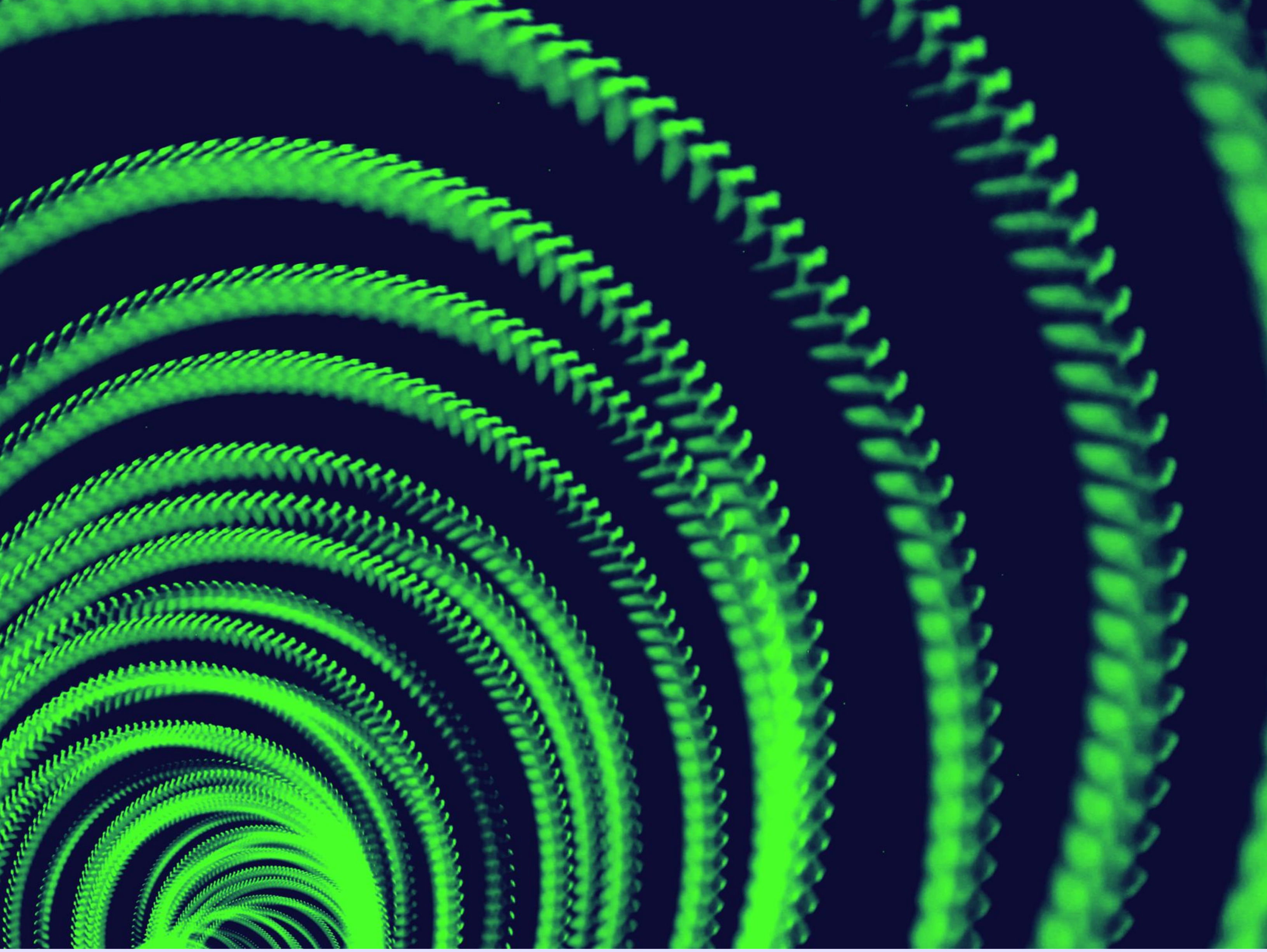


Securing Virtualized Environments:

THE IMPERATIVE OF PREEMPTIVE PROTECTION

CENTRIPETAL

In the digital age, virtualization has become the cornerstone of many modern IT infrastructures. With Virtual Desktop Infrastructure (VDI) and Virtual Server technologies playing mission-critical roles in numerous organizations, ensuring their security is paramount. However, like all software, these technologies are susceptible to vulnerabilities. Securing virtual environments can bring unique challenges highlighted by well-known and often exploited vulnerabilities as well as limited patching opportunities on mission critical infrastructure. Intelligence powered cybersecurity can deliver a reprieve from the risks incumbent in critical systems, offering protection during the vulnerability window.

VDI infrastructure from Citrix and VMWare have been frequently in the news over the last year as new and damaging vulnerabilities have been identified by both research teams and hackers. Exploits of these vulnerabilities have caused extensive damage to many organizations and businesses worldwide. In the UK, one Citrix vulnerability (CVE-2023-3519) was identified by the NCSC as being the vector of several attacks on critical national infrastructure. CISA in the US reported similar exploits of this vulnerability. And the well documented 'Citrix Bleed' vulnerability had even broader impact globally. VMWare also had multiple remote code execution vulnerabilities that were exploited in the wild including CVE-2022-22954.

Of course this is not unusual, all software systems are prone to security vulnerabilities. However, many critical systems are dependent on virtualization technologies and as a result, these specific vulnerabilities can have broad implications in several key verticals including healthcare, manufacturing, and law enforcement. The challenge with many critical systems is that opportunities to patch may be limited and highly restrictive. IT administrators do not want to impact business operations by taking systems offline even for a few minutes.

As a result, patching is often delayed by:

30 – 90 days

leaving a window of vulnerability that malicious actors can exploit.

To mitigate the risks associated with vulnerabilities in unpatched critical systems, businesses and organizations should look at preemptive protection solutions powered by threat intelligence.

While an inward security focus might look at vulnerabilities and how they can be patched, an outward focus looks at where exploits will come from and what will they look like. Threat Intelligence provides the visibility of threat actors and the attack vectors they are employing.

By leveraging that threat intelligence at massive scale and in real time, Centripetal implements a highly effective enforcement solution that shields against malicious actions and attempts to exploit vulnerabilities. The real time nature of the intelligence feeds means that Centripetal's CleanINTERNET® product provides a preemptive protection layer, blocking vulnerabilities from being exploited across the network. Additionally, because Centripetal blocks all known malicious IOCs, attempted exploits can be blocked before the vulnerability is known about by the wider community. Indeed, it is by providing protection during the entire window of vulnerability, that Centripetal delivers mitigation from an imperfect patching process. While waiting for the opportunity to patch a critical and vulnerable system, CleanINTERNET® provides the reassurance of a robust defense against any attempt to exploit those vulnerabilities.

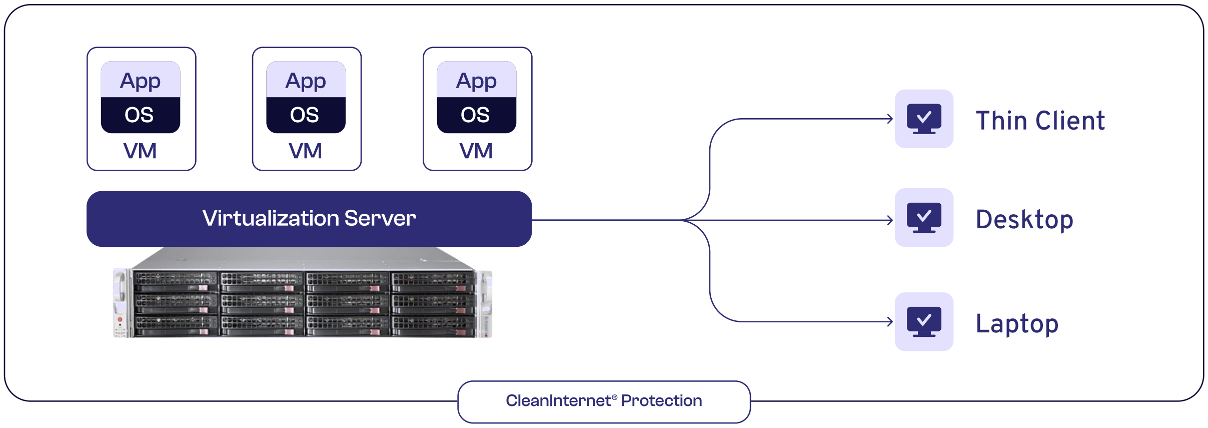
Understanding the lifecycle of a vulnerability is crucial for developing effective security measures. By acknowledging the inevitability of vulnerabilities and adopting preemptive protection measures, organizations can effectively mitigate the impact of security breaches, while executing a considered and more confident patching plan.

CleanINTERNET® leverages threat intelligence to gain visibility into global attack activities, enabling organizations to stay ahead of emerging threats.

The solution utilizes real-time threat intelligence to deliver preemptive protection, significantly reducing the risk of exploitation.

In conclusion, securing virtualized environments requires a proactive stance against vulnerabilities. Preemptive protection measures offer organizations the means to defend against evolving threats and safeguard their critical assets. While patching remains essential, preemptive protection ensures that organizations are not solely reliant on reactive measures. By embracing preemptive protection strategies, organizations can navigate the complex landscape of virtualization security with confidence.

Protecting Virtualized Environments



ABOUT CLEANINTERNET®

CleanINTERNET® is an intelligence-powered security solution using high performance computing technology, patented software algorithms and uniquely skilled security analysts to deliver a robust alternative protection strategy at significantly lower cost.

CleanINTERNET® presents an alternative approach to cybersecurity, putting threat intelligence at the forefront, moving from reactive to proactive defense, and helping security teams be more efficient and effective.

ABOUT CENTRIPETAL

Centripetal, the global leader in intelligence powered cybersecurity, is operationalizing the world's largest collection of threat intelligence, in real-time, to protect organizations from every known cyberthreat through its innovative patented technologies.

The company's CleanINTERNET® solution delivers the only proactive approach to intelligence powered cybersecurity, leveraging the latest computing technology and skilled operations intelligence analysts, at dramatically lower cost.

For More Information

centripetal.ai

CENTRIPETAL

CENTRIPETAL

centripetal.ai