WHITEPAPER

Attivo NETWORKS®

9 NOTABLE 2020 CISO CHALLENGES - ARE THEY THE SAME AS YOURS?

INTRODUCTION

The world has changed in so many ways in 2020. Even with the best-laid plans and precautions, CISOs had to respond to the COVID-19 pandemic quickly, revising strategies and transitioning from "unprepared" to "prepared." Here is a list of nine important things CISOs are tackling as they look to stay one step ahead in these rapidly changing times and how the Attivo Networks ThreatDefend solution is helping organizations to mitigate their existing security challeneges and risks.

1. HOLD PLEASE

Many big projects, planned and in progress, have been put on hold indefinitely based on budget uncertainties and the prioritization of addressing the surge in remote workers.

Unfortunately, rather than following suit, attackers are actively seeking ways to exploit the disruption caused by the pandemic.

It is clear that returning to "normal" may not happen any time soon or even in the ways we previously knew them. CISOs need to get more creative in how they grant their security teams resources and funding to advance and improve their security postures. Many of these projects will focus on expanding VPN access and new forms of infrastructure for scalability to cover any environment on any device. As such, these new services now occur more frequently in the cloud, given their on-demand nature and access for remote users. As CISOs make these changes, they must evaluate their current security controls and identify gaps covering these new and potentially permanent remote users and how they can manage privileged access management.

ATTIVO SECURITY TIP

As organizations change their remote access programs and increase their use of split-tunneling VPNs to keep business traffic separate from personal traffic, they will face new security challenges. Traditional controls and baselines will no longer be adequate, and they will also need to ramp up supplier access monitoring to ensure compliance with data handling standards.

The Attivo ThreatDefend® platform reduces remote security team and administrator risk related to VPN and AD reconnaissance threat detection. It also provides proactive threat detection with decoy VPN credential bait and cloud and SaaS credential monitoring.

With this solution, security teams can monitor for the use of disabled SAAS accounts and services, as well as unauthorized queries to Active Directory that indicate attacker attempts to escalate privileges and identify critical targets. The platform can create detection campaigns that reference cloud administration activities and alerts if a remote worker or supplier's endpoint attempts to gain administrative access to cloud resources, thus protecting the business' VPN infrastructure.

2. SECURING THE REMOTE USERS

The general mandate from executives was to get employees up and running first and then address security afterward. To achieve a quick transition and restore operations, many organizations had to complete rapid assessments, tweak controls, and make do with technologies they already had. Most companies were not adequately prepared for this transition and saw their remote workers spike from sub 10% to 100% in many cases. They found their current VPN infrastructure unable to address the flood of remote traffic and the associated risks that came with it. The security teams suddenly found themselves at the mercy of remote users and the user's ability to secure their devices, because much of the traffic was no longer routing through existing perimeter security controls. The risk of stolen VPN and SaaS credentials also surged as many users did not apply secure practices in how they used or shared this information.

ATTIVO SECURITY TIP

By deploying the Attivo ThreatDefend platform, organizations can reduce their risks related to split-tunneling VPN operations and SaaS credential security. The solution provides rapid detection of attackers attempting reconnaissance within the VPN subnet. It can create VPN credential and concentrator decoys to detect attacks targeting the VPN infrastructure. These decoys engage the attacker while providing high-fidelity alerts and recordings of their activity for faster investigation and response. Given that all detection alerts originate from direct engagement, the security teams also benefit from the fact that each alert represents confirmed malicious activity, a policy violation, or a configuration issue (i.e., misconfigured storage buckets). Platform users cite a 12X improvement in investigation and response time, which can be invaluable during the surge in alerts they are likely seeing and in the challenges associated with trying to address all of them.

3. SECURING THE QUICK WIN

CISOs are seeking out tools that help them find their devices, understand patching holes, and identify exposed or orphaned credentials that create risk. There are many tools available to help assess vulnerabilities. However, visibility remains a top challenge, and CISOs are assessing their tools to understand exactly what they can see today and what tools they need to provide additional information and insight into risks to close these security gaps

ATTIVO SECURITY TIP

The ThreatDefend platform takes low effort to implement, maintain, and operate while adding value with the early visibility and detection of attacks that target on-premises, cloud, and remote work environments.

The platform simplifies operations by using machine learning to understand the network and create decoys and lures that mirror-match to production assets, objects, and credentials. Because of this, security teams gain valuable insight into adds/changes to the network and can now see new unauthorized devices entering the environment.

Additionally, as part of the Endpoint Detection Net (EDN) product suite, organizations gain insight into the attack paths an attacker can take to get to their target assets. A security team can view this topographically, making it easy to understand associations. Alternatively, they can view it in a table form so they can see possible first, second, and third hops an attacker could take in their journey based on the use of exposed, orphaned, and misused credentials. This functionality is unlike other visibility tools, and existing customers have used it heavily during these changing times to reduce their overall attack surfaces.

4. LOCK DOWN THE ENDPOINT

CISOs are dealing with three key priorities in securing endpoints. The first is providing secure network access, the second is blocking malware, and the third is preventing unauthorized credential access and use. Some may seek to turn unmanaged computers into managed corporate assets, though most will focus on security policies and controls for unmanaged devices.

Typically, organizations will employ Endpoint Protection Platform (EPP) solutions as part of their essential baseline Typically, organizations will employ Endpoint Protection Platform (EPP) solutions as part of their essential baseline security controls along with firewalls, IPS/IDS, and proxies. If kept up to date, these traditional "antivirus" platforms should catch attacks with a known signature. Effective antivirus software will probably stop about half of the attacks and will do a good job stopping most commodity malware or ransomware. If the attacker modifies the signature of the attack in any way, that's where the EPP solution will have trouble.

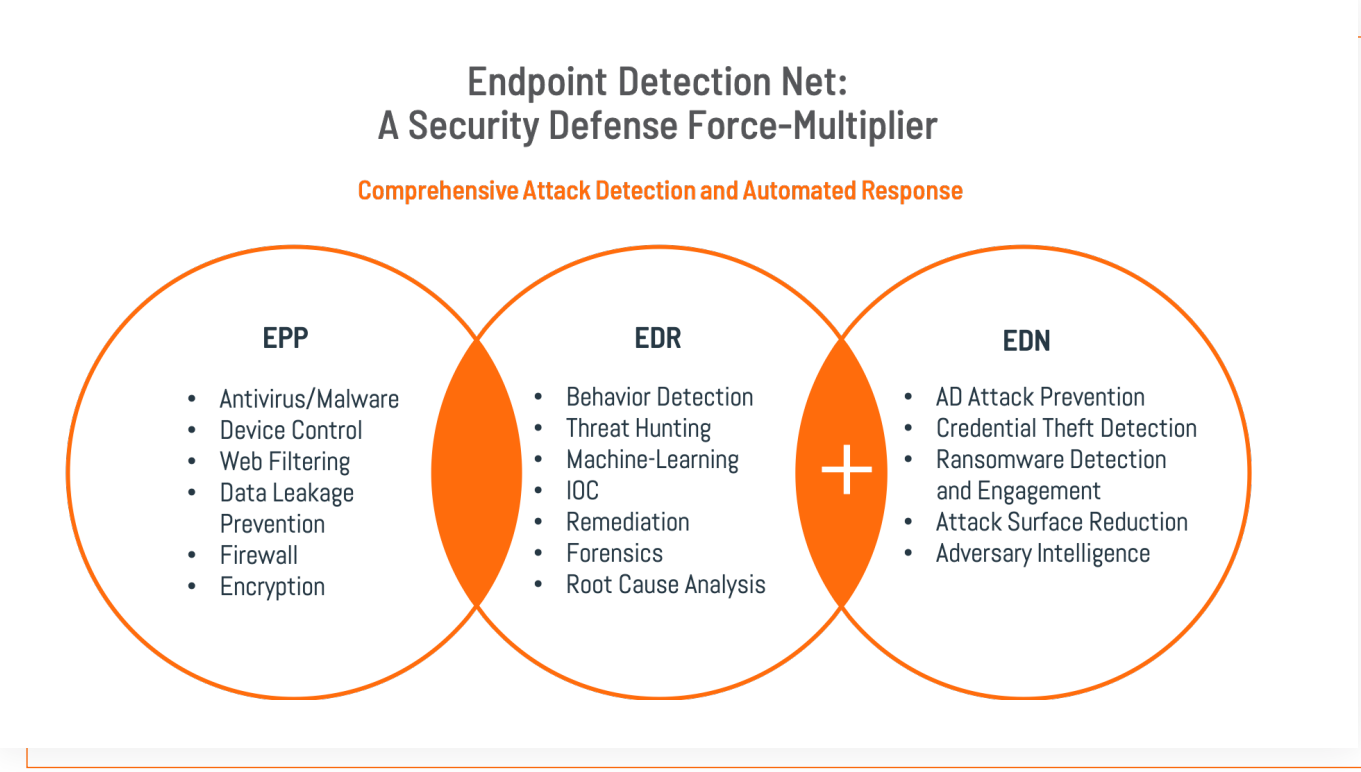
The next line of defense is Endpoint Detection and Response (EDR) solutions. Advanced EDR can look at processes, process flows, and process chains to see if something looks unusual—for instance if a process is spawning another process or invoking an API that doesn't seem right. This type of observation can also be helpful after an attack. As InfoSec teams investigate an incident and attempt to piece together what happened, EDR can supply the process flows that it mapped during the attack. Like EPP, EDR, while effective, does not stop everything—it will likely derail most but not all attacks, significantly boosting a system's ability to detect a wider variety of malware and ransomware attacks.

If the malware/ransomware manages to evade EPP/EDR solutions, the ability to engage in deception-based detection within the network becomes critical. Advanced deception technology quickly detects multiple forms of lateral movement. It includes the ability to hide production shares, redirect the ransomware to deceptive file shares, and occupy the attack by feeding it false data. Upon engagement, the decoy environment triggers an alarm, allowing defenders to isolate the program manually or automatically, halting the attack from spreading further. Together, cyber deception and EPP/EDR technology create a comprehensive defense for quickly identifying and isolating malware/ransomware while providing critical telemetry for incident response and investigation.

ATTIVO SECURITY TIP

Attivo has risk reduction offerings for all three of these endpoint security priorities. The Attivo Endpoint Detection Net (EDN) family of products contains several solutions that enhance EPP/EDR controls to strengthen security at the endpoint. The EDN solution adds stolen credential visibility by creating fake credentials stored on endpoint systems. It also protects against mapped share traversal by created and mapping hidden shares that point to decoy file servers. If attackers follow these shares, they engage with decoy file shares that alert on access. The suite provides additional ransomware protection by engaging the malware with high-interaction deception to slow down its spread while alerting on the activity. The EDN or standalone ADSecure solutions both add Active Directory reconnaissance protection to identify unauthorized AD access. As attackers query AD to identify critical accounts and servers to target, the solution returns false results that lead the attack to decoys for engagement. Additionally, the ThreatDefend platform contains native integrations with many popular EDR solutions to provide quick detection coupled with automated or manual response actions, such as isolating an infected system for rapid containment.

The Attivo EDN suite has endpoint functions that work with EPP/EDR solutions to protect the remote worker and network functions that detect malicious activity and cover the VPN infrastructure. The solution enhances existing security controls with visibility and detection to close gaps, plus native integrations with endpoint controls like CrowdStrike, McAfee, CarbonBlack/VMware, and Tanium to accelerate incident response.



EXAMPLES OF HOW THE EDN SUITE WORKS

Solution 1) With the Attivo EDN suite on an endpoint, organizations can detect when an attacker attempts to extract information from the AD controllers through a VPN-connected home system. It can also identify attempts to steal and reuse credentials on a VPN-connected system by creating fake credentials that point to decoys. These decoy systems can be in the cloud, on the VPN segment, or in the internal enterprise network.

Solution 2) Engagement decoys offer network services such as file shares that the home system can connect to and access once they are on the VPN connection. These decoy shares can detect and slow down ransomware infections that attempt to spread to network shares but stay hidden from the legitimate user.

5. NETWORK LATERAL MOVEMENT, EAST-WEST THREAT DETECTION

Organizations use traditional perimeter security controls like firewalls to prevent malicious north-south traffic from entering the network. The growth of VPN users comes with the need for more firewalls and other gateway appliances, but once a user connects to the VPN, it becomes east-west traffic. With more network traffic coming from the VPN segment to the rest of the internal infrastructure, it is even more challenging to identify malicious traffic. Organizations need a way to detect suspicious east-west traffic indicative of lateral movement, both in on-premises networks as well as through remote access. One way to protect against such lateral movement is to adopt a zero-trust architecture. However, this involves more than just deploying a single solution. It is a long-term initiative that requires significant time and planning. Zero-trust architectures assume that nothing inside the network is implicitly trusted, and every service, application, user, object, or entity must verify every attempt to access the network from outside or inside. To get to zero-trust, one must apply the right controls like network segmentation, Identity and Access Management (AM), application control firewalls, appropriate policies, etc. With long-term projects on hold for many companies, zero-trust is not something one can quickly implement. As such, organizations are looking to modify or adapt other existing security controls to reduce their risk.

As part of their baseline security controls, organizations typically deploy Intrusion Detection/Prevention Systems (IDPS) to identify and block unusual traffic. While common at the perimeter as a security control, IDPS usually do not deploy inside the network because the tuning required to avoid false positives can be challenging. However, if an IDPS is all that is available, an organization can deploy it internally as a stop-gap measure with the understanding that it will be prone to false positives. Network Traffic Analysis (NTA) tools are another potential solution to handle internal visibility. NTA tools aim to provide visibility into the entire network, from perimeter to the datacenter, core network, IoT, and SaaS environments by recording traffic and then analyzing it. It often uses machine learning to create a baseline of normal behavior within the network and then identifies anomalies that deviate from the baseline as security incidents. As such, NTA can work in a threat hunting capacity as well as a detection capacity, since analysts can look at the traffic packet captures for additional threats. These packet captures also provide IoCs and forensic evidence to help with investigations. A properly configured NTA tool may also cover Active Directory by identifying unusual traffic from a system to the AD controller.

PROTECTION FUNCTIONS

- signatureless detection
- east-west
- file-less
- zero-day

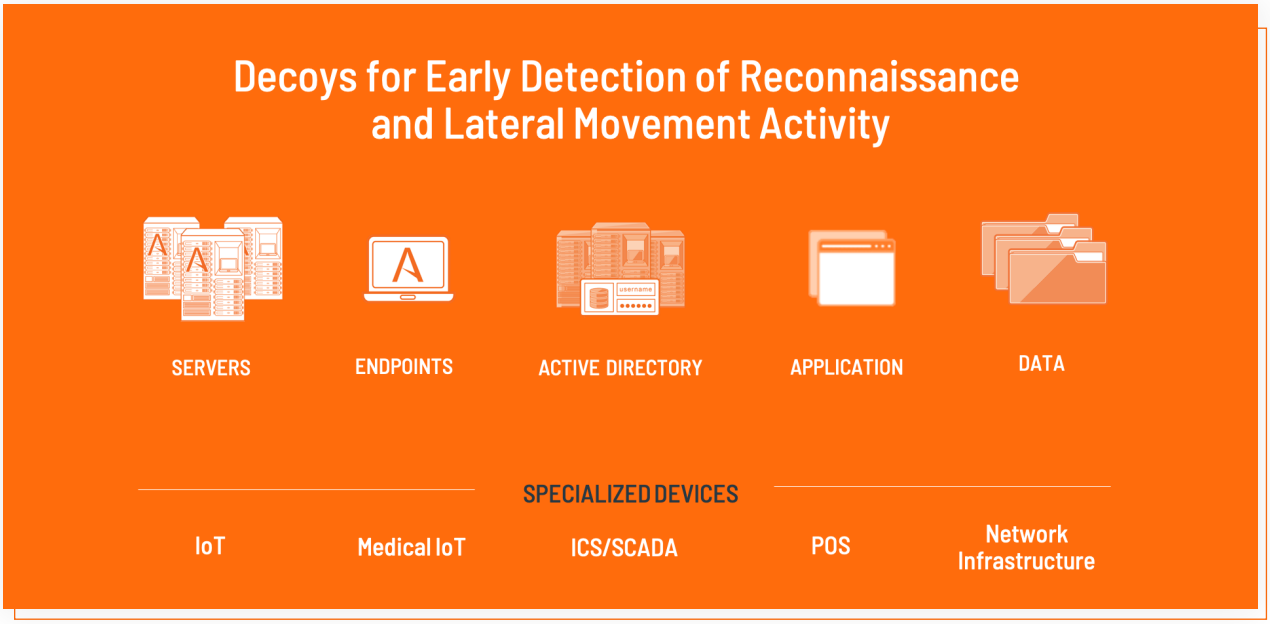
While IDPS and NTA are useful, they still leave gaps in coverage that attackers can exploit. IDPS and NTA do not detect network-based credential theft activities like Man-in-the-Middle (MitM) attacks. Because MitM is a passive activity specific to a network segment, NTA will not usually identify the traffic as unusual, and IDPS will not block or detect it. Furthermore, IDPS and NTA will not recognize, delay, or otherwise block ransomware spreading across the network to mapped shares. Once an attacker finds a way to bypass signature-based IDPS, there is nothing it can do. While NTA does attempt to identify the attacker by looking at abnormal traffic, the length of time it can look backward for investigations is limited to the amount of storage capacity the system has. For NTA to be effective, it must record all network traffic and then filter out what it considers background noise to save space while tagging the metadata for efficient search. Recording and storing all those packet captures and keeping them for any meaningful length of time for investigations takes a great deal of storage because of the sheer volume of traffic generated by even a small network.

With the increase in VPN use, IDPS and NTA controls can lose some effectiveness. While it is not unusual to deploy them in a VPN environment, IDPS still has issues dealing with internal traffic. NTA baselines no longer apply because all traffic now originates from the VPN subnet, so it becomes much harder for it to identify abnormal traffic.

ATTIVO SECURITY TIP

The Attivo ThreatDefend platform has extensive network security functions that enhance existing network perimeter security controls. Additionally, with the growth of VPN infrastructure, attackers are opportunistically targeting home users as a way to gain access to corporate networks and evade perimeter defenses. Deception acts as an early-warning system to identify such activity, so the security team can respond quickly to a compromise before the attacker has the opportunity to establish a foothold. The additional endpoint components for protecting remote workers, ease of deployment, and the ability to enhance and automate existing controls make the ThreatDefend platform a quick win.

As part of the ThreatDefend platform, the BOTsink deception server houses and deploys full OS network decoys that organizations can customize to look like any system or server in the network. By mirror-matching production systems and not merely relying on emulation, the decoys look like authentic production systems and blend into the environment. The decoy systems only communicate internally within the deception environment and remain hidden from normal network operations, so employees should not see or interact with them in any way during their regular business activities. Notably, because these deception systems offer no employee production value, any interaction is suspicious and should be viewed as malicious, a policy violation, or network configuration issue that needs addressing. The organization can deploy decoys to any network segment, including the VPN segment, to gain visibility to activities that an IDPS or NTA solution would consider background noise, such as excessive ARP broadcasts, network discovery activities, or MitM activity. Because these decoys are full OS virtual machines, they can hold any data, run any application, or offer any network services. They can fully interact with attackers as if they were real production systems, recording all network, memory, and disk activity with full forensic captures. Security teams can then use this information to develop threat intelligence to tune their IDPS further or hunt with NTA tools, gaining further benefit from the deception and using it as a force multiplier to improve their security.



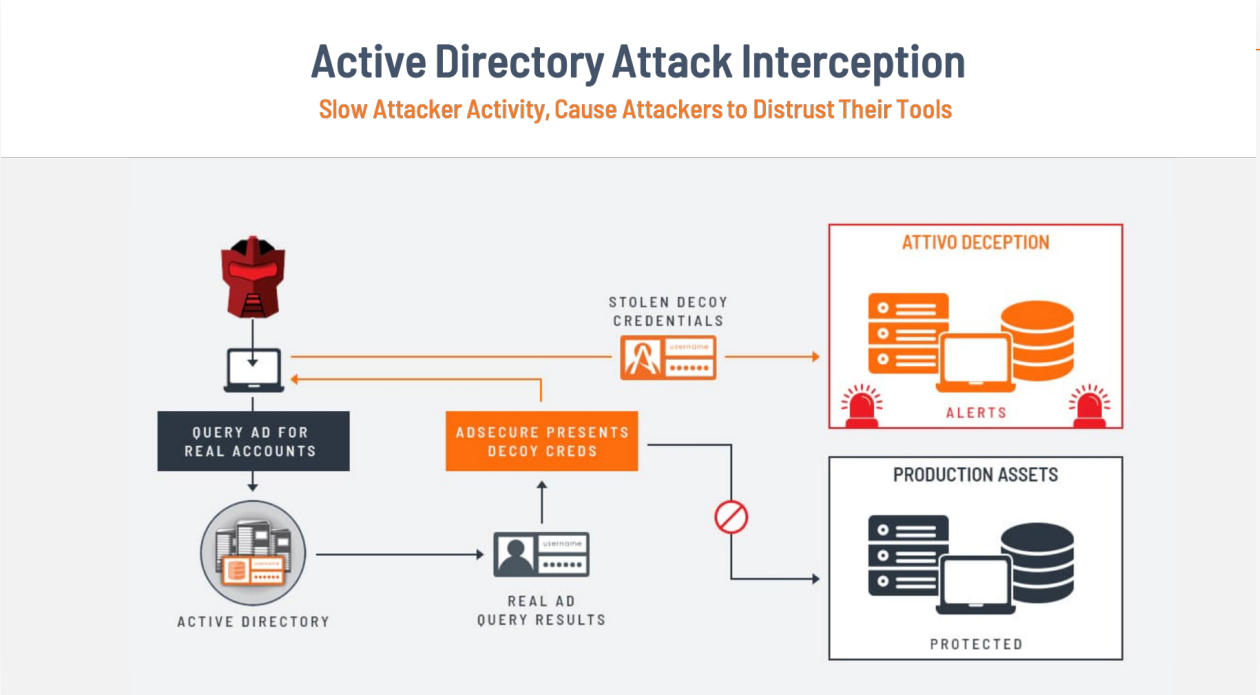
6. PRIVILEGED ACCESS MANAGEMENT

Many CISOs are now mandating multi-factor authentication (MFA) as employees migrate to working from home offices. While MFA is useful, attackers have ways to bypass it. They know that MFA works for interactive logins (where the user inputs an account name and password) but not against non-interactive resource access. For example, email clients and mapped shares are non-interactive services that need a separate password or hash the OS loads into memory to reconnect to servers on login. Attackers can steal these in-memory tokens with applications like Mimikatz and use them to gain access to the network. Windows systems also use an authentication mechanism called a Kerberos ticket to avoid storing passwords locally or transmitting them for authentication. This mechanism uses symmetric-key cryptography to grant and verify session-specific tokens for access. Every time a user logs in or tries to access a network resource, a Kerberos server provides authentication tokens that validate the user, the session, and the length of time the access is valid. While much more secure than just relying on sending passwords, Kerberos tickets can reside in memory for up to ten hours. Attackers can steal these Kerberos tickets and reuse them for access to the network resource.

ATTIVO SECURITY TIP

Attivo deception covers this gap in MFA with the Endpoint Detection Net (EDN) product family. The EDN family of products ambushes attackers at the endpoint with the ThreatStrike and ADSecure solutions. The ThreatStrike solution creates and stores fake credentials on user systems and servers, both in credential storage and within memory. These deceptive breadcrumbs include credentials, as well as decoy hashes, access tokens, and Kerberos tickets. When attackers steal the locally stored credentials using Mimikatz or a similar tool, they also take the fake credentials, which lead to decoys on the network. If they follow the credentials, they will engage with the decoys, which generates an alert while recording all of their activities for developing adversary intelligence.

The ADSecure solution detects and alerts on unauthorized AD queries from such tools as PowerShell, Bloodhound, or others. When the AD controller replies with the query results, the ADSecure solution replaces the critical accounts and objects with fake data that leads to the decoys. These AD objects include user accounts, groups, service accounts, or Service Principal Names to counter activities like Kerberoasting. The attacker will falsely believe they have successfully gained the information they are seeking, and all the while, when the attacker follows this data, they will land in the deception environment. This misinformation is not only effective for early detection but also in slowing attackers as they can longer trust their attack tools.



7. DATA LOSS TRACKING

Data Loss Prevention (DLP) is a security control designed to detect potential data breaches/data exfiltration transmissions. It prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest. Network DLP typically works at network egress points near the perimeter. It analyzes network traffic to detect outbound sensitive data in violation of information security policies, with multiple security control points reporting activity to a central management server for analysis. Endpoint DLP manages data at rest and limits data communications between groups to prevent attaching or sending sensitive information during communications such as email, instant messaging. For DLP to work correctly, the organization must classify data by sensitivity so the DLP solution can apply appropriate protections. Then it must be on all network egress points and endpoint systems for full coverage. A properly configured DLP solution takes a lot of effort to deploy across the organization and to classify all sensitive data accurately. Even with a properly configured DLP solution, it's still vulnerable to stolen credential attacks. An attacker who steals the correct credentials can bypass any DLP protections to access the sensitive data, and by encrypting it before transmission can avoid any exfiltration protection without the organization's knowledge that sensitive data left the network.

ATTIVO SECURITY TIP

Attivo offers several benefits that enhance existing data security controls. The ThreatDefend platform includes the DecoyDocs function to provide data loss tracking and visibility into data theft. The DecoyDocs function embeds a

beacon into a fake document that returns information on the host that opens it post-access, whether inside the network or outside. If opened internally, it shows full host information or, if externally, the Internet IP address. The ThreatDefend platform also includes full OS decoys that an organization can use to house decoy databases, file servers, or other services that hold data. It can also add security to on-premises and cloud storage and data functions. Altogether, these add visibility, detection, and alerting to bridge any coverage gaps with existing data security solutions.

8. SECURING CLOUD OPERATIONS

With many remote workers now operating externally, organizations are increasing their use of cloud, IaaS, and SaaS services. Whether for data storage, collaboration, remote applications, cloud computing, or other business functions, the ease of access makes these platforms ideal for remote work. However, this comes with its own set of security requirements since, while the cloud or platform provider secures the infrastructure, each organization is responsible for protecting its data in the cloud. It can pose a challenge when trying to secure cloud-resident information since in-network security tools may not scale or work in a cloud environment. Many organizations turn to cloud-specific security tools such as Cloud Access Security Brokers (CASB), Cloud Workload Protection Platforms (CWPP), and Cloud Security Posture Management (CSPM) for cloud protection.

A CASB solution is an on-premises or cloud-based software that sits between cloud service users and cloud applications. It monitors all activity to the cloud environment and enforces security policies. A CASB solution can offer a variety of services such as monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware.

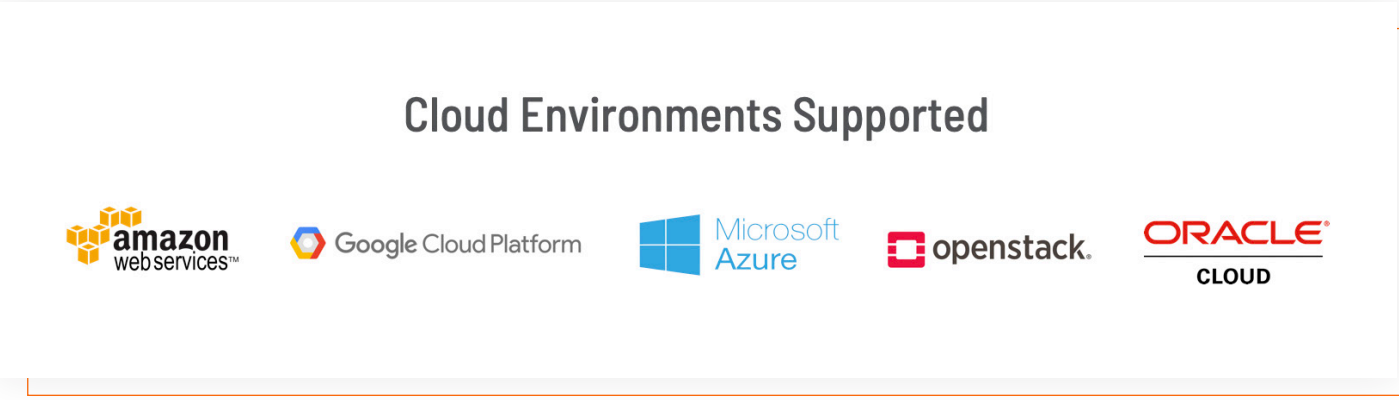
CWPP solutions manage and protect cloud workloads, primarily used to secure server workloads in public cloud Infrastructure as a Service (IaaS) environments. CWPP capabilities vary across vendor platforms but commonly include functions such as system hardening, vulnerability management, host-based segmentation, system integrity monitoring, and application whitelisting. CWPPs enable visibility and security control management across multiple public cloud environments from a single console.

CSPM solutions provide capabilities for organizations to correctly configure public cloud IaaS and PaaS services and address cloud risks. Primary uses cases include compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization. Because public cloud infrastructure is continually changing, CSPM security tools monitor enterprise cloud environments to identify gaps between their stated security policy and the actual security posture. At the heart of CSPM is the detection of cloud misconfiguration vulnerabilities that can lead to compliance violations and data breaches. CSPM offerings typically use APIs of the underlying cloud providers to monitor public cloud environments for security or policy violations with the option of remediating the violations to ensure continuous compliance.

While deploying all three types of solutions is an effective way to secure an organization's cloud environment, there are still some gaps that attackers can leverage to access data in cloud environments. For example, a stolen SaaS credential gives the attacker access to the environment even with a CASB solution in place. Attackers can leverage insecurely configured serverless computing functions to steal embedded access tokens. An attacker on a VPN user's system gains access to any IaaS cloud storage solutions from inside the organization. With access, the attacker can conduct network discovery to find other cloud workloads to target. With some organizations moving AD to the cloud, securing cloud resources becomes even more critical.

ATTIVO SECURITY TIP

The Attivo ThreatDefend platform offers deception that enhances these cloud security solutions. The Attivo BOTsink server deploys decoys, including full OS VM decoys for running decoy cloud workloads, storage buckets, containers, serverless functions, and other native cloud technologies. These decoys give visibility into the cloud environment for attack activity that attempts to conduct network discovery, move laterally, or exploit cloud resources. The EDN ThreatStrike solution creates fake credentials or API keys that lead to the cloud decoys and can embed these in both real and fake serverless functions. It can even create fake mapped shares on endpoints that point to cloud decoys. The EDN ThreatPath solution reduces the attack surface by identifying stored cloud credentials on endpoints for removal. The EDN and ADSecure standalone solutions protect AD in the cloud by returning fake AD objects to unauthorized attacker queries and the ability to lead the attacker into a decoy. Additionally, the DecoyDocs function alerts when an attacker accesses it from within the cloud or after exfiltration. These solutions provide a layered defense, add collective value, and enhance other CASB, CWPP, and CSPM coverage.



9. MAINTAINING COMPLIANCE AND ADHERENCE TO REGULATIONS

CISOs often face stringent data protection regulations, and despite dramatic shifts in operations must still prevent privacy invasions and combat increasing cyberattacks. Consequently, CISOs must not neglect the need for aligning their organizations' security structures with any new or incumbent regulations.

ATTIVO SECURITY TIP

The ThreatDefend platform is another tool that CISOs can use to show compliance with many regulatory requirements for data security. Several data security regulations mandate that organizations must show that they have actively responded to a breach and must have plans that show how they would do so. The ThreatDefend platform can play an active role in a compliance plan when embedded into an organization's security policies and used for early detection of and response to threats. The platform uses a deception fabric of realistic decoys, lures, and deceptive files and data designed to misdirect and derail attacks. The attackers waste time and effort chasing deceptions and tripping virtual mines that alert to their presence. Once the attacker engages, the platform records their movements and gathers the threat and adversary intelligence required to substantiate the attack and record the information for compliance and forensic reporting. The extensive third-party integrations make for a fast and efficient incident response to an attack, demonstrating that the organization has taken effective corrective action to respond to the breach. These functions give organizations a means to show that their compliance plans have protections around critical data, can record attacker activities, and are responding quickly and effectively to breaches. The platform also has features that enable compliance with regulatory requirements for data-across-borders and data localization. These include the ability to anonymize or prevent the collection of identifiable data and ensuring it stays in-country.

SOME FINAL OBSERVATIONS

1. These are stressful times, and cooperation between security and IT/network is critical for maintaining uninterrupted operations, quickly rolling out new services, and keeping risk low.
2. CISOs will need to be prudent in their investments. However, they must still find ways to reduce gaps and risk by activating features on their existing solutions and by giving priority investment to new technologies that complement their current security stack. Ideally, their solutions of choice will integrate for improved efficiencies, automation, and faster response.
3. CISOs will need to remain diligent in their training and regular communications to remind employees to operate safely and update their software frequently. They will also need to work closely with HR and supplier management to manage employee transitions for removing credential access and the risk of data theft.
4. Data security remains a big issue and calls for increased end-user and supplier monitoring and data loss prevention and tracking.
5. CISOs are asking trusted vendors for help. They are discovering security product capabilities that they have, and in some cases, are finding free features and services they were unaware of or underutilizing. In other cases, they are quickly seeing the gaps and are finding new complementary solutions that help close them or complete the offerings they already have. Many will also include automation that will come with the upside of speed to deploy and operational efficiency.

CISOs face new security challenges every year, each with their unique requirements for keeping pace with the constant evolutions of the high-tech world we operate in now. Attivo Networks can help with the challenges of today as well as how to scale where the attack surface is continually evolving, and threats are getting progressively more aggressive and destructive.

We welcome you to schedule a briefing with one of our security experts so that we can help you address critical security challenges while reducing risk and operation costs.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com