Hope Is Not A Strategy:

Rethinking Data Protection in the Age of Zero-Day Attacks

In the cybersecurity landscape, the term "zero-day" strikes fear among IT professionals worldwide. But what exactly does it mean? And why should it prompt us to reassess our security strategies?

Recent data from Google's Threat Analysis Group (TAG) and Mandiant underscores the escalating frequency of zero-day vulnerabilities. In 2023 alone, 97 zero-day vulnerabilities were exploited - a significant rise from the previous year's count of 62.

Our whitepaper delves into the shift required in cybersecurity, highlighting the urgency of safeguarding data amidst the rising threat of zero-day attacks. We challenge the conventional wisdom of relying solely on perimeter-based security and urge businesses to take a proactive approach centred on zero-trust data access.

Hope is not a strategy. It's time to move beyond hope and adopt robust, proactive strategies to protect our data and systems from these ever-evolving threats.

> **Hope is not a strategy. To protect our data and systems from the ever-evolving threats of zero-day attacks, we must adopt robust, proactive measures beyond traditional perimeter security.**
>
> *Simon Pamplin – CTO, Certes*

Understanding Zero-Day Attacks

A zero-day attack is an exploit or vulnerability that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. It strikes without warning, bypassing traditional security measures and leaving organisations vulnerable to data breaches, ransomware, and other malicious activities. According to IBM, “zero day” refers to the fact that the software or device vendor has zero days to fix the flaw because bad actors can already use it to access vulnerable systems.

Currently, the industry focuses on reactive solutions and patch management to address known vulnerabilities, which means zero-day attacks remain a persistent threat. They leave huge numbers of users/organisations wide open to cybercrime until the vendor identifies the problem and releases a solution.

The reality is, that no amount of perimeter security or credential-based authentication can fully mitigate the risk posed by these unseen threats so you cannot hope that you’ve done enough.

Keeping up with Zero-Day Attacks

The ongoing battle against zero-day exploits mirrors a game of cat and mouse between security teams and cyber attackers. As soon as one vulnerability is fixed, attackers are already searching for the next weakness to exploit.

For years, organisations have heavily invested in perimeter security tools like firewalls and intrusion detection systems. While these defences offer some protection, they work reactively - they can't stop zero-day attacks from occurring.

This solution is like strengthening the doors and windows of a house, only to find intruders sneaking in through the ventilation system. It pushes the question, why are reactive responses still the go-to option?

This approach - responding to known threats and guarding against previously identified vulnerabilities - causes organisations to go around in circles, mistakenly hoping and believing that their existing perimeter security is sufficient to protect sensitive data, many organisations overlook the fact that hope is not a strategy and this approach does not work, as evidenced by the rise of data breaches. It is crucial for organisations to move beyond reactive measures, focus on protecting the target of these attacks (the data) and proactively address emerging threats to truly safeguard their data.

This is why security teams are faced with such a tough challenge when it comes to zero-day vulnerabilities. These hidden weaknesses linger undetected and unpatched, allowing attackers to breach systems and cause damage before defenders can respond. Such vulnerabilities slip past traditional cybersecurity risk management and mitigation efforts, leaving organisations exposed to unforeseen dangers such as the stealing of sensitive data. To help security teams, CISA offers a catalogue of known exploited vulnerabilities with descriptions of potential threats and the actions to take to address the vulnerability. However, it is too late by this point as the attacks have already happened.

We also see similar advice from the UK National Cyber Security Centre who advise all UK businesses to document the information their organisation holds and to have a good backup system in place in the event of a ransomware attack.

> **Zero-day attacks exploit unknown vulnerabilities, bypassing conventional security measures and leaving organisations exposed to severe risks. We must prioritize zero-trust data access to safeguard our most valuable assets.**
>
> *Paul German– CEO, Certes*

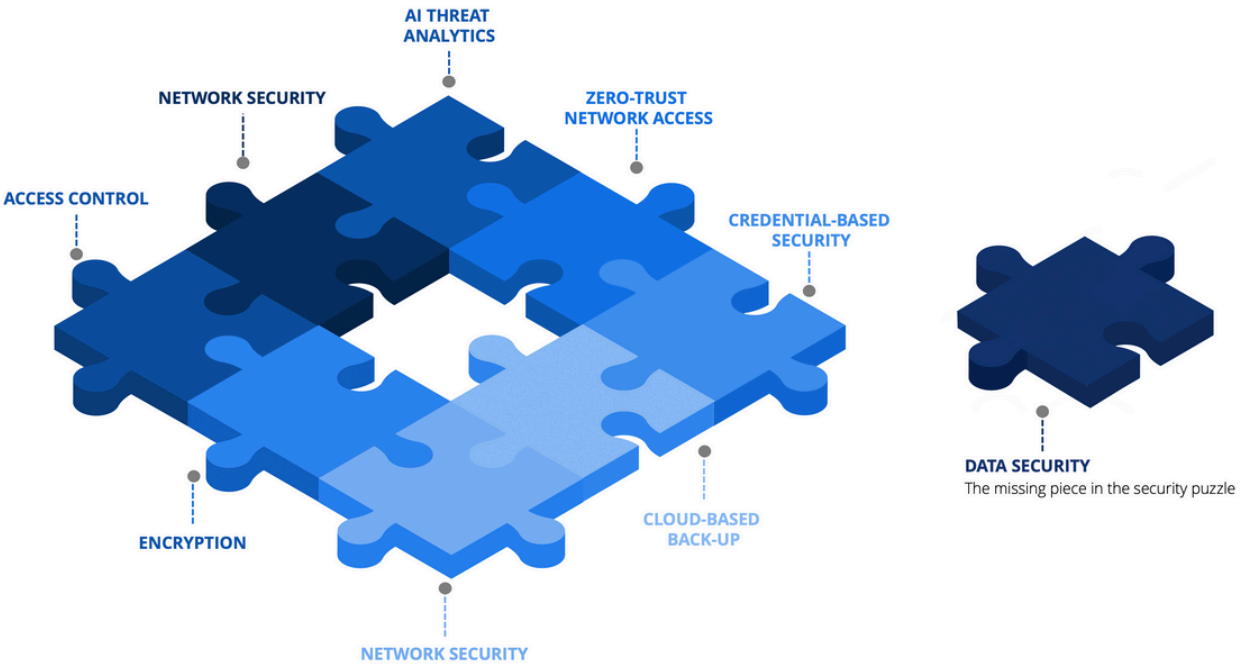
Redefining Security: Zero-Trust Data Access

Leading network security vendors, including Palo Alto Networks, CISCO, and Fortinet, frequently disclose Common Vulnerabilities and Exposures (CVE) related to zero-day vulnerabilities. Notably, CISCO made headlines when it revealed that a state-backed hacking group exploited vulnerabilities in its Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls in November 2023 to spy on government networks.

Despite this, they maintain a reputation for security. However, their reliance on reactive security measures leaves them struggling to address new risks. The rise of AI-driven hacking tools only amplifies the threat of unknown or zero-day attacks.

To combat the escalating threat of zero-day attacks, we need to shift our focus away from relying solely on perimeter defence and towards safeguarding our data. This is where zero-trust data access comes into play – a proactive strategy that operates on the assumption of no inherent trust, even within the network perimeter.

Zero-trust data access involves granular control over who can access data, from where, and using what device. By enforcing rigorous access controls, organisations can reduce the potential impact of breaches and mitigate the consequences of zero-day exploits.



These capabilities are central to data-centric security solutions like Certes DPRM. Designed to prioritise the protection of data itself, independent of infrastructure security, these solutions ensure that even in the event of a zero-day attack, your data remains secure and intact, wherever it resides.

Challenging Industry Norms

The cybersecurity industry is ripe for disruption. Traditional vendors endorse solutions focused on breach detection and recovery, perpetuating the myth that perimeter security alone is sufficient. However, hope is not a strategy, and you cannot assume you've done enough to protect your information. It's time to challenge these norms and demand proactive measures that prioritise data protection.

Zero-day attacks are not a distant threat - they are a stark reality facing organisations of all sizes and industries. To stay ahead of the curve, we must rethink our approach to cybersecurity and prioritise zero-trust data access above all else.

> **"In the battle against zero-day exploits, traditional reactive responses are no longer sufficient. To stay ahead, organisations must shift focus from perimeter defenses to securing data itself through zero-trust access controls."**
>
> *Simon Pamplin – CTO, Certes*

By embracing the principles of zero-trust data access, organisations can fortify their defences against the ever-present danger of zero-day exploits. It's time to break free from the confines of perimeter security and forge a new path towards a more resilient and secure future.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai