Technology Challenges + Solutions

Use Cases by Challenge

Missing or Poor Data Encryption

Government agencies are a prime target for both foreign and domestic cyber attacks that continue to increase dramatically in terms of volume and sophistication. While fighting to prevent attacks set out to retain control of access to data that have missing or poor data encryption, agencies continue to be the susceptible target of criminal intent.

Solution

Secure sensitive data and host applications in a disguised fashion with controlled access and non-traceable connectivity. Create protected environments within and across multiple public and private clouds.

Misconfigurations

System, software and hardware misconfigurations are becoming extremely common as digitalization continues to be part of the security team's transformation strategy. Security teams are overwhelmed with the changes happening around them and oftentimes put configuration validation on the back burner. Misconfigurations give adversaries specific targets to probe, looking at common software and hardware for common configuration errors.

Solution

Augment or replace your existing WAN connections to increase privacy and security between the enterprise, branch, datacenter, internet, and cloud.

Weak/Non-Existent Authorization Credentials

and sophistication. While many academic institutions struggle to prevent malware and control access to their data and internet communications, they are particularly susceptible to targets of credential harvesting and other authorization attacks such as brute forcing which give bad actors access to the user account once the credentials are correctly identified.

Solution

Students & Faculty are under threat from ransomware. Deploying ConcealSearch to individuals secures their email and browsing sessions by proactively isolating their networks and systems from web-borne threats. This limits an adversary's ability to capture the user credentials, eliminating the potential vulnerability surrounding credentials.

Malicious Insiders

When legitimate credentials of employees, contractors, business associates or others are maliciously or intentionally abused, extreme harm can be caused to the target organization. Detection and response capabilities are less likely to pick up on the malicious activity of a legitimate user in the moment. This reality makes the exfiltration of confidential data such as personal identifiable information of employees or customers or financial information related to the organization extremely hard to catch in the act.

Solution

Through the investment of Conceal, a malicious insider's ability to cause harm or havoc originating from the web is remediated. Through the combination of ConcealBrowse, ConcealSearch, and ConcealCloud, it is near impossible for a user to download malicious content or perform corruption via the internet.

 | (706) 481-2642 | conceal.io | info@conceal.io

Zero Days

Unknown vulnerabilities discovered by adversaries are extremely harmful to organizations that have invested in the software with the zero day. When exploited, these vulnerabilities can cripple the victim organization until they are able to identify the vulnerability themself. Since zero-days are not defendable until after the attack has happened, threat actors that discover a zero day are able to cause extreme havoc in the industry.

Solution

Conceal addresses the privacy and security needs of Law Enforcement agencies offering additional security, privacy, performance, and significant cost reductions. Entities that conduct investigative research and intelligence collection utilize Conceal's solutions to remain unidentifiable to criminal elements, prevent websites from filtering or denying content, and enable discreet online surveillance.

Unpatched Software

Unpatched and out of date software opens an organization's network up to a variety of vulnerabilities. Threat actors can target software with known patches to test an organization's patch management strategy. With unpatched software, threat actors can exploit vulnerabilities that the patches are looking to remediate.

Solution

Insurance companies are trusted institutions that protect individuals and businesses against risk. Yet, they need to protect against their own risk due to the volumes of customer data, communications, intellectual property and content they handle while operating on the internet and across a network. Conceal solutions obscure critical identity and address privacy and security needs by offering enhanced safety, confidentiality and performance at significant cost reductions.

Weak/Non-Existent Authorization Credentials

With weak and non-existent authorization for employee credentials, adversaries can brute force their way into a user account. Without complex authorization requirements, cyber criminals can gain an employee's credentials through trial and error, giving them the keys to the kingdom once they are inside.

Solution

Cyber attacks targeted at the critical infrastructure industry are not new and are rising. Conceal provides the results to strengthen your enterprise's defenses against threat actors and cyber threats. Conceal addresses these issues by creating solutions for security, privacy and performance with significant cost reductions. Conceal products guard against cyber threats like ransomware and malware; prevent websites from filtering or denying content; and provide a reduced cyber-attack vector.