




Breaching the Energy Sector: Protecting Critical Infrastructure Against Advanced Cyber Exploits

The recent cyberattack on Halliburton, a global leader in the energy sector, is yet another alarming indicator of the growing and increasingly sophisticated threats targeting critical infrastructure. The energy sector is a prime target for cybercriminals due to its essential role in global economies and the potential to cause mass disruption. This latest example once again exposes the security gaps that persist within critical infrastructure, and how criminals exploiting vulnerabilities in systems like Active Directory (AD) can cause potentially devastating consequences for business and industry.

Security must extend beyond the perimeter

Sophisticated attacks like those on Halliburton and other critical infrastructure entities show that organizations can no longer solely rely on perimeter-based security. A proactive, multi-layered defense is essential to thwart these ever-evolving threats.

In this whitepaper, we explore how Data Protection and Risk Mitigation (DPRM) solutions can secure and segment AD – mitigating the risk of critical vulnerabilities.

A decorative graphic consisting of a grid of binary code (0s and 1s) in a light blue color, set against a dark blue background. The code is arranged in a pattern that suggests a digital tunnel or data flow.

Traditional perimeter-based security is no longer sufficient to combat advanced threats like ZeroLogon, which target core infrastructure systems such as Active Directory.

Paul German – CEO, Certes



By implementing a consistent policy-defined data protection approach rather than traditional network-focused segmentation, organizations can significantly reduce the likelihood of a successful attack on their AD systems.

We will examine how [DPRM](#) can serve as a proactive defense mechanism, limiting attackers' ability to exploit vulnerabilities like ZeroLogon, and thereby ensuring the integrity and security of your organization's most critical assets.

Halliburton attack – a wakeup call to the utilities sector

The attack on Halliburton earlier last month forced the energy giant to shut down some of its internal systems in an attempt to prevent further unauthorized access. Official details as to the nature of the attack are still to be confirmed, but the compromise of core systems like AD could have led to this widespread operational disruption.

Using built-in functionalities of network infrastructure and applications, attackers can evade detection and blend seamlessly into normal network traffic (referred to as 'living-of-the-land' attacks). This stealthy operation means that attackers can remain undetected by traditional security measures, further demonstrating the need for proactive solutions that strengthen defenses at entry points and throughout the network.

As the world's second-largest oil service company, any disruption not only impacts Halliburton's reputation but puts its customers and the entire supply chain at risk. So, the operational disruption to Halliburton's internal systems and global connectivity networks reinforces why the security industry must change its approach and not rely on traditional measures that have proved ineffective and unable to prevent ZeroDay attacks or exploitations of vulnerabilities in pivotal functions such as Active Directory.



A broader industry crisis

While it's unclear whether the Halliburton attack was indeed ransomware, early [reports](#) suggest that the RansomHub ransomware gang was the likely perpetrator. This possibility is alarming, given the increasing frequency of high-profile ransomware attacks on critical infrastructure in recent years.

For example, the ransomware attack on the Colonial Pipeline in 2021 saw the shutdown of one of the USA's largest fuel pipelines. As a result, approximately 100 million gallons of oil were stopped from Houston to the New York Harbour, causing mass shortages and panic buying.

Data segmentation and cryptographic protection are key to mitigating the risks posed by sophisticated cyber exploits. Certes DPRM's policy-driven approach not only restricts lateral movement across networks but ensures that sensitive communication channels remain secure, even when attackers gain a foothold.

Simon Pamplin – CTO, Certes

Compromised Active Directory: granting unrestricted access to your data

Active Directory is an attractive target for attackers because of the crucial role it plays in managing user identities and access controls. Compromising AD means attackers can potentially gain access to a treasure trove of critical and sensitive resources across the network.

A key objective in these attacks is often the extraction of the NTDS.dit file, which stores vital and sensitive data, including hashed password values. While this file is in constant use, making it difficult to extract, attackers can use available tools like Volume Shadow Copy, NTDSUtil, or snapshots in virtual environments to obtain it from critical systems. Once extracted, tools such as Mimikatz or Hashcat can be used to enable attackers to elevate privileges and entrench their presence within the network. This post-compromise lateral movement sustains persistent detection evasion, making it exceedingly difficult to identify and remove attackers from the system.

Ultimately, the end goal often involves gaining access to Operational Technology (OT) assets where the consequences of regulatory fines for breaches of Personally Identifiable Information (PII) only pile on to the very real threat of critical infrastructure shutdown.

A broader industry crisis

One of the most concerning vulnerabilities exploited by attackers in recent attacks on AD environments is ZeroLogon. This critical flaw in the Microsoft Netlogon Remote Protocol, used by Windows servers for authentication, allows attackers to manipulate authentication exchanges and reset the password of a Domain Controller (DC) with alarming ease. Once exploited, ZeroLogon can lead to a complete compromise of the AD environment, giving attackers full control over all systems within the domain. This access can be used to deploy ransomware, steal sensitive data, or even shut down operations entirely.

How can Certes DPRM prevent such exploits?

Deploying Certes Data Protection and Risk Mitigation (DPRM) to secure and segment AD environments offers a robust defense against exploits like ZeroLogon (CVE-2020-1472) through a combination of granular security controls:

1 Data Segmentation and Microsegmentation:

- Certes DPRM enforces strict data segmentation, ensuring only authorized and authenticated users or systems can communicate with critical resources like domain controllers.
- By segmenting the AD environment and restricting communication flows between servers, workstations, and DCs, Certes DPRM reduces the attack surface. Even if an attacker gains access to the network, lateral movement is stopped, preventing the exploit from reaching the DC.

2 Cryptographic Data Protection:

- Certes DPRM enables policy-defined data protection in transit across the network. With the Netlogon protocol traffic encrypted with quantum-safe algorithms, it becomes virtually impossible for attackers to intercept and manipulate the authentication process – a key step in the ZeroLogon exploit.
- By enforcing protection policies on sensitive communication channels, Certes ensures that vulnerabilities like ZeroLogon cannot be easily exploited through traffic interception or tampering.

With real-time monitoring and strict access control policies, Certes DPRM minimizes the potential damage of breaches by limiting unauthorized access and rendering stolen data valueless.

Paul German – CEO, Certes

3 Policy Enforcement:

- Certes DPRM allows organizations to define and enforce consistent security policies, including restrictions on the types of communication allowed between various network segments.
- Policies can be created to ensure that only specific, trusted systems can interact with the domain controllers, only under specific protocols or conditions, and from trusted/known locations.
- E.g. By limiting end-user access to only Read Only Domain Controllers (RODC), and defining the direction and location of update flows to the RODC, DPRM can control and prevent any changes to privilege levels. This means attackers can only communicate with RODCs, which lack replication permissions, thereby halting persistent malicious activities.

4 Real-time Monitoring and Alerts:

- The system continuously monitors network traffic and enforces policies in real-time with no impact on performance no matter where the data travels or is taken. Separating data security from network security keeps the security posture consistent and not dependent on infrastructure be that physical, virtual, or cloud.
- Typical security monitoring is reactive, requiring a breach to occur before acting to prevent the spread. Certes DPRM assumes the infrastructure will be breached so focuses not on patching the infrastructure but on making the subject of the breach (the data) inaccessible or valueless to the attacker. In this way, DPRM is resistant to a ZeroDay attack in a way that traditional network security is not.

5 Access Control and Least Privilege:

- Certes DPRM supports the principle of least privilege by controlling and limiting access to AD components based on role and need.
- Even if an attacker compromises a user account, they are constrained by strict access controls, removing their ability to exploit the vulnerability.

Proactively stopping sophisticated cyber attacks in their tracks

By deploying Certes DPRM to secure and protect Active Directory, organizations can prevent the exploitation of vulnerabilities like ZeroLogon by limiting attackers' ability to communicate with and compromise domain controllers.

Access to Active Directory is typically the first port of call for the majority of network breaches, DPRM separates the protection of data from the access to the network. By doing so it can protect data outside of credential or network access methods rendering the data only accessible to trusted locations and devices that are themselves protected by DPRM policies and enforcement points.

The combination of data segmentation, quantum-based cryptography for data in transit, strict policy enforcement, and real-time monitoring creates a robust defense that minimizes the risk of such critical exploits compromising the AD environment.

By adopting proactive measures like Certes DPRM, organizations can protect their own operations and also contribute to the broader defense of the industry against sophisticated cyber threats. Now is the time to strengthen your defenses and ensure the security of your most critical assets.

As attacks on critical infrastructure grow more sophisticated, industry players must rethink security from the inside out. Certes DPRM offers a proactive solution by enforcing least-privilege access to Active Directory components, ensuring that even if attackers infiltrate the system, their impact is severely restricted.

Simon Pamplin – CTO, Certes

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai

