DECEMBER 2021

ARMOR

WHITE PAPER

THE MSP GUIDE TO SECURING ANY CLOUD ENVIRONMENT

INTRODUCTION

Most organizations are already past the initial stages of a cloud adoption strategy. Of all the organizations surveyed in Flexera's 2021 State of the Cloud Report, 91% said they already have a multi-cloud strategy, 82% said they already have a hybrid-cloud strategy, and 90% said they are expecting cloud usage to exceed previous plans due to COVID-19.[1]

While the prospect of having more productivity, innovation, and flexibility is driving many businesses to the cloud, the increased usage and complexity in cloud environments is exposing them to greater risks. In addition to the threats from deliberate cyberattacks, there are also risks due to misconfigurations.

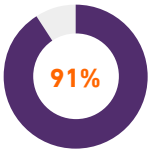
Businesses lack in-house resources to mitigate these risks. Fortunately, they're well aware of it. That's why 83% of decision-makers with in-house security teams plan on outsourcing security tasks to an MSP by the close of 2021.[2]

No doubt, MSPs, especially those serving healthcare/healthcare tech, financial services/banking/fintech, retail/ecommerce, and other compliance-centric industries, are standing in front of a tremendous opportunity just waiting to be tapped.

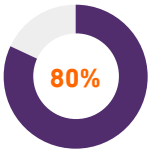
The question is: How can MSPs with limited cybersecurity talent and tools take advantage of this opportunity and protect their customers' assets stored or deployed in various clouds?

Your best option is to use a cloud workload protection platform (CWPP). Ideally, a single CWPP could defend multiple private, public, and hybrid cloud environments against even the most sophisticated threats while mitigating accidental risk in various public clouds. With help from the right CWPP vendor, you can leverage the advanced capabilities of a CWPP to provide simultaneous defense-in-depth security to all your customers' cloud workloads, regardless of size, location, and cloud service provider.

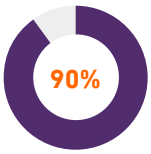
STATE OF CLOUD



of organizations already have a multi-cloud strategy



of organizations already have a hybrid-cloud strategy



of organizations are expecting cloud usage to exceed plans due to COVID-19

WHAT SECURITY SAFEGUARDS CAN A COMPREHENSIVE CWPP DELIVER?

A comprehensive CWPP can have all the tools needed to detect vulnerabilities, thwart attacks, and ensure regulatory compliance in your customers' cloud workloads. At a minimum, a robust CWPP should be able to deliver the following security safeguards:

INTRUSION DETECTION/INTRUSION PREVENTION

Your customers' cloud environments can have hundreds or even thousands of active connections on any given day. Some may be involved in automated B2B transactions with trading partner servers. Others may be supporting end users interfacing with cloud-based applications. These, along with several other open ports in your customers' cloud environments, provide an expansive attack surface that threat actors can exploit through the internet.

One way to protect your customers' cloud environments from network-based threats is by using an intrusion detection/intrusion prevention system (IDS/IPS). A capable CWPP would have an IDS/IPS that can monitor inbound and outbound network or host traffic for malicious activity, and then prevent detected threats from passing through. An IDS/IPS generates security telemetry that is used for protection as well as visibility.

FILE INTEGRITY MONITORING

One leading indicator of compromise (IOC) is unauthorized changes (e.g., updates, deletions, and writes) to critical system files. A file integrity monitoring (FIM) system can detect these changes and send out alerts or update a status indicator on a dashboard to warn security analysts of potential threats.

When used in concert with other security safeguards in a CWPP, a FIM can provide an additional layer of detection in case a threat manages to evade other defenses. For example, if an attacker is somehow able to evade your CWPP's IDS/IPS and infiltrates one of your customers' servers, they will usually attempt to make changes to system and configuration files. A FIM can detect those attempts and warn you through alerts.

MALWARE PROTECTION

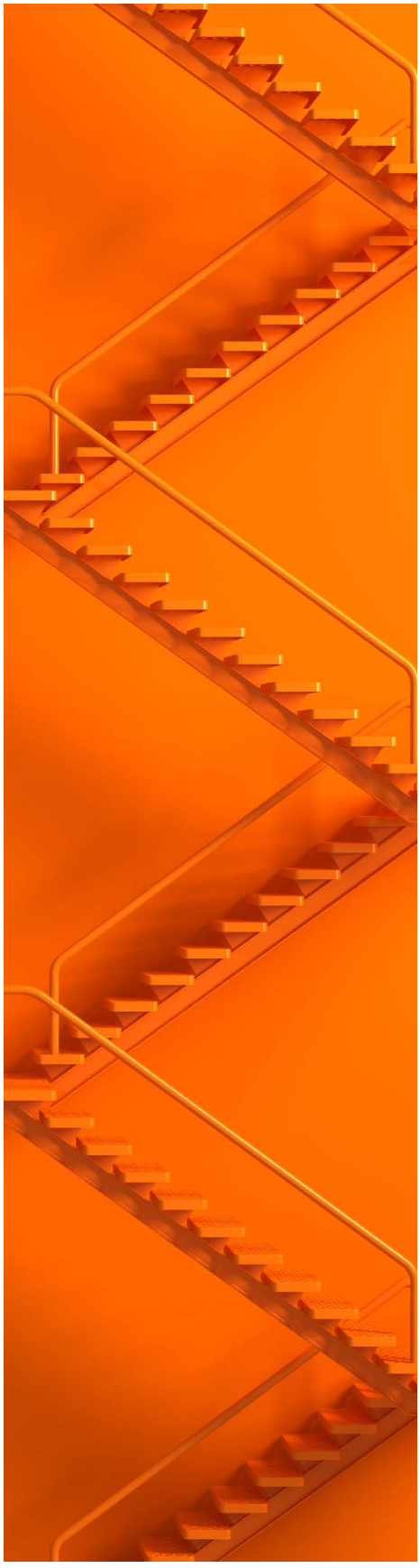
Malware outbreaks can degrade workload performance, cause data loss, or, in the case of ransomware, cripple entire networks. Sometimes, malware infections even serve as precursors or diversions for a larger cyberattack.

To prevent malware-induced disruptions in your customers' cloud environments, a CWPP should be capable of protecting against malware infections as well as generating logs that you or a security expert can use for deeper analysis.

VULNERABILITY SCANNING

System and application vulnerabilities are often exploited by threat actors as entry points into your customers' cloud environments. Vulnerability scans can pinpoint these vulnerabilities before attackers can get to them. These scans also come in handy during a customer's compliance audit. Assuming the scan results are favorable, you can furnish your customer with a copy of the vulnerability report, which they can then submit to auditors as part of compliance evidence.

Some CWPPs can also scan container images—a must-have for your customers with DevOps (software development and IT operations) teams that develop applications using containers. This enables you to detect and inform customers of vulnerabilities in their container images so they can remediate the issues early in their software development lifecycles.



WHAT DOES A CWPP OFFER TO SUPPLEMENT IN-HOUSE RESOURCES?

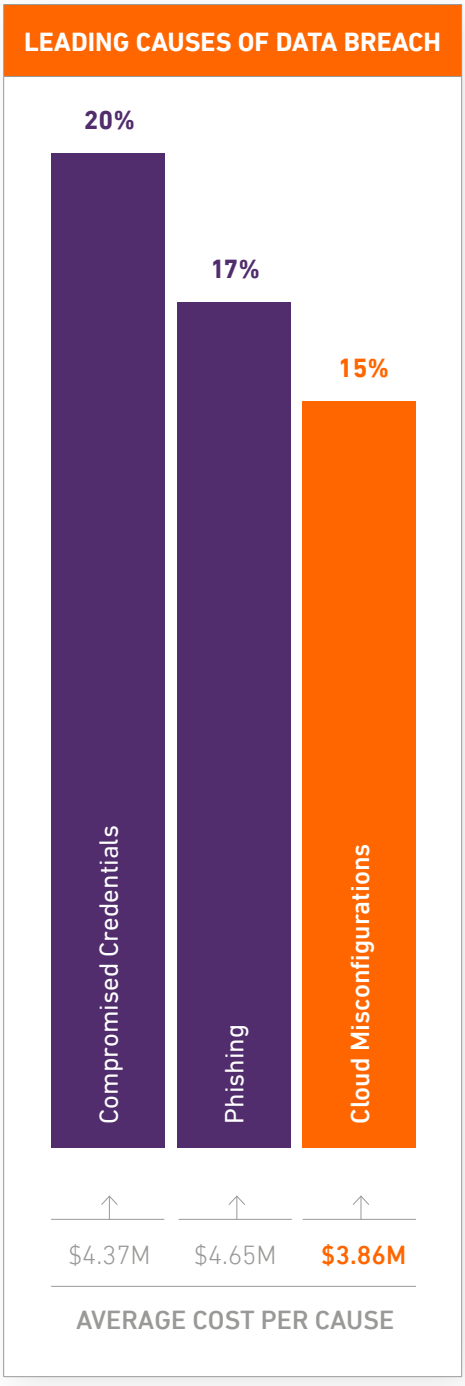
Cloud misconfigurations are among the leading causes of a data breach. In the 2021 edition of IBM's Cost of a Data Breach Report, cloud misconfiguration ranks third among the most common initial attack vectors and is responsible for 15% of data breaches.[3]

Whenever company data can be easily shared to the whole world through an accidentally misconfigured cloud setting (e.g., leaving a cloud server's access setting public), threat actors don't have to do much to get what they want. With cloud management consoles getting ever more user-friendly, a data breach can be just a simple toggle away.

In small, 10-to-20-person organizations, where the most tech-savvy person is usually the designated all-around, one-man IT team, accidental data breaches are bound to happen. Ad hoc IT personnel often lack the training and mindset to follow strict security practices. All they're focused on is getting the job done—and it usually doesn't involve security.

Small and medium-sized businesses that hire MSPs to take over cybersecurity and cloud administration duties can minimize the risk of these accidental data breaches.

However, when you take into account the complexity of each cloud environment MSPs need to protect against both intentional and accidental threats, the task can be pretty daunting—especially for small and medium-sized providers. MSPs need to supplement in-house resources to overcome deficiencies in their cloud security ventures. With the help of a CWPP, you can be well-equipped to fill that need.



SPECIALIZED CYBERSECURITY DISCIPLINES, INCLUDING THREAT DETECTION AND RESPONSE

In order for businesses to improve their overall cloud security against intentional and accidental threats, they have to find people with the right skill set. Unfortunately, the skills gap that has plagued the cybersecurity space and has prevented businesses from filling badly needed positions for years continues to persist.[4]

An MSP armed with a CWPP can fill that gap. With the help of a CWPP, an MSP can infuse their customers' cloud environments with basic as well as specialized cloud security disciplines, including threat detection and response. Threat detection and response is crucial in bringing down dwell time or the duration a threat actor enjoys unfettered access in a customer's cloud until completely removed.

By leveraging alerts generated by a CWPP's security safeguards, an MSP can quickly identify and respond to threats before bad actors can take a foothold or infiltrate other components of the cloud environment.

EDUCATION AND DISSEMINATION OF THREAT INTELLIGENCE TO MITIGATE THREATS

Sun Tzu once said: "If you know the enemy and know yourself, you need not fear the result of a hundred battles." This also applies to cybersecurity. A CWPP can help you understand the tactics, techniques, and procedures used by threat actors, which in turn can help you educate your customers so they can make smarter decisions. The result is you can show value to your customers while helping them better protect their business against cyberthreats.

At the same time, you can use threat information to build more appropriate defenses for your customers, taking a preemptive approach to protecting their environments from compromise. Proactive security measures such as threat intelligence can help in that regard. Threat intelligence, in particular, enables informed, data-driven decision-making, resulting in more effective and efficient defenses.

A CWPP can help you correlate threat intelligence feeds with CWPP alerts and log data of suspicious events from your customers' applications, VMs, hosts, and other cloud workloads. The combination of all this enriched data will allow you to obtain insights for defense building as well as for education and information dissemination.

> **If you know your enemy and know yourself, you need not to fear the result of a hundred battles.**
>
> — Sun Tzu

24/7/365 MONITORING AND PROTECTION

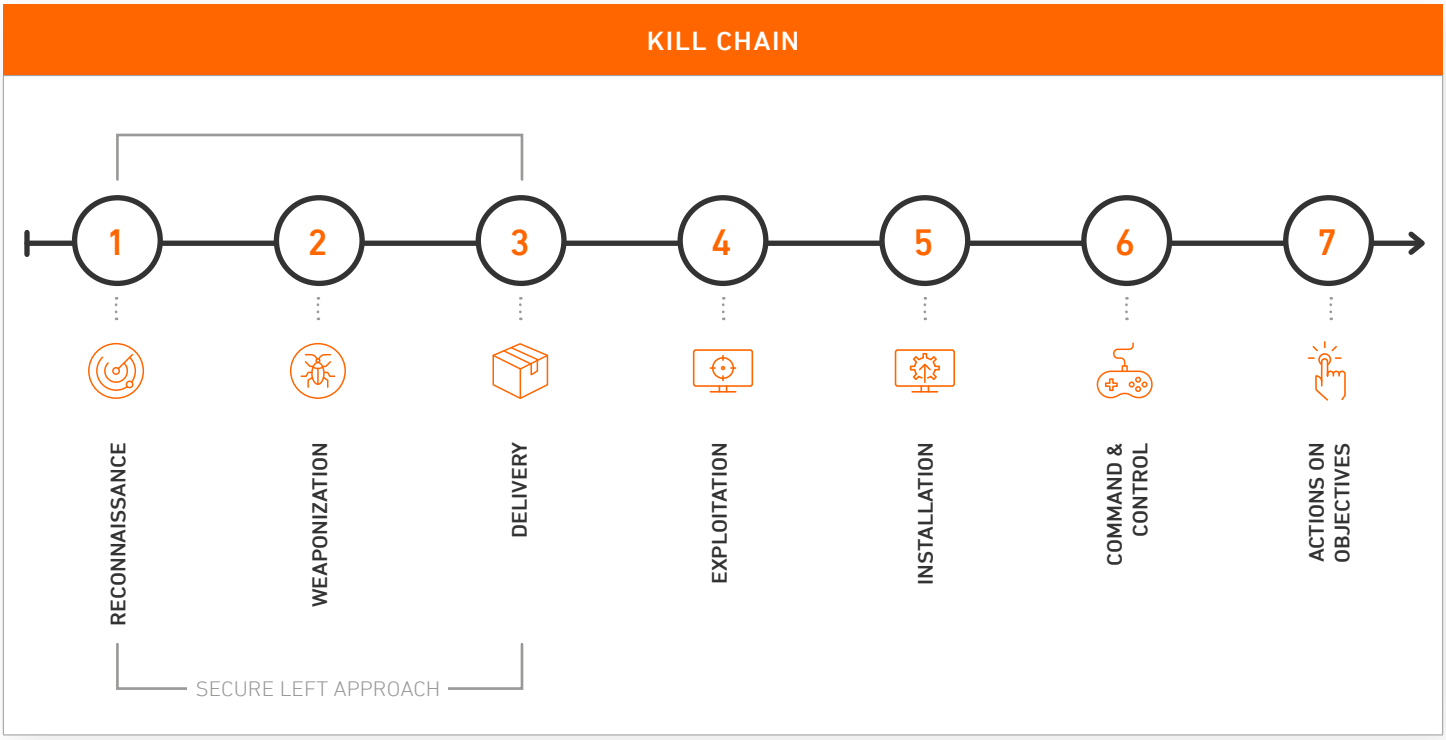
Small and mid-sized businesses seldom have IT staff working overnight and weekend shifts. This gives threat actors several windows of opportunity to carry out attacks with no fear of being identified.

While MSPs can provide coverage during those times, most MSPs have less than 10 employees, who already are often tasked with managing up to 15,000 endpoints.[5] With so little manpower and a vast attack surface to secure, MSPs can't possibly provide effective 24/7 monitoring and protection day in and day out.

By leveraging a CWPP's ability to provide visibility, control, and protection to many types of cloud workloads, regardless of size and location, MSPs can streamline and simplify much of their security processes. This would make providing 24/7/365 security coverage on customer workloads more doable.

REAL-TIME RESPONSE AND GUIDANCE TO ADDRESS NETWORK INTRUSIONS

According to the Cost of a Data Breach Report, it can take up to 329 days to identify and contain a cloud-based data breach. It doesn't have to be that long. As implied in the classic cyber kill chain, attackers pay a visit to the victim's infrastructure several times throughout the duration of a cyberattack, from the "reconnaissance" stage all the way to the "actions on objectives" stage.



Any one of these multiple intrusions should be detectable and addressable with the right tools. The best CWPPs can generate alerts from log data in real time, as well as provide appropriate remediation guidance. With that visibility, you can offer instantaneous response to potential network intrusions in your customers' workloads, reduce the chances of an attacker finding and exploiting any vulnerabilities in those workloads, and eliminate threats early in the kill chain.

WHAT CAPABILITIES DOES A COMPREHENSIVE CWPP DELIVER?

A CWPP shouldn't simply be all about security safeguards—although they should certainly be a big part of it. Rather, in addition to those safeguards, it must also deliver capabilities that can greatly simplify your role as a cybersecurity provider for various organizations, especially those operating in data privacy/protection-sensitive industries or jurisdictions.

SEAMLESS INTEGRATION OF BEST-OF-BREED TOOLS, PLATFORM, AND EXPERTISE

In building defenses for your customers' cloud environments, one option would be to buy point solutions that address specific use cases. You may acquire a vulnerability scanner, an IDS/IPS, a FIM, a malware protection solution, and so on, depending on the use case that needs to be addressed. There are, however, several issues with this approach.

First, it means you have to deal with multiple vendors. Second, for each point solution, you will have to carry out installations across all your customers' environments. Installing and tuning every solution (each with its own bundle of intricacies) on every single cloud environment (whether public, private, or hybrid), can be time-consuming and complicated.

Having disparate tools can also be an obstacle should you need to pull those tools together for event correlation or security automation/orchestration—an absolute necessity if you wish to eliminate a lot of your false positives and streamline your threat detection/response processes.

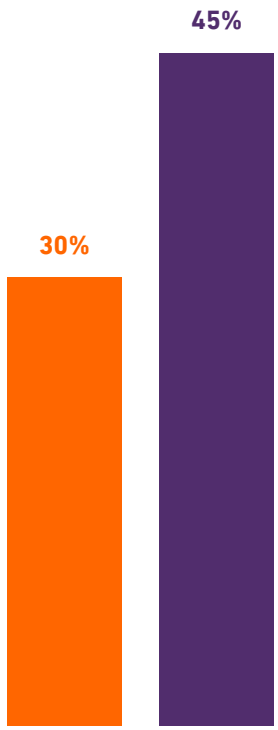
IBM's Cyber Resilient Organization Report 2020 revealed that nearly 30% of organizations surveyed use more than 50 distinct security solutions and technologies.[5] The problem is, too many point solutions in a security stack results in alert and screen fatigue, which can degrade a security analyst's ability to identify and respond to threats.[6]

A better option would be to use a robust CWPP. Since it's just one product, you only have to deal with one vendor. Secondly, a well-designed CWPP would already have best-of-breed security tools right out of the box.

That means, regardless of the use case or number of use cases, you normally only have to install a component of the CWPP—instead of a component of each tool—on your customers' environments. More importantly, because all tools run on top of the same platform, they can be easily integrated for event correlation and automation/orchestration purposes.

By combining your cybersecurity expertise with a CWPP, you can be more efficient and effective in securing your customers' cloud environments.

SECURITY SOLUTIONS & TECHNOLOGY USE



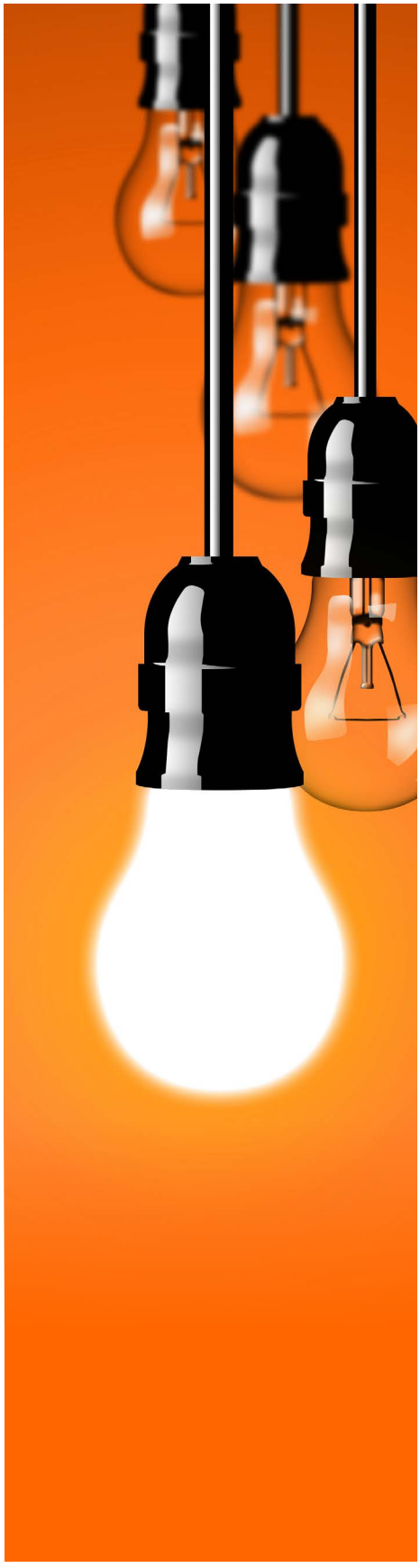
Nearly 30% of organizations use more than 50 separate security solutions and technologies, and 45% use more than 20 tools when specifically investigating and responding to a cybersecurity incident.

SECURITY AND MULTI-TENANT MANAGEMENT IN A SINGLE PORTAL

For most businesses, a basic CWPP should already meet most if not all cloud security needs. But for MSPs, it's a different story. MSPs not only have to configure and monitor a number of security tools, but also have to attend to multiple cloud environments that belong to different customers. These environments may have to be treated separately.

For this reason, MSPs should be looking for a CWPP that supports multi-tenant scenarios. A multi-tenant-capable CWPP will enable you to manage all your customers' cloud workloads in a simplified, cost-efficient, and highly scalable manner using a single platform while preserving logical separation between customers.

If you can find a CWPP that consolidates all administrative functions for all security solutions and all customer cloud environments in a single portal, that would be ideal. A CWPP with unified view and control capabilities that spans multiple workloads, IT assets, cloud deployments, and customers, can greatly simplify management, eliminate fatigue, and improve incident response.



STREAMLINED COMPLIANCE

The shared responsibility models of large public cloud providers such as AWS, Azure, and GCP, reduce the scope of an MSP's responsibilities in helping customers meet compliance mandates. For instance, the MSP is no longer responsible for securing the underlying compute, storage, and networking hardware. However, due to the complexity of today's cloud environments, mostly being hybrid deployments, it can still be extremely challenging for MSPs to help customers meet regulatory requirements.

To keep compliance-related obligations under control, MSPs must choose a CWPP with an infrastructure that readily adheres to major compliance frameworks such as CMMC, HIPAA, PCI DSS, ISO 2001, and HITRUST. If possible, the platform should also be capable of clearly mapping controls with specific compliance frameworks, as this would make it easy for you to generate reports that your customers can use as compliance evidence in their audits.

By choosing the right CWPP, you can significantly reduce the time and effort you and your customers need to put into compliance-related activities.

WHAT ADVANTAGES DOES ARMOR PROVIDE FOR MSPs?

Armor Anywhere is Armor's enterprise-grade cloud security and compliance platform. It's not just a CWPP. Armor Anywhere is more of a CWPP on steroids, combining cloud workload protection with cloud security posture management (CSPM), endpoint detection and response (EDR), and log and data management. For MSPs, getting all that in a single platform can be a game changer. Still, that's just one of the many advantages Armor delivers. There's more.

STREAMLINED MANAGEMENT, REDUCED COMPLEXITY

As a platform, Armor Anywhere streamlines management, reduces complexity, and eliminates fatigue caused by false positives. It provides MSPs with unified visibility and control over customer workloads and assets through a "single pane of glass"—the Armor Management Portal (AMP). Through AMP, MSPs can view a variety of security metrics, including health status, vulnerabilities, security incidents, potential threats, activities on hosts, and so on.

From that same interface, MSPs can also perform a range of operations such as adding or removing resources, changing configurations, accessing support options, turning up or turning down security and compliance controls, and more.

The value of this unified view and control is further magnified by Armor Anywhere's built-in multi-tenant capabilities, which make it considerably easier for MSPs to manage multiple customers, regardless of size, location, and environment.

FLEXIBLE PRICING AND DEPLOYMENT OPTIONS

One of the top benefits of cloud computing is its ability to eliminate capital expenses. Organizations that use cloud services no longer have to pay upfront costs for physical infrastructure and equipment, as these are already handled by the cloud service provider.

Instead, organizations are allowed to take advantage of flexible pricing models that scale with their business. A pricing model that allows businesses to start on smaller, more affordable terms as well as adjust to growing and shrinking demands enables healthier cash flows.

Armor Anywhere's pricing, which is based on the number of endpoints (i.e., cloud workloads, laptops, desktops, servers, etc.) provides that level of flexibility. You can start small by enrolling as few endpoints as you want or need, and then ramp up spending as your need and capacity increase.

Pricing isn't the only area where Armor offers maximum pliability. Armor Anywhere also features deployment flexibility with multiple deployment options. The Armor Anywhere agent can be deployed on all major server operating systems, including Windows Server, Red Hat Enterprise Linux, Ubuntu, Amazon Linux, Oracle Linux, and CentOS.

All this versatility makes it easier for you to service your customers' varied IT environments, meet growing customer demand for cloud capabilities, and address their corresponding security needs.

EMPOWER MSPs TO FULFILL SHARED SECURITY MODEL

The shared responsibility model adopted by public cloud providers delineates the responsibilities for cloud security between themselves (the providers) and their customers. Under this model, the provider is responsible for "security of the cloud," while the customer is responsible for "security in the cloud." When an MSP comes in on behalf of a customer, a large part of that customer's responsibilities are absorbed by the MSP.

Taking on the security responsibilities of a customer may be par for the course for any MSP willing to offer cloud services. However, it can be overwhelming when you have to deal with the responsibilities of multiple customers. Even keeping track of the cloud configurations of each customer and making sure they adhere to security standards can be quite a challenge.

Armor Anywhere alleviates this burden by:

1. Taking charge of securing several components under the customer's and MSP's domain.
2. Enabling the MSP to monitor and control security components in all its customers' cloud environments from a single pane of glass.

PARTNER-FOCUSED DELIVERY OF TOOLS, RESOURCES, AND EXPERTISE

We understand the value partners bring to our business. That's why a lot of what we do is geared toward making our partners' experience with Armor as seamless as possible. And it all starts with the tools, resources, and expertise we share with you.

TOOLS

To make it easy for MSPs to manage their customers on Armor Anywhere, we've incorporated several features and tools specifically designed for this purpose. This includes management tools for multi-tenancy (so you can onboard and manage new customers from a single location), licenses, billing, and customer support. This means, Armor Anywhere is the only place you need to go for customer management tasks, whether it's related to cybersecurity or business.

RESOURCES

We provide a wealth of resources to support your go-to-market strategies, boost outreach efforts, and enhance your mastery in cybersecurity and compliance. This includes:

- The partner portal – Here you'll find marketing assets that your business can easily modify to suit the needs of your prospects/target audience. We strengthen the reach of your go-to-market approach to help you win new business.
- Market Development Funds (MDF) – This fund is meant to give the boost you need to implement your outreach/marketing strategies.
- Go-to-market expertise – Our solution consultants and partner success managers will work directly with your team to develop a go-to-market strategy that fits your business needs—whether it's winning new business, adding services to your existing client base, or both.
- Technical resources – You'll have access to comprehensive training and support, including docs.armor.com, which provides all technical resources your team may need.

EXPERTISE

Our team of cloud, security, and compliance experts are here to give you best practice recommendations as well as provide guidance in CWPP implementation, deployment, and management; meeting audit requirements; and achieving regulatory compliance. Think of us as an extension of your team, ready to provide support to you and your end clients when needed.

CONSOLIDATING BEST-IN-BREED SECURITY TECHNOLOGIES AND A 24/7/365 SOC IN A SINGLE PLATFORM

Armor Anywhere consolidates the capabilities of an IDS/IPS, FIM, malware protection system, vulnerability scanner, log and data management system, and several other security solutions in a single platform. That same platform further integrates with a robust data lake, SIEM, and SOAR (security, orchestration, automation, and response) system for data enrichment.

This allows all these technologies to function as a cohesive unit with superior degrees of accuracy, precision, efficiency, and speed, thereby providing greater defense-in-depth security for your customers' workloads.

The efficacy of these technologies is augmented by Armor's 24/7/365 security operations center (SOC) team, which analyzes alerts and log data and responds to threats before they can escalate. Not only that, the team also apprises anti-virus vendors of newly discovered malware so that signatures can be created for them.

New and emerging threats are immediately incorporated into the platform's risk mitigation/detection modules. Thus, even if a threat is discovered in just one of your customers' workloads, all your customers benefit from the added protection.

OPERATIONAL WITHIN MINUTES AS OPPOSED TO DAYS/WEEKS/MONTHS

Armor Anywhere is a software-based solution. Indeed, there are security solutions out there that are hardware-centric. These are physical appliances that are usually stationed at the perimeter of a data center but can also be deployed within, especially when the organization using them has implemented some form of microsegmentation in the data center.

Although some of these appliances, e.g., next-generation firewalls (NGFWs), also feature multiple security safeguards such as IDS/IPS, malware protection, etc., one major downside of these solutions is that they take too much time to deploy. Because these are physical hardware, they need to be shipped, unpacked, and physically installed on a rack in a data center before they can be configured. Now, imagine doing this for multiple customers.

There's none of that with Armor Anywhere. There's nothing to ship, unpack, or physically install on a rack. As a result, you can start securing and monitoring your customers' workloads within minutes as opposed to days, weeks, or even months when working with physical appliances.

IMPROVED SCALABILITY AND ABILITY TO DO MORE WITH LESS

When you work with point solutions, onboarding or managing customers can be excessively complex, time-consuming, and costly. Every time you onboard a new customer, you have to go through the same labor-intensive processes of installing, configuring, tuning, and scripting every single security solution that the customer requires. And then if updates or any changes have to be made later on, you'll have to dive into every customer environment where those changes need to be applied.

Considering the limited in-house resources of small and medium-sized MSPs, these complexities can hinder scalability and business growth, as, at some point, adding a new customer would no longer be feasible from a management and profitability perspective. Having all necessary security safeguards in Armor Anywhere means you eliminate all the labor-intensive processes, as everything is done in one place.

When you onboard a new customer, the single most important process is simply to deploy the Armor Anywhere agent. The agent is lightweight and can be placed on any cloud, whether public, private, hybrid, or on-premises.

Once the agent is deployed, all security scans, alerts, and activity logs are automatically sent to AMP, where you can then view, analyze, and respond accordingly. Any updates, new services, configuration changes, etc., on Armor Anywhere, can be applied to all your customers across all of their Armor-managed cloud environments.

This paves the way for greater scalability, the ability to do more with less despite limited in-house resources, and, ultimately, a better capacity to support business growth.

STREAMLINED COMPLIANCE FOR STANDARDS INCLUDING HITRUST, HIPAA, PCI, AND GDPR

MSPs that add cloud cybersecurity services to their business aren't just entering the complex world of risk mitigation, threat detection, and incident response. They're also entering the onerous and often murky path of regulatory compliance. Since a single customer can be subject to multiple compliance standards, you need to make sure your customers' environments are compliant to each standard's set of regulatory requirements.

With Armor Anywhere, the specter of compliance is significantly diminished for three reasons. First, Armor Anywhere is already audit-ready. Its built-in security safeguards readily tick off key controls in major compliance standards, including PCI-DSS, HIPAA/HITECH, HITRUST, ISO 27001, GDPR, and others.

Second, Armor Anywhere already comes with cloud security posture management (CSPM) capabilities. A CSPM can automatically scan your customers' public cloud environments, assess those environments for adherence to major security and compliance frameworks, identify misconfigurations that violate those frameworks, and then provide step-by-step procedures to remediate the issues.

Through its CSPM features, Armor Anywhere can make it is easy for you to remediate any accidental risk caused by misconfigurations across all your customers' cloud environments. You can even leverage the reporting function of the CSPM module to provide instant, detailed, and verifiable evidence for your compliance auditors.

Last but not least, Armor's team of cybersecurity experts are ready to provide assistance in case you need additional help in your compliance endeavors.

THIRD-PARTY VALIDATION

Armor's outstanding reputation as a cybersecurity provider and MSP partner has gained recognition from various industry experts. Our most recent accomplishments in this area include the following:

- **GARTNER MARKET GUIDE FOR CLOUD WORKLOAD PROTECTION PLATFORMS (2021)**

Armor was identified as one of the few enterprises offering managed CWPP, which, as per Gartner, reduces the need to develop in-house skills.[7]

- **EMERGING TECHNOLOGIES: GROW YOUR SECURITY SERVICES PORTFOLIO WITH MANAGED DETECTION AND RESPONSE**

In June 2021, Armor was featured in a Gartner research paper titled: "Emerging Technologies: Grow Your Security Services Portfolio With Managed Detection and Response".[8]

- **EMERGING TECHNOLOGIES: ADOPTION GROWTH INSIGHTS FOR MANAGED DETECTION AND RESPONSE**

In August of the same year, Armor was once again featured in another Gartner research paper titled: "Emerging Technologies: Adoption Growth Insights for Managed Detection and Response".[9]

- **CRN PARTNER PROGRAM GUIDE (2020)**

In its 2020 Partner Program Guide, CRN, a brand of The Channel Company, awarded Armor a 5-star rating, a distinction given to organizations who offer the best partnering elements in their channel programs.

CONCLUSION

The cloud security market offers huge opportunities for MSPs. However, small and medium-sized MSPs with limited in-house cybersecurity talent and tools can be at a disadvantage, especially when pitted against larger, more established players in the market. One way to level the playing field is to leverage the capabilities of a comprehensive cloud workload protection platform, particularly Armor Anywhere.

Armor Anywhere helps small and medium-sized MSPs by:

- Augmenting existing cybersecurity expertise and technologies
- Providing the necessary security safeguards to mitigate intentional and accidental risks
- Reducing complexity in managing disparate tools
- Delivering partner-focused solutions
- Improving scalability and business growth; and
- Streamlining compliance

ABOUT ARMOR

Armor is a global cybersecurity company. We make cybersecurity and compliance simple, achievable, and manageable for managed service providers (MSPs) and their customers across endpoint, network, server, and cloud environments. Armor provides unparalleled insight into threats and helps our partners respond quickly and effectively. MSPs who use Armor benefit from an enterprise-grade security platform, cybersecurity expertise, and resources to help quickly scale their cybersecurity practice. Armor has partnered with leading MSPs to secure more than 1,500 customers in over 40 countries.

SOURCES

1. "Cloud Computing Trends: 2021 State of the Cloud Report," 2021
2. "Objectives and Challenges Driving IT in Today's Enterprise," 2021
3. "Cost of a Data Breach Report 2021," 2021
4. "The Cybersecurity Skills Gap Persists For The Fifth Year Running," 2021
5. "2020 MSP Benchmark Survey Results Report," 2020
6. "Cyber Resilient Organization Report," 2020
7. "What Is Cloud Computing? A Beginner's Guide"
8. "2021 Gartner Market Guide for Cloud Workload Protection Platforms," 2021
9. "Emerging Technologies: Grow Your Security Services Portfolio With Managed Detection and Response," 2021
10. "Emerging Technologies: Adoption Growth Insights for Managed Detection and Response," 2021

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167