MARCH 2020

ARMOR

WHITE PAPER

NAKED DATA: BENEFITS OF CSPM TOOLS

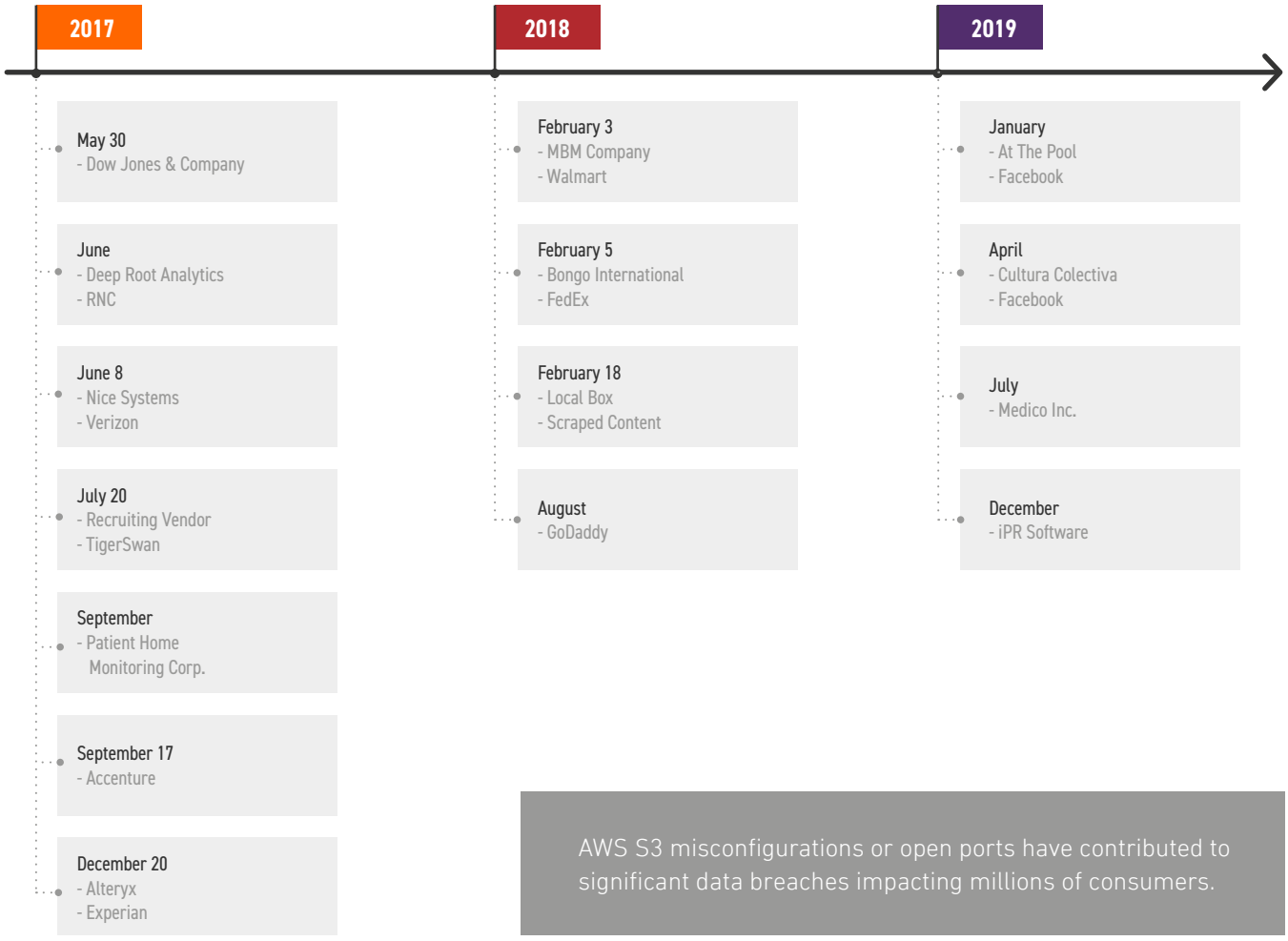
INTRODUCTION

A major credit bureau had millions of its records, which were stored in the cloud, exposed to the world as a result of a simple misconfiguration. This is one of many examples where organizations exposed millions of files including sensitive consumer data; voter registration and healthcare records; credit card information; and even application forms for military and government agencies. The news reports were disturbing as the exposures raised the specter of the cloud having no tolerance for even the most innocent of mistakes. "Misconfiguration" became the operative word.

Fast forward to today, and there is a pool of vendors wanting to sell you tools—conveniently referred to as cloud security posture management, or CSPM, tools—to identify misconfigurations in the cloud and help you avoid being another example of what can go wrong.

But what is the reality behind the headlines? What do these tools really do to address risk? Do you need these types of tools when operating in the cloud? Also, who in your organization can benefit from these tools?

CALENDAR OF UNFORTUNATE EVENTS



AWS S3 misconfigurations or open ports have contributed to significant data breaches impacting millions of consumers.

The major data exposures that took place at these organizations were extensively reported. Each of these organizations saw their data in the cloud directly or indirectly exposed. The number of stolen records was staggering to say the least. The incidents served as a wake-up call to others considering the cloud to host their applications and data: Be very careful, or else.

However, the news isn't all bad and the underlying cause, the misconfigurations, is solved more easily than one might think.

Here's the reality of the incidents mentioned before:

100%
Involved an unsecured S3 bucket in AWS.

920 MILLION +
Records were exposed publicly.

8
Involved data exposed by an affiliate, partner, or customer of a larger organization.

100%
Were announced to the media by either UpGuard (based in Mountain View, California) or Kromtech (based in Dubai, UAE) as a public service announcement and/or a positive press opportunity (for the organization).

The good news is that for most organizations, making sure your AWS S3 buckets are properly configured will ensure you avoid joining the list of victim organizations.

But, before you get too comfortable with the idea that misconfiguration risk is easily addressed and your exposure is unlikely, let's discuss the real value of CSPM solutions available today.

THE ACCIDENTAL & THE INTENTIONAL RISK

As organizations look to migrate applications and data to the cloud, they are realizing that many of their IT staff lack cloud security expertise. The cloud represents a fundamentally different approach to computing, and the security differences between the cloud and traditional on-premise infrastructures are night and day.

So, we've put together a simple way to think about the cloud as it relates to security against cyberthreats and misconfigurations, as well as other controls and settings that aren't correctly configured in the cloud—the accidental and the intentional.

THE ACCIDENTAL

These are the inadvertent and overlooked security and compliance settings, controls, and configurations that can potentially expose your applications and/or data to the public or to hackers.

Sure, exposure of millions of records, if you have them, would be a worst-case scenario and the most devastating to your business. However, this is also the most unlikely scenario now that you know not to mess with the default AWS settings for your S3 bucket, which limits public access to it. What is more likely, is that a misconfiguration or incorrect setting leads to your cloud footprint being incompliant with a major mandate which your organization is subject to, or settings allow a user to access your web application.

This is where CSPM vendors and tools have emerged to fill the gap and address accidental risk.

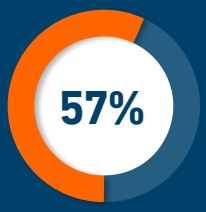
THE INTENTIONAL

The cloud is a target for threat actors. In fact, in a recent analysis conducted by Armor, there were 681 million cyberattacks against our 1,000+ client base. The most frequent types include attacks against known software vulnerabilities, brute-force attacks/attacks involving stolen credentials, web application attacks (e.g., SQL injection, cross site scripting, cross site request forgery attacks, and remote file inclusion), and attacks targeting the internet of things (IoT).

Armor's Threat Resistance Unit (TRU) expects more of the same in 2020 with additional emphasis on:

- IoT attacks and distributed denial of service (DDoS) campaigns
- Exploits and attacks targeting containers and cloud services
- Targeted ransomware
- Sophisticated phishing campaigns

BE AWARE



Of survey respondents were either "concerned or very concerned that in the next 12 months, misconfigured systems, such as server workloads and cloud services, could lead to a successful attack that [would threaten] their infrastructure, data assets, and business operations." Source: Oracle & KPMG.

Of cloud security failures, through 2022, will be the customer's fault. Source: Gartner.

Of enterprises, by 2021, "will unknowingly and mistakenly have some [infrastructure-as-a-service (IaaS)] storage services, network segments, applications, or APIs directly exposed to the public internet, up from 25% at YE18." Source: Gartner.

Of organizations, through 2024, "implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration." Source: Gartner.

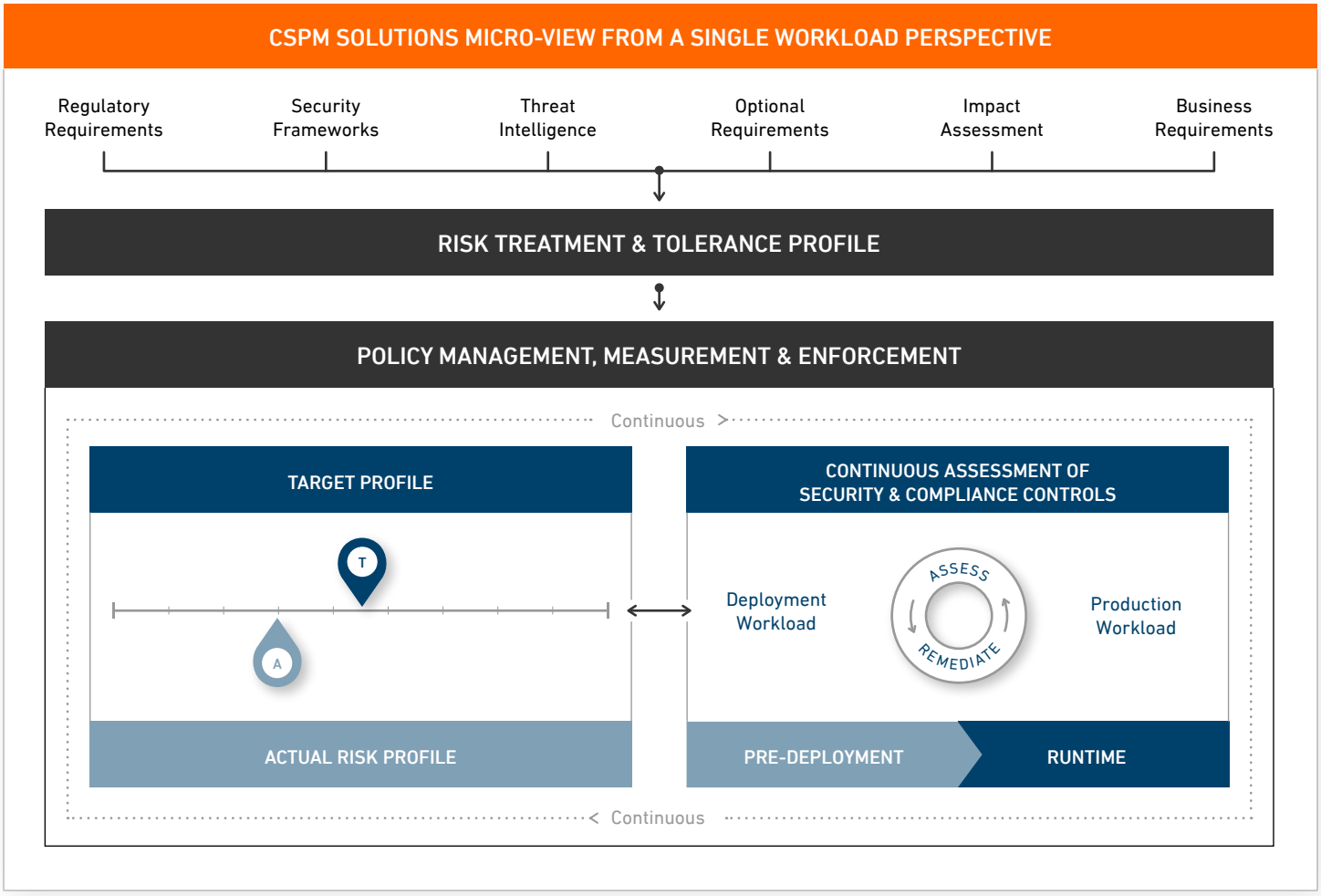
CLOUD SECURITY POSTURE MANAGEMENT

We've referred to vendors and tools when talking about CSPM. The fact is that, as vendors have emerged offering these solutions, we've seen their adoption and integration by other organizations. In the future, these will just be tools integrated with other solutions that address the intentional part of the cloud security and compliance problem.

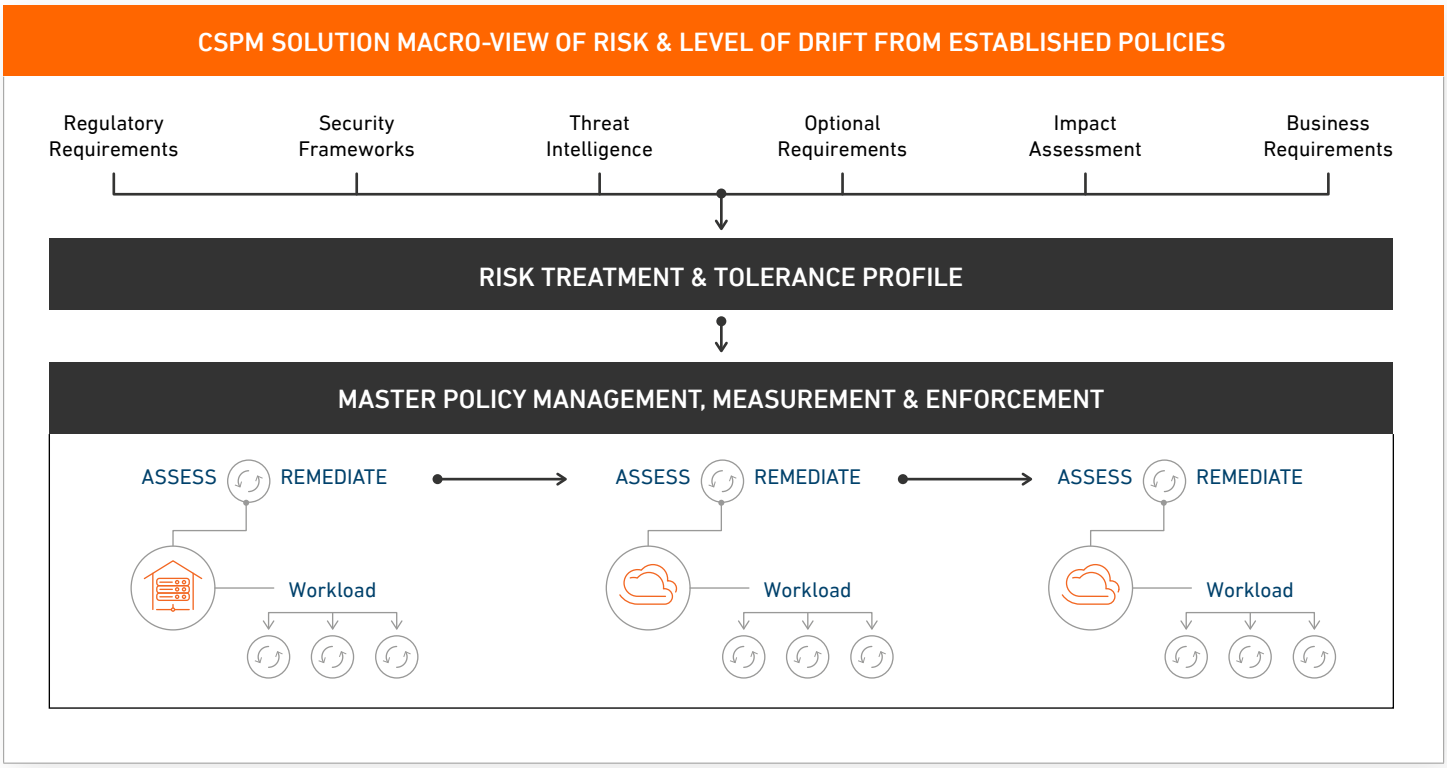
What Do Cloud Security Posture Management Solutions Do?

- Identify your cloud environment footprint and monitor for the creation of new instances or buckets (i.e., shadow IT).
- Provide policy visibility and ensure consistent enforcement across multiple cloud providers.
- Scan your compute instances for misconfigurations and improper settings that could leave them vulnerable to exploitation.
- Scan your storage buckets for misconfigurations that could make data accessible to the public.
- Audit for adherence to appropriate compliance mandates.
- Perform risk assessments vs. frameworks and external standards such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).
- Verify that operational activities are being performed as expected (e.g., key rotations).
- Automate remediation or remediate at the click of a button.

Typical CSPM services conduct these activities on a continuous basis and can include automation capabilities to correct issues without human intervention or delay.



Going beyond the micro view of a single workload, now consider how CSPM solutions can provide a macro view of risk and the level of drift from established policies.



What Do Cloud Security Posture Management Tools Find?

- Cloud configurations and settings that violate compliance requirements; instances of not following established account hygiene best practices (e.g., ensuring host operating system (OS) logs are being gathered, API event logging is turned on, and network flow logs are being collected, if applicable).
- Excessive account permissions. Highly empowered accounts, or accounts where permissions are granted but never used represent an increased attack surface. Developers often provision accounts and services with more permissions than necessary in the name of development speed and reducing runtime issues. However, this increases risk, which CSPM solutions identify.
- Accounts and services where multifactor or other strong authentication methods are not used (e.g., weak passwords).
- Excessive or misconfigured network connectivity. Public clouds enable micro-segmentation by default to enforce the principle of least privilege. Network connectivity should be provisioned to the minimum needed—otherwise known as Zero Trust Networking.
- Assets, workloads, and/or services with direct connectivity to the internet.
- SSH/RDP for remote management open to the public internet.
- Data storage exposed directly to the internet.
- Data storage and file shares that are promiscuously shared.
- Data/database storage services that are not encrypted at rest.
- Improper use of encryption key management.
- Expired keys/certificates, or those nearing expiration.
- Externally facing web servers without the use of a web application firewall (WAF) or load balancer.
- APIs exposed directly to the internet.
- Use of API-based applications and services without the use of an API gateway control point.
- Any areas of infrastructure where the observed runtime state has deviated in a risky way from the desired state. Ideally, you should also proactively identify preproduction instances where a developer has deviated in a risky way from the desired state before an application is placed into production.

The value of CSPM tools is straightforward. They help organizations address the accidental side of security and compliance when deploying applications and data to the cloud.

Cloud Security Posture Management: Not Just for Security & Compliance Teams

It's clear that security and compliance will be accomplished in the future through collaboration and close relationships among IT; security; governance, risk and compliance (GRC); and DevOps teams. To that end, modern CSPM solutions are designed with security-as-a-service (SECaaS) in mind. They are easy and fast to deploy, provide simple-to-digest results and reporting, and provide subscription models that align to actual cloud usage. This means that CSPM tools provide DevOps with an effective way to integrate security and compliance measures to address potential configuration and settings issues they may have caused during development. CSPM solutions provide key capabilities for DevOps, security, IT, and GRC teams alike and contribute to the required collaboration necessary to achieve security and compliance outcomes in the future.

What's in a Name? Not Enough in Our View

CSPMs play a pivotal role in helping organizations address compliance with major mandates or frameworks. This was a driver for their development in the first place. We feel the category would be better served by the name "cloud security and compliance posture management" (CSCPM), as these tools have always focused on the value of continuous security and compliance in a strictly cloud native way.

Remediation Is King

CSPM solutions provide various remediation capabilities that are critical for teams today. It's simply not enough that security solutions alert to potential areas of risk or threat. Tools must go beyond to automatically remediate potential issues with minimal-to-no human intervention required. Doing so provides tremendous value for security and DevOps teams. In addition, remediation at a broader and even global scale means that CSPM tools can drive faster iterative change at scale across workloads and environments than what teams could do on their own.

Cloud Security Posture Management Evolution

Expect to see CSPM tools change quickly as new capabilities are added including automated provisioning, automated remediation, new threat detection capabilities (i.e., the process of addressing some of the existing intentional issues), and risk prioritization—to name a few.

ARMOR RECOMMENDATION

We hope this perspective helps you see CSPM tools in the same light we do. CSPM tools provide very clear safeguards and value to organizations that are expanding workloads into the cloud.

We recommend that organizations with applications and data in the cloud take a hard look at CSPM tools and the benefits they provide in terms of addressing security and compliance.

<table>
<tr><th>THE ACCIDENTAL</th><th>THE INTENTIONAL</th></tr>
<tr><td>CLOUD SECURITY POSTURE MANAGEMENT +</td><td>CLOUD WORKLOAD PROTECTION</td></tr>
<tr><td rowspan="4">SPEED
SCALABILITY (UP & DOWN)
SIMPLIFIED COMPLEXITY
PORTABILITY
CONSUMPTION-BASED MODEL</td><td>SECURITY & COMPLIANCE OUTCOMES</td></tr>
<tr><td>PRE-DEPLOYMENT</td></tr>
<tr><td>RUNTIME</td></tr>
<tr><td>UNIFIED VISIBILITY</td></tr>
</table>

In addition, we believe a combined approach of CSPM and defense-in-depth security protections, to address the intentional aspects of security and compliance for your workloads in the cloud, best allows organizations to maintain security and compliance of their responsible areas per the shared responsibility model.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in a private, public, or hybrid cloud—or in an on-premise IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, helps customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

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