WHITE PAPER

Architecting Security into Your Modern Enterprise

HOW TO BUILD TRUST IN THE NEW AGILE, ELASTIC, MICRO-EVERYTHING & ADAPTIVE WORLD

AUGUST 2020

<epam>

Table of Contents

Introduction

Today, everything is digital. While some enterprises are more digital than others, most companies have been pushing to become more adaptive and agile through transformation, with the goal of achieving accelerated time-to-value for customers and making services far more scalable and accessible than ever before. Concurrently, the enterprise threat landscape has become increasingly dynamic, expansive and fluid—making it harder for traditional security models and controls to defend against exploits.

The constant battle between nefarious actors against your enterprise's IT and security teams, and even against your product development and service teams requires a proactive, intentional and scalable approach to cybersecurity. The yield for attackers is only getting higher, and so the challenge is on. Those who can adapt to this new paradigm will be trusted by consumers and continue to move at an incredible speed. And those who cannot compete against malicious attackers will unfortunately face:

BRAND DAMAGE

LOSS OF CUSTOMERS

BUSINESS DISRUPTION

REGULATORY FEES (OUT OF COMPLIANCE)

Traditional measures, such as ring fencing, will still be necessary and crucial; however, these alone are not strong enough to withstand the ever-changing attack vectors. The only way to stay ahead of threats is embedding security, by design, within your organization and approaching it holistically—it must be integral to how you develop software, how you build the cloud, how you design your data strategy. And, maybe more importantly, security must be woven into your business and systems fabric, not just leveraged as a blanket perimeter measure. It has to be running in your code instead of after it. Finally, it must defend itself and not rely on rigid barriers in case something falls through. Because something always does.

Introduction (cont.)

It's time to engineer a trusted future through strategically architected cybersecurity. In this white paper, we examine the many moving parts of the security landscape and highlight the most critical areas your company should focus on.

CLOUD SECURITY

IDENTITY & ACCESS MANAGEMENT

WORKING FROM ANYWHERE

APPLICATION SECURITY

IOT SECURITY

REGULATORY NON-COMPLIANCE

DATA LOSS & BREACHES

Cloud Security

Cloud adoption has reached new heights. According to a report released in March 2020, IDC expects that 90% of enterprises worldwide "will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs" by 2022.[1] The cloud has been the obvious solution on the path to reaching flexibility and adaptability for many reasons, including:

ACCESS & SCALE

The cloud offers better scaling capabilities to help quickly accommodate changing business demands. It also provides a higher level of access because employees aren't tethered to a set workspace—as they can use business applications on any device—and can therefore move more flexibly. However, the more dynamic the environment, the the more complex it is to secure it. The good news is that, by building secure code in your software-defined network and clusters, you can scale your cloud along with your security measures.

FREQUENT, AGILE RELEASES

It's widely understood that smaller iterations and frequent releases are key to agility and faster time-to-market. The cloud enables companies to easily accomplish this, and thus dynamic application cluster rates have skyrocketed. With every new release and update, there is the potential for new vulnerabilities, and hence a set of controls built into your release pipeline is crucial so you can stay ahead of the exposure.

DATA INSIGHTS

Data-driven insights help companies make more informed decisions, faster. The value and promise of data analytics and data density that the cloud provides is huge. Data is a prime target for nefarious actors, especially when there is high data intensity. A holistic data strategy and implementation with levels of data classification is vital to target and layer controls.

Cloud Security (cont.)

With pressure to act fast, it's been absolute pandemonium for IT organizations recently—and all eyes are on IT teams to succeed. Their biggest threat against success is implementing security measures that can handle the cloud's massive scale, as traditional models are no longer suitable.

Because of the cloud's elastic, flexible and dynamic nature, IT organizations often **lose the visibility and control** they once had over assets and operations, including network boundaries and data, after transitioning to the cloud. For example, SaaS and other cloud-based services are relatively simple for individual business units to purchase or subscribe to without any oversight from the purchasing or IT departments. Unlike the **shadow IT** issues from years ago, which required some level of development efforts, users can now simply click a few links, supply a corporate credit card number and download a cloud service provider (CSP)'s API. This can lead to sharing sensitive corporate information with a **potentially vulnerable third party.**

Cloud adoption with security as an afterthought ultimately creates barriers to innovation. By building security into the system, organizations can enable the innovation and agility that the cloud promises

[1] https://www.idc.com/getdoc.jsp?containerId=prMETA46165020

Identity & Access Management

One of the most fundamental controls to protect your organization is being able to identify end users reliably and consistently—whether it's a customer, an employee or a partner. As the number of users grows, it becomes increasingly difficult to manage.

This is compounded with the fact that most modern systems involve identities from multiple sources, like CSPs, with different protocols, federated attributes and identity mappings. The following are some of the security mishaps that can occur when the IT organization does not have proper identity and access management (IAM) protocol in place:

- Employees, such as administrators, for both enterprises and CSPs **may abuse their authorized access** to networks, systems and data, and are positioned to cause damage or exfiltrate information through their access privileges.
- CSP on-demand self-service features increase unauthorized use by making it very easy for IT personnel **to provision additional resources without IT management** consent. When developers have open access to 'spin up' new virtual private cloud (VPC) instances for a PoC or demo and forget to spin it down after it's complete, this can increase operational costs because the organization will continue to be billed regardless of whether or not the resource is used.
- Services provisioned or used without IT management's knowledge present significant risks to an enterprise. The use of unauthorized cloud services **could result in malware infections or data exfiltration**, as the organization is unable to protect resources it does not know about.
- When an **attacker gains access** to a user's cloud credentials, the attacker **can then access the CSP's services to provision additional resources** (assuming the credentials allow access to provisioning), as well as target the company's assets.[2] The attacker could leverage cloud computing resources to target a company's administrative users, other companies using the same CSP or the CSP's administrators. An attacker who gains access to a CSP administrator's cloud credentials may also use those credentials to access the company's systems and data.
- Hackers may attempt to discover and compromise vulnerable, internet-accessible APIs. CSPs provide APIs to companies via the internet for interacting with and managing cloud services (also known as the management plane). These APIs may contain the same software vulnerabilities as an API for an operating system, library, etc. If a vulnerable API is discovered by a hacker, **these vulnerabilities can be turned into successful attacks, and enterprise cloud assets can be compromised**. From there, attackers can use these assets to perpetrate further attacks against other CSP users.

Mapping out a cloud-based identity management strategy is essential—it all starts with designing your identity and access strategy and implementing sustainable processes and systems. The key strategic focus areas include effectively identifying end users and assigning access privilege, segregating groups, assigning and revoking privilege access, looking for imposters and hijacked identities and maintaining the validity of the users.

[2] http://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html

Working From Anywhere

Now that remote work is more prevalent than ever before, there are significantly more entry points for attackers to exploit. With your enterprise exposed by these expanded attack surface areas, your IT organization is being stretched incredibly thin as they address the associated network and service challenges, including:

WORKSTATION & REMOTE NETWORK SECURITY

The type of device that an employee uses can have a major impact on your organization's security. For example, if an employee uses a personal device on an unsecured network, your IT team will have less visibility and control. First, you must assess what devices are being used for remote work. Then make sure that devices are updated regularly. To provide more secure network access, there are many valuable tools, such as VPN, firewalls and network traffic analysis (NTA).

NETWORK PERIMETER

Many companies on their digital transformation journey start by trying to secure cloud ring fencing, layering different products into the mix and utilizing other methods that worked well in a traditional on-premise scenarios. It's extremely challenging to ring fence when your perimeters are constantly changing, almost in real time. All endpoints must be carefully managed and treated as an extension to your existing network, while protecting and encrypting all traffic in between.

ACCOUNT ACCESS

When your entire workforce is remote, there's less visibility into and control over access. Employing the zero-trust model ensures tightened security in a remote work world. The zero-trust model must receive proper attention as early in the process as possible to make adoption easier and more cost-effective. There are different ways to approach zero trust, with the most common approach being to employ very strong IAM by verifying identity every time access to any resource is needed.

EMPLOYEE EDUCATION

Given the drastic increase in phishing attempts and business email compromises, employee education and buy-in is a critical endeavor to combat attacks. Constant and clear communication with employees, coupled with regular training programs, can help curb potential threats.

This new environment demands new security processes, and it's critical to strike a balance between moving fast and not acting too hastily in developing a plan. Effectively reducing risks will require a heightened focus on monitoring employee network activity and all remote connections, security events on key business systems, the network perimeter and employee workstations.

Application Security

Applications are complex and constantly changing. End users now expect releases in days or weeks, not months. And there is no such thing as defect-free software—each platform has its flaws, and every flaw is a potential vulnerability.

Security has to be architected into your software strategy. It cannot be an afterthought, and the only way to ensure scalability and sustainability is to tightly mesh your software and development processes. You must take both offensive (outside-in) and defensive (inside-out) approaches, aligning them with governance and compliance.

To secure your applications in the new agile and DevOps world, you need a well-designed security program from day one. The architecture of an application is critical from a security perspective because it could either simplify and harden the system or introduce weakness or difficult-to-control attributes.

It could also push the responsibility down to the production environment, making it much harder to secure and far more complex to keep up to date. Layering is key to increasing the effort needed for attackers to get to your digital assets.

Ultimately, you need to pair up your controls with modern methodologies and tools to help your developers build better and more secure software, while maintaining DevOps speed.

IoT Security

IoT devices are pervasive and hold a lot of valuable information about the way your company does business. As more and more data is generated through these devices and floods your enterprise systems, it becomes highly vulnerable for a number of reasons.

First and foremost, these devices largely take the form of legacy hardware and were designed to be left unattended. This means that they're extremely difficult to manage properly and are limited as to when they can be patched and updated. Here are some of the high-level security complexities to consider:

IDENTIFICATION

There are many ways to spoof, replicate and even corrupt data from less powerful IoT devices and sensors. Trusting your incoming IoT data all starts with reliable device identity. While it's still difficult to secure and prevent lifting, embedding signed identities or hidden keys is a good first step.

LEGACY HARDWARE

Not all edge devices can be patched or upgraded remotely, or even on-site, making it hard to stay up to date regarding known vulnerabilities. In fact, one of the most common attacks is to scan for devices with older software and exploit well-known configurations or software defects.

LOWER-END DEVICES

Implementing strong protection, monitoring and encryption in IoT and edge devices is a challenge because they're usually less powerful when it comes to CPU, memory and storage.

DATA VOLUME

The amount of data generated by sensors and actuators presents a different level of complexity, especially when the data is mixed with both sensitive and raw data—sometimes even in the same stream.

Because of their scale and nature of deployment, securing both the edge devices and communication channels and the information they generate are challenging. Therefore, they're a big target for botnet and often used for load generation and as an entry point for attacks.

The key to success is to take an end-to-end approach by architecting and building back-end functionality and chart security measures to ensure that the widely dispersed raw data that IoT devices produce is properly protected.

Regulatory Non-Compliance

Today's regulatory agencies have put increased scrutiny on data protection. When IT organizations have less visibility into enterprise data storage, particularly in the cloud, they're less capable of verifying that data was securely deleted.

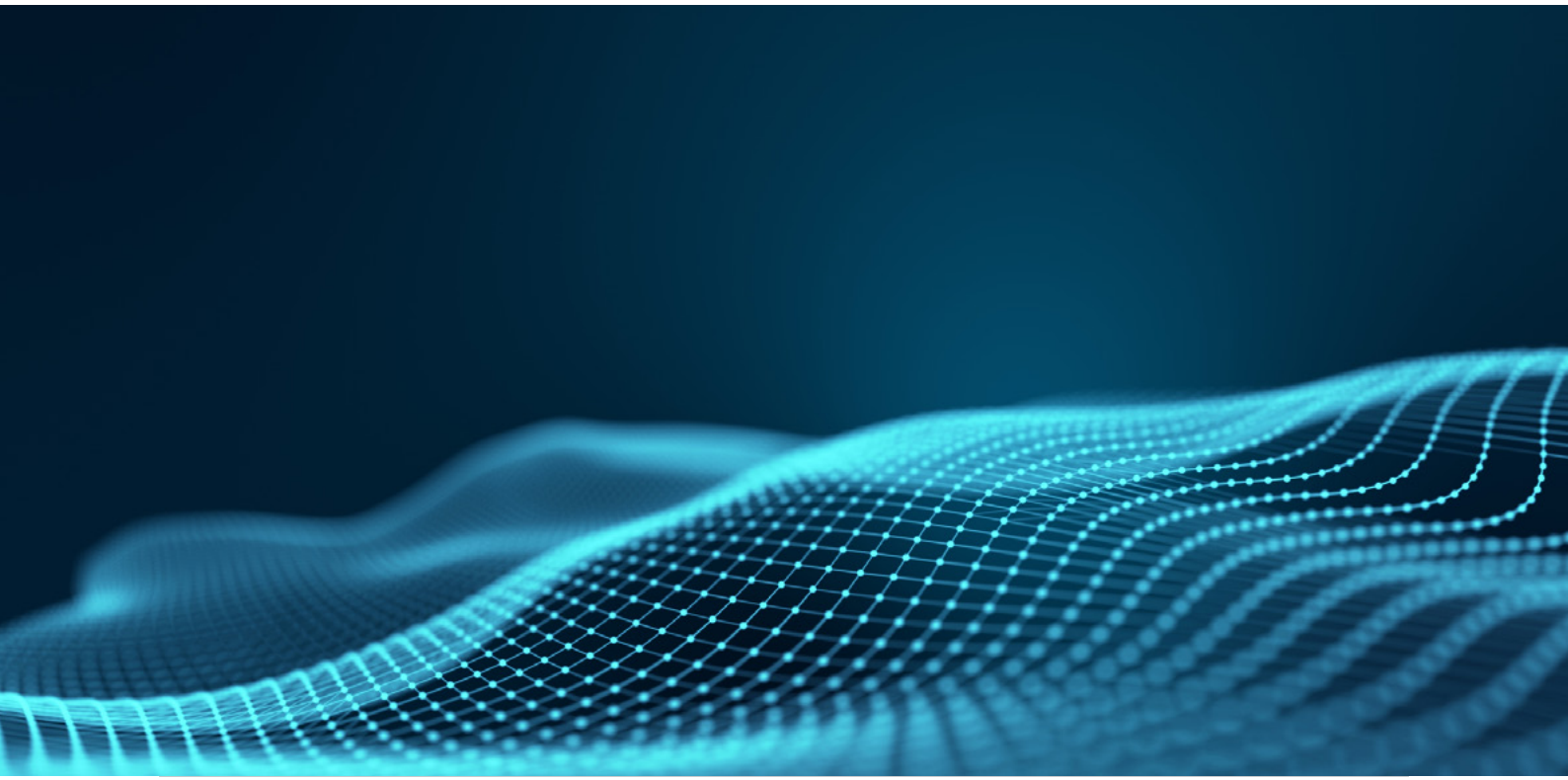
If a CSP outsources parts of its infrastructure, operations or maintenance, these **third parties may not support the requirements that the CSP** is contracted to provide with a company. A company must evaluate how the CSP enforces compliance and check to see if the CSP flows its own requirements down to third parties. If the requirements are not being levied on the supply chain, then the threat to the company grows, and increases further if a company uses more CSP services.

Non-compliance with regulatory requirements, such as GLBA, CCPA, SOX, HIPAA or GDPR, **may result in significant fines and penalties.** For example: 1) GDPR fines can be up to 4% of global revenues or $20M, whichever is higher[3]; 2) Fines under the CCPA's Direct Right of Action clause can be $100-750 per consumer incident as part of civil penalties while the state can issue fines of up to $2,500 per accidental violation/$7,500 per intentional violation.[4]

When governance and compliance are built into your software, this is called Compliance as Code, where you perform constant micro audits as part of your automation strategy. The reports are near real time, and focus on continuous improvements and actionable outcomes.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1

[4] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375



Data Loss & Breaches

Data loss in the cloud can occur for many reasons, such as malicious attacks, accidental deletion of data by the CSP or a major physical outage. The burden of avoiding data loss and leak does not fall solely on the CSP's shoulders. For example, if a company encrypts data before uploading it to the cloud but loses the encryption key, the data will be lost.

This risk of data loss increases as organizations use more CSP services. Recovering data from a CSP may be easier than recovering it on an on-premise environment because an SLA designates availability and uptime percentages.

If system and software vulnerabilities are exploited within a CSP's infrastructure, platforms or applications that support multitenancy, this can result in a failure to maintain separation among tenants. Data breach events against a multi-tenancy environment could lead to a much larger data spillage event beyond a single tenant environment. As a result, multitenant environments represent a more advantageous target for hackers.

It's critical to have a cloud-specific data security strategy since this is where most data lives nowadays. This starts with your data classification and takes into account your elastic and agile access semantics. Then, carefully look at your encryption strategy—at rest, in use and in transit—and make sure you understand how the keys are managed and refreshed. Last but not least, have a robust loss prevention and service continuity plan.

Taking a Holistic Look at Your Security Program

Your security measures, or lack thereof, can make or break your business. Ideally, an enterprise should prioritize charting a well-defined security roadmap. More often than not, companies perform insufficient due diligence, making moves without understanding the full scope of security or considering both their own and their vendors' measures. Without accounting for the entire security environment, companies become susceptible to the many risks we've outlined and turn into prime targets for attack.

For your company to manage security effectively, it must be architected into your digital ecosystem. In addition, you need a combination of proactive (offensive security) and reactive (defensive security) measures within a governance model, with each pillar working together continuously and synchronously. Security cannot be an afterthought. It requires gaining full organizational support as well as clearly defining and periodically updating internal ownership to account for any changes. Additionally, any risks must be communicated to internal stakeholders, including C-level management, as part of governance flow, to enable better risk transparency.

In order to keep pace with the rapidly changing threat landscape, it's important to assemble a team that regularly keeps track of what's happening more broadly in the cloud security market and ensure that these updates are tied close to processes and the governance model.

The first step: Start with an overall assessment of your security posture, understand your exposure and weaknesses, and design in a cybersecurity strategy that can match your business agility and speed.

ABOUT EPAM

Since 1993, EPAM Systems, Inc. (NYSE: EPAM) has leveraged its software engineering expertise to become a leading global product development, digital platform engineering, and top digital and product design agency. Through its 'Engineering DNA' and innovative strategy, consulting, and design capabilities, EPAM works in collaboration with its customers to deliver next-gen solutions that turn complex business challenges into real business outcomes. EPAM's global teams serve customers in more than 30 countries across North America, Europe, Asia and Australia. As a recognized market leader in multiple categories among top global independent research agencies, EPAM was one of only four technology companies to appear on Forbes 25 Fastest Growing Public Tech Companies list every year of publication since 2013 and was the only IT services company featured on Fortune's 100 Fastest-Growing Companies list of 2019.

Learn more at **www.epam.com** and follow us on **Twitter @EPAMSYSTEMS** and **LinkedIn.**

GLOBAL

41 University Drive,
Suite 202
Newtown, PA 18940, USA

P: +1-267-759-9000

F: +1-267-759-8989

B762_v4_08/2020

<epam>