WHITEPAPER

The Value of CAASM During A Recession

LUCIDUM

Introduction

In today's increasingly digital economy, cybersecurity is a critical concern for organizations of all sizes and industries. As businesses continue to rely heavily on technology to store, process, and transmit information, the risk of cyber-attacks has increased, making it more important than ever for organizations to take a proactive approach that identifies and mitigates vulnerabilities in an organization's technology infrastructure. Cyber Asset Attack Surface Management (CAASM) is a proactive approach that is a valuable component of an organization's cybersecurity strategy, especially during the recession.

Economic downturns often result in tighter budgets, making it crucial for organizations to invest in cost-efficient solutions that reduce the risk of cyber-attacks. Cyber Asset Attack Surface Management (CAASM) is a cost-efficient solution that identifies and mitigates vulnerabilities in an organization's technology infrastructure.

CAASM is a proactive approach to cybersecurity.

Aimed at identifying and mitigating vulnerabilities before they can be exploited by cybercriminals. Proactively identifying and mitigating vulnerabilities in an organization's technology infrastructure prevents data breaches and network intrusions, thereby lowering the cost of incident response and recovery.

CAASM minimizes the need for additional cybersecurity personnel.

By automating the process of identifying vulnerabilities in an organization's technology infrastructure, CAASM allows the existing security analysts and incident responders to concentrate on remediation.

CAASM prioritizes vulnerabilities.

With limited resources and budget, organizations need to address the most critical vulnerabilities first. CAASM solutions often come with built-in risk scoring mechanisms that help organizations prioritize vulnerabilities. Organizations can then focus their resources on the vulnerabilities that pose the greatest risk to their operations, rather than wasting time and money on less critical vulnerabilities.

CAASM solutions help organizations quickly respond to cyber threats.

By providing real-time monitoring and alerts, CAASM solutions helps organizations quickly detect and respond to cyber threats. Furthermore, CAASM solutions often come with built-in incident response playbooks and automated remediation capabilities, which can help organizations to quickly and effectively respond to cyber threats.

CAASM also helps organizations comply with regulations and industry standards.

Such as HIPAA, SOC2, and PCI-DSS. By identifying all assets and users in an organization's technology infrastructure and finding potential vulnerabilities, CAASM helps avoid costly penalties and fines.

CAASM solutions integrate with other security solutions.

This allows organizations to leverage their existing security investments and extend their capabilities, getting more out of the existing solutions. For example, by integrating with a firewall, a CAASM solution can include information about blocked traffic from known malicious IP addresses and include this information in reports and dashboards, reducing the risk of a successful cyber-attack. By integrating with a SIEM solution, a CAASM solution can provide additional context and correlation to security events, making it easier for organizations to detect and respond to cyber threats.

CAASM solutions can save organizations money in unused cloud instances and unused licenses.

Because CAASM solutions discover all assets, both cloud and on premises, CAASM solutions can highlight the cloud resources that are not being used or are used very sporadically. CAASM solutions can also highlight unused seats in enterprise software licenses. Both these features can save organizations money, summary, CAASM is a cost-effective solution that can help organizations to reduce their risk of a costly cyber-attacks, do more with their existing security staff, comply with regulations and industry standards, get the most out of their existing solutions, and save money on unused resources.

During a recession, investing in CAASM is a smart move for organizations that want to maintain their cybersecurity posture while being cost-effective.

About Lucidum

Lucidum was built by cybersecurity experts on a mission to gain full visibility into their tech ecosystem. We take pride in our innovative platform, and we're thrilled each time we offer our customers the ability to see and understand what was formerly lurking just off the radar.

We put everything in your sights, giving you the power to understand what it is and what it's doing. Understand the lay of your tech landscape, lock onto threats, and keep your perimeter secure – all empowering you to defend and dominate your space in an increasingly threatening world.

LUCIDUM