDR solutions extend protection to the network to provide additional visibility across the environment. If an attack somehow bypasses both an antivirus and an EDR solution, the ability to detect lateral movement and other network traffic indicators could uncover a threat actor that has successfully infiltrated the environment.

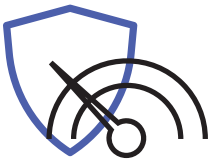
Key Cyber Security Challenges

Cont'd

Siloed security controls

While each of these security controls described above extend needed visibility across the environment, they are not without their problems. First, antivirus, EDR and NDR solutions are notorious for false positive alerts. Security analysts either chase down these false flags or tend to ignore all but the highest risk alerts. In the first instance considerable time is wasted, in the second instance ignoring alerts is far from good security practices and opens the company to compromise.

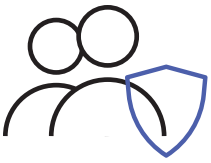
Siloed controls also mean more "panes of glass" for the security team to monitor and access when investigating potential threats. Because each security tool has a separate management console and presents information differently, it is challenging for security analysts to make sense of all the information being presented and then link activities together between the various security controls to see the big picture. This is why stealthy attacks are able to bypass environments with multiple layers of controls.



Small security teams with limited bandwidth

Putting siloed controls aside, which do create significant manual overhead, most security tools require a meaningful human investment to operate. When threats are discovered, security analysts must investigate to determine the root cause and then uncover the full scope of the attack across the environment.

Once the root cause and scope are determined, all threat components must be fully remediated. This often involves access to multiple systems and can be a painstaking, time consuming process.



Small security teams with limited cybersecurity skills

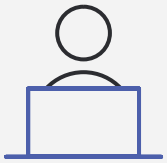
With the threat landscape rapidly evolving even the largest, well funded security teams are vulnerable to threats. Look at any review of breaches against large companies and it's quick apparent that even the best cybersecurity experts with leading-edge tools are challenged to protect their organizations. For smaller security teams with limited technology budgets and cybersecurity expertise, the risk of breach is compounded exponentially.

The Cynet-VARS Approach

Cynet was built for smaller cyber security teams with limited bandwidth, cybersecurity expertise and technology budgets. Cynet XDR provides a single, unified platform to automatically prevent, detect, investigate and fully remediate the broad range of attack vectors faced by energy sector companies. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

Cynet XDR is the only solution that triggers an automated investigation following each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities to fully eliminate the threat. Cynet also provides a broad set of automated and highly customizable remediation actions to address threats according to your preferences. Moreover, Cynet provides an expert team of cybersecurity experts to augment and guide your team 24 hours a day, 7 days a week – included with the Cynet 360 platform.

Cynet Benefits for Energy



Easy to Deploy and Operate

The Cynet agent can be deployed to over 5,000 endpoints in less than an hour. While many solutions require months to deploy and become fully operational, Cynet is fully functional within 24 hours of deployment, providing all the insights and protections available in the platform. The Cynet console was built to be intuitive and effortless so smaller security teams do not need years of expertise to operate.

Full Visibility Out of the Box

Cynet XDR provides complete visibility and multiple points of telemetry leading to low false positives and early detection of stealthy threats. A single, unified Extended Detection and Response (XDR) platform that provides Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), User and Entity Behavior Analytics (UEBA) and Deception technology fully integrated and easily configurable with a single dashboard out of the box.

Cynet Benefits for Energy

Cont'd

Automated Protection

Cynet's Incident Engine automatically performs all required threat investigation and response actions, uncovering the root cause and full scope of high risk threats and taking appropriate actions to fully eradicate the threat across the environment. Cynet additionally provides an array of remediation playbooks that can be executed automatically in response to a detected threat for immediate response or can be triggered manually to provide more oversight and control. Cynet's autonomous response actions provide the comprehensive protection needed by smaller and overburdened security teams.

Include Managed Detection and Response Oversight

All Cynet clients are automatically protected by a comprehensive Managed Detection and Response (MDR) service, included with the Cynet platform at no extra cost. Small security teams at energy companies rely on Cynet's MDR team (CyOps) to proactively monitor their environment 24x7 to ensure nothing is overlooked. They can contact VARS at any time for guidance in configuring the Cynet platform, providing attack investigation expertise and guiding them on all necessary response actions. CyOps becomes an extension of the engergy company security team, adding resources and world-class cybersecurity expertise.

Summary

Protecting energy company environments from cyberattacks is beyond challenging, especially with a smaller, less experienced security team. With limited budgets, most small to mid-sized energy companies cannot obtain, integrate and operate the required security controls to protect the organization from advanced threats. Energy companies rely on Cynet's intuitive, comprehensive breach protection platform to solve their security challenges, knowing they always have a team of cybersecurity experts watching their backs.