Alibaba Cloud

Optimize Infrastructure and Application Security with Alibaba Cloud Solutions

Contents

01 Overview

The constantly transforming technological landscape has made our lives better, with digitization, mobility, and the Internet of Things (IoT) currently at the forefront. Using multiple devices is the new normal, and it is now almost unthinkable to live without our smartphones or tablets. Organizations have embraced the need for employees to use personal devices, with the concept of Bring-Your-Own-Device (BYOD) flourishing.

Furthermore, IoT has empowered consumers and organizations with smart devices that generate tons of data and insights, which help make smarter decisions. However, such data is also at risk of being stolen by cyber criminals. The average cost of a data breach in 2020 is projected to be more than USD $150 million according to Juniper Research. Security experts attribute this threat to the increasing connectivity (both inter and intra) between business infrastructures and to the rise of the public cloud.

This whitepaper looks at various categories of security risks, such as physical and logical, that organizations face today, and discusses new vulnerabilities that cyber criminals can exploit. It also evaluates the drawbacks and limitations of existing security solutions and then moves on to discuss Alibaba Cloud Security Solutions for gaining stronger immunity against physical and logical security threats. Finally, it discusses the superiority and suitability of these solutions in helping organizations achieve their security goals.

02 Introduction to Security

Technological advancement has long been a difficult balance between progress and solving new challenges. The drawback of increased connectedness is that such technologies are not fail-proof. Cyber criminals can draw on a wide array of techniques that have advanced over the years, and which organizations and consumers struggle to keep apace in mitigating. The proliferation of devices connected to the internet, along with the boom in personal devices, has offered attackers ample opportunities to exploit users. Industry reports predict that cybercrime will cost businesses USD $2 trillion by 2019.

There has also been seismic growth in cybercrime, both in its sophistication and effectiveness. Cybercriminals have shifted their focus towards the corporate world after identifying potential for bigger rewards. They are adopting techniques traditionally seen in advanced espionage attacks and are using them for targeted infections. This further reiterates that cybercrime is maturing, and that organizations are on the radar of cyber criminals.

This was highlighted by two breaches of Yahoo in the last quarter of 2016, when it reported two major data breaches. The first breach occurred in 2013 when personal information related to one billion Yahoo accounts was compromised. Then, in 2014, a hacker stole account information from at least 500 million user accounts.

These examples make a strong case for cyber security. However, physical security is equally important from an organization's perspective, especially as the interdependence between physical and logical security is as important now as ever. As a result, strong integration between the two is needed. Defending against cyber attacks is meaningless if attackers can gain physical access to an organization's infrastructure, such as a server or personal computer. This increases the threat of attacks launched by an insider with access to internal hardware. To maintain security, organizations should defend against all potential threat sources.

03 Prevalent Security Threats in the Cloud Landscape

3.1 Attacks due to Architectural Vulnerabilities

Cyber criminals hack web servers for two reasons; to control servers and to spread malicious programs. A typical server offers much more bandwidth to carry out more effective attacks, as compared to an attack launched from an individual workstation. Servers allow hackers to launch attacks from one location, instead of using multiple workstations. Further, servers are available around the clock, unlike a personal computer.

Typically, cyber criminals profit from conducting cyber attacks either by selling stolen data or by demanding ransom for returning hacked files. On other occasions, hackers do this merely as a form of mischief, with no particular goal in mind. They are likely to use malicious attacks to uncover secret and confidential information from enterprises or even governments. According to Verizon's annual Data Breach Investigations Report released in 2016, 89% of all cyber-attacks involve espionage or financial motivations.

Protecting web servers is critical. Not only can a company lose data, but cyber criminals can use the server to infiltrate the company's network. It can be used to launch new attacks on other businesses.

Enterprise networks are now without physical boundaries and are more fluid than before. IT teams require tools for visibility into their installed asset base and related activities. As employees connect their devices to the network remotely, these devices simultaneously connect to other networks and devices. Organizations cannot control the security of these devices, and they do not know which devices are legitimate. Such a high volume of connections overwhelms organizations as they struggle to monitor all devices. This benefits the attacker, as the organization is less equipped to defend itself.

3.2 Internet of Things

The burgeoning of cyber-physical systems and the Internet of Things (IoT) has opened up new opportunities for cyber criminals to exploit connected devices and launch large-scale attacks.

This can be attributed to the poor monitoring and security of IoT-enabled devices, which makes them easier to manipulate. Devices can be enslaved to launch distributed denial-of-service (DDoS) attacks, or they can be used to hack private networks and remotely distribute malicious software. Launching destructive attacks has become easier and has reduced barriers to entry for cyber criminals.

What's more, with devices connected to the same network, a single vulnerable or infected device can act as a gateway to the hundreds or thousands of other inter-connected devices. Ensuring zero vulnerability for all devices is tough, which makes it easier for cyber criminals to find a target for launching an attack. There are options like botnets and rootkits for them to use, while there is no dearth of possible entry points into a network. Cyber criminals leverage hacked IoT devices as proxies to carry out attacks, with attackers able to mask their real location to remain anonymous.

3.3 Ransomware

Ransomware consists of malicious programs (malware) that infiltrate an organization's IT infrastructure and locks valuable data with high encryption that is difficult to decrypt. After compromising a server, attackers can move within the network and push the malware into thousands of computers and end-user devices. Typically, data remains in the original location. However, after ransomware is implanted in a server, anyone without the decryption key will not be able to access the files on that server.

Ransomware attacks are on the rise, with Kaspersky reporting that more than 4,000 ransomware attacks have occurred daily since early 2016. One of the main reasons for this has been the growth of encryption techniques. This has resulted in a 600% increase in new ransomware families since December 2015. It is important that organizations boost their security to prevent ransomware attacks, as they stand to lose significant revenue during downtime. Organizations may have to shut down systems to deal with the infection and prevent it from spreading. Consequently, their reputation will also take a hit.

Further, the risk of losing sensitive data, including company records, intellectual property, or customer information, can cause irreversible damage to an organization's brand value and erode consumer confidence. There is no guarantee attackers will share the decryption key after they receive the ransom. Hackers may even threaten to publicize the stolen data to coax more money from the targeted organization. Even if this doesn't eventuate, similar attacks can occur again if the affected organization does not upgrade its security infrastructure.

A ransomware attack against a Los Angeles hospital system, Hollywood Presbyterian Medical Center (HPMC) was carried out in 2016, which allegedly demanded a ransom of USD $3.4 million. The attack blocked access to the company's network, email, and patient data for ten days.

In such situations, the affected organization has to decide whether it is going to give in to the attacker's demands and pay the ransom. If they refuse, they run the risk of having to wait indefinitely for the files to be restored from backup. A healthcare organization or a financial institution might not be able to wait, and hence have no choice but to pay the ransom. Another concern is that the attackers might destroy the decryption key if the ransom is not paid by the set deadline, with the organization permanently losing all its data. This is what has made ransomware an effective weapon for cyber criminals.

3.4 Mobility and Bring Your Own Device

With the growth in mobility, employees now use personal devices for work. Realizing the changing expectations of employees, organizations have developed a variety of Bring Your Own Device (BYOD) policies. Although this has increased the productivity of the workforce, the scenario increases security risks. BYOD has reduced the control and security measures organizations can deploy. While traditionally they could focus on their in-house infrastructure, now IT departments have to contend with a plethora of devices outside that perimeter.

Users can access organizational data via the Internet on their smartphones. The boundary between work and personal usage is consequently blurred. A user might unknowingly download a malicious application or software for personal use, which can compromise organizational data on the device, with organizations having no control over the situation. With numerous devices to potentially target, the attack vector for criminals has expanded significantly.

As such, mobility has redefined how organizations look at their IT infrastructure, with devices no longer located on-premise falling under their purview. A holistic approach to security that clearly defines the security risk is essential to counter threats and safeguard organizational data on personal devices.

3.5 Physical Security Threats

Organizations should be wary of all physical security threats that exist. They should not fall into the trap of ignoring physical security, as there might be a natural tendency to do so with the prime focus always being on cyber security and cyber threats. Threats need not always use the online channel.

Online hackers are not the only cause of data breaches and other debilitating cyber attacks. Internal employees of an organization with authorized access to sensitive elements of the IT infrastructure can likewise cause cyber attacks. Such insider threats should be taken seriously, with Verizon reporting that 77% of data breaches in 2015 involved an insider. The motivation for insider attacks range from emotionally driven attacks, such as revenge over losing employment, a bad performance review, or another office incident prompting an employee to seek ways to sabotage their employer. Additionally, financial hardships can push employees to steal sensitive information and sell it on the dark web.

Although unlikely, a hacker may physically enter an organization's premises to set off an attack from the inside. Any person with malicious intentions who can physically access an organization's laptop or server will be in a position to breach security and compromise the organization's availability and the integrity of information systems.

Another scenario where physical security plays a key role is during a natural disaster like an earthquake, flood, hurricane, or a fire. In such cases, organizations can permanently lose their entire data center, or fundamental parts of it. It is imperative that companies take note of the physical security of their IT facilities to maintain organizational security.

04 Shortcomings of Existing Security Solutions

The current physical and logical security measures deployed by organizations are not in sync. This is a huge problem because physical security vulnerabilities can prevent organizations from achieving their cyber security goals. This lack of integration makes access management a challenging task, as the current processes used for monitoring and managing physical access are complex and inefficient. This increases the threat of insider security breaches. Hence, there should be high integration between physical and network access.

On the cyber security side, servers typically have installed within them many types of firewall and protection software that claim to defend against Distributed Denial of Service (DDoS) attacks. However, given the restrictions imposed on them by the server's inbound bandwidth, these methods can only filter minuscule DDoS attacks. If a DDoS attack exceeds a server's inbound bandwidth, the server's protection software is of no use. At the same time, when this security software runs statistical calculations, it occupies CPU and memory resources. Therefore, while providing defense, this software affects server performance to a certain extent.

In addition, a content delivery network (CDN) commonly used to achieve website acceleration and distributed access with smart DNS, can mitigate DDoS attacks, but cannot protect against a customized application attack.

Since the launch of firewall hardware in 2000, professional scrubbing and firewall hardware have matured in defense algorithms and detection capabilities. To effectively deploy them, the expertise of a professional operator to adjust configurations is desirable. Even if a user purchases defense equipment that can combat an attack of 100 Gbps, the services on the user's server are affected by a 1Gbps DDoS attack due to 1Gbps outbound bandwidth.

Web Application Firewall is a popular product used to defend against malicious web attacks. Typically, it provides protection for web access. However, it is unsuitable for database protection, because database access requires multiple sources, apart from web-based applications. Other sources like internal organization applications also access databases and are a potential source for data breaches. However, traditionally WAF ignores this traffic as it focuses on outside access concerning HTTP traffic. This leaves the door open for inside traffic to wreak havoc.

Typically, at least three different types of access to a database exist outside of web access. Firstly, other systems in an organization may access the database. For example, an e-commerce app sometimes updates prices and inventory through different automated processes.

Secondly, individuals may access the database through internal applications that may have an interface through which employees can add notes or send information to customers. Finally, for all databases, there are database administrators (DBA), IT managers, Quality Assurance (QA) teams, and programmers with access to the database. Each entity accessing the database is a potential source of database breach.

Cyber attacks aimed at internal systems and computers are attacks that bypass WAF, intrusion prevention systems, and other web based protection systems.

05 Alibaba Cloud Solutions

With increased focus on enhancing organizational security, Alibaba Cloud has invested in state-of-the-art security solutions to help businesses counter new security threats. Understanding an organization's need for an effective solution that seamlessly integrates physical and logical security, Alibaba Cloud offers a range of security solutions to maintain high availability and minimize the risk of malicious attacks. Outlined below are the security solutions that Alibaba Cloud offers.

5.1 Anti-DDoS Security

5.1.1 Anti-DDoS Basic

Alibaba Cloud Anti-DDoS Basic is a cloud-based security service that integrates with Alibaba Cloud ECS instances and offers DDoS attack mitigation by routing traffic away from your infrastructure. It also features auto-detection and prevention of various types of attacks, including those at the application and volumetric level. As an Alibaba Cloud global service, Anti-DDoS Basic enables you to meet stringent security requirements for your cloud hosting architecture without any investment.

5.1.1.1 Features

Reliable

Quickly detects attacks, launching a defense in real-time to protect customer data and applications from DDoS attacks.

Protection Against Vulnerabilites

Offers a protected cloud with comprehensive security protection for all Alibaba Cloud deployments.

Simple to Use

Convenient to use from the Alibaba Cloud Management Console. No alterations are required for CNAMEs or name servers which save overhead costs.

Secure

Defend against different types of DDoS attacks, such as SYNflood, UDPflood, and ICMP flood. The product also delivers real-time information to users on existing site attacks.

Notifications

Sends automatic notifications to users via text messages or email about attack related information, including intrusion time, targeted ECS instances, with real-time alerts for active DDoS attacks.

5.1.2 Anti-DDoS Pro

5.1.2.1 Features

Alibaba Cloud Anti-DDoS Pro is a flagship security service developed by Alibaba Cloud. It is an attack protection service, designed by the Alibaba Cloud security R&D team. The product can defend against layer-3 to layer-7 DDoS attacks such as SYN flood, UDP flood, ACK flood, ICMP flood, DNS Query flood, NTP Reflection and Amplification flood, HTTP flood and web application attacks.

To achieve this, it resolves the domain name to the Anti-DDoS server for web services by replacing the service IP address of the application server with the IP address of the Anti-DDoS server for non-web services and configuring the user's source site IP address.

This directs all public network traffic to the Anti-DDoS server, which then forwards user access traffic to the origin site IP address. In this process, the Anti-DDoS server cleans and filters out malicious traffic, with only traffic deemed safe returned, also ensuring stable access to the origin site IP address.

5.1.2.2 Defense against DDoS Attacks

Anti-DDoS Pro offers the following mechanisms for defending against DDoS attacks:

Real-time Detection

Anti-DDoS Pro performs real-time detection and mitigation on all incoming traffic. It can detect DDoS attacks in real-time by studying the traffic composition and baselines.

Protocols Filtering

Filters and drops out TCP/UDP fragments and packets with illegal TCP flags or protocols.

Source IP Authentication

Uses a unique source IP authentication algorithm designed primarily to identify and filter requests from spoofed IP addresses.

Blacklisting Malicious Source and Destination IPs

Limits traffic based on the source or destination IPs, to stay within the corresponding traffic threshold, to prevent overloading of the server. It also blacklists all malicious IP addresses detected.

IP Reputation Check

With the help of big data generated insights, Alibaba Cloud tracks IP addresses from all over the Internet and filters out traffic with sub-standard record and reputation as well as spoofed IP addresses.

Attack Fingerprint Pool

Through policy learning, the system regularly updates the pool with new and common attacks of botnets and malware to identify and filter known attacks.

Full-site Protocol Support

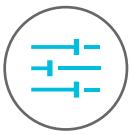
Anti-DDoS Pro provides full support for the TCP/UDP/DNS/HTTP/HTTPS protocol stack. In addition to websites, the service can also protect games, audio/video, and mobile application services.

5.1.2.3 Defense against HTTP Flood Attacks

As part of its holistic approach to defending against HTTP Flood Attacks, Anti-DDoS Pro has different solutions for each of the steps involved.

Detection

Computes the frequency of requests, cookies, referrers, URLs, and other related fields of a user's URL. This information helps create policies for detecting HTTP flood attacks.



Configuration

A user can specify the URLs (regular expressions supported) and URL groups considered suspicious, and hence need to be blocked on detection. The policies for detecting HTTP flood attacks for various URL groups can be different.

Cookie/source/browser Authentication

This service performs authentication by matching verification information and eliminating malicious requests which can cause HTTP flood attacks.

Time-related Parameters

Automatically updates parameters such as maximum access times, post times, and frozen duration for each of the attacks without any manual setup.

Identification of Genuine IP Addresses using Proxy Servers

When a proxy server is used to initiate HTTP flood attacks, the service automatically identifies the genuine IP address and filters out malicious requests.

QPS Limitation

Sets mandatory QPS flow controls to set an upper limit of queries that web servers have to process. This ensures they do not crash due to an excessive number of queries. However, a user can specify the URLs (regular expressions supported) and change the set limit for queries.

5.2 Web Application Firewall

Web Application Firewall (WAF) is a web application based security Software-as-a-Service (SaaS) product that helps protect and secure sensitive organizational data. It detects malicious web requests through its built-in security strategy. Organizations need to change their website's DNS records so that all requests pass through WAF. This enables it to provide protection against web-based attacks including SQL injections, XSS, Malicious BOT, command execution vulnerabilities, and other common web attacks.

The primary benefit of WAF is that it protects against custom web applications, which would otherwise be unprotected when guarded using other technologies that only shield against known threats.

WAF also protects web applications by inspecting incoming traffic and controlling access to them. It decouples the traffic between a web server and the Internet, hence ensuring browsers are not connected directly to the web server. It identifies and takes defensive action against threats maliciously woven into innocent-looking website traffic that slips through traditional defenses. This includes blocking technical and business logic attacks before fraudulent transactions are processed.

Alibaba Cloud WAF effectively integrates black/white list rules, logic algorithms, threat intelligence, and user behavior-based learning models to block malicious requests. It also defends against the OWASP top 10 web vulnerabilities to protect any website.

5.2.1 Features

Following are some specific features of WAF:

Precise Access Control

WAF handles cyber attacks by controlling frequent access from a single or range of source IPs, providing redirect jump verification, and determining whether the access requests are raised by a human operator or a machine. Along with the precise access control filters, WAF uses the abnormal referer and user-Agent fields to protect against massive slow request attacks and identify abnormal response codes, IPs, and URL distributions.

WAF Modes

To meet varying needs of organizations, WAF operates in two distinct modes. In the Prevention Mode, it actively blocks intrusions and attacks detected by its set rules. In the Friendly Observation Mode, it enables observation mode for new website services. In this mode, WAF issues warnings for possible attacks that match the protection rules but does not block them, thereby reducing the false-positive.

WAF also provides real-time request level protection for web applications through in-depth analysis of HTTP/HTTPS traffic. Compared to traditional firewalls, it completely parses and verifies each field of an HTTP request including common HTTP headers, referer, user-agent, URL, and request parameters.

5.3 Mobile Security

Alibaba Cloud Mobile Security service ensures the security of mobile applications with extensive vulnerability testing and malware protection. It ensures end-to-end protection throughout the mobile application lifecycle, through the design, development, testing and release phases.

5.3.1 Features

The following are key features of this solution.

Quick Application Vulnerability Detection

For static vulnerability detection, this service scans and locates vulnerabilities by performing taint analysis to retrieve variable values accurately. It also analyzes and tracks vulnerabilities at the granularity of the register. For dynamic vulnerability detection, it performs Fuzz testing to restore the real Android environment.

Application Vulnerabilities Resolution

A complete remedial solution is offered for mobile applications based on the vulnerability scan results.

Advanced Security with Application Hardening

Various methods like re-encoding, shelling, and modifying the command calling sequence are deployed to enhance the anti-cracking capability of your application. It also uses techniques that focus on application hardening intensity, while maintaining the compatibility of your application. It effectively prevents hackers from using static analysis tools such as APKTool, dex2jar, and JEB to analyze applications' Java-layer code.

Core Application Hardening Techniques

- **SO shelling -** The SO file is shelled to effectively prevent malicious users from using tools such as IDA and readelf to analyze SO file logic.
- **DEX shelling -** The DEX file is shelled by using loading and remedial techniques during dynamic running. This effectively prevents hackers from dumping the Java-layer code memory.
- **Constant Encryption -** Plaintext constant strings are encrypted in the DEX file. The dynamic decryption feature is leveraged to decrypt strings during runtime, greatly increasing the difficulty in reverse analysis.
- **Java Command Translation –** The calling relationship link of the service logic at the Java layer is modified to ensure the protection of the Java-layer code from hackers, by denying access to the entire service logic.
- **Java Execution Simulation -** Commands are detached from the DEX file, with execution simulated in a user-defined execution environment. This helps effectively prevent malicious users from getting a dump of any Java-layer code using commands.

5.4 Physical Security Solutions

5.4.1 Access Controls

Alibaba Cloud has established stringent access management processes, including access card systems and fingerprint access control systems, to ensure only authorized users enter the respective facility. Users need to request visitor access to a data center and server room areas and get approval before the visit. This gives the organization time to conduct a thorough background check and avoid allowing access to anyone with malicious intent.

A valid official identification document (ID) is required during registration. An on-site operator must accompany visitors during the visit to the server room areas. Data center managers perform a monthly review of the access card system and fingerprint access control system to ensure that only authorized personnel gain access.

5.4.2 Decommissioning

Discarded or damaged data storage media must be demagnetized and bent for data removal before being removed from a data center. To deliver optimum data security, Alibaba Cloud has agreements in place with hardware providers to ensure that no storage media is returned to them.

5.4.3 Security Monitoring

Data center facility management is responsible for monitoring the intercom and emergency communication systems, smoke detectors, lightning protection and grounding devices, fire alarms and sprinkler systems, power supply, electrical circuit system and control panels, ventilation and air conditioning systems. Also, personnel on duty monitor the operation of data centers 24/7. Video surveillance is installed at the entrance, equipment delivery areas and dedicated areas within the data centers. Security personnel present on-site perform inspections to prevent unauthorized access.

Alibaba Cloud maintains the risk inventory of each data center, and communicates the risk inventory to the corresponding risk manager, who is responsible for conducting risk assessments and periodic contingency drill testing, with suppliers asked to issue an improvement plan for operational risks. In this way, Alibaba Cloud can manage the day-to-day operations of all IT infrastructure while ensuring maximum security.

5.5 Logical Security Solutions

5.5.1 Access Provisioning

Alibaba Cloud has policies and procedures established for logical access management of employees. The operations personnel manage cloud products or services through the operations platform. Access is granted with role-based access controls (RBAC), which follow the rule of the least privileges necessary for the operations platform. Controls are set to ensure segregation of duties and access rights in consultation with the client. Alibaba Cloud also enforces two-factor authentication to authenticate users. Upon employment termination, the Human Resource system automatically synchronizes users' termination information with other systems to ensure such employees cannot enter the facility.

5.5.2 Network Security

A network configuration scanning tool is deployed to scan network device configurations within the network security domains on a daily basis. Alibaba Cloud's security team follows up on the scan results and documents the results together with any action items. Network device configuration is backed up to ensure timely recovery of configurations whenever needed.

5.5.3 Data Transmission

Alibaba Cloud supports secure communication channels with strong cryptographic protocols for safe data transmission. Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is deployed in the Management Console and Open API gateway of Alibaba Cloud. Also offered is Alibaba Cloud Security Certificate Service, in which tenants can purchase and deploy digital certificates directly through Alibaba Cloud's platform to replace Hyper Text Transfer Protocol (HTTP) with HTTPS to implement transmission encryption.

Alibaba Cloud also supports IPSec VPN and leased line connections, which tenants can apply for by submitting tickets to access the cloud environment for service management and data transmission and to establish secure communication channels. This ensures customers have complete visibility over their usage, and no one can hack into their accounts and provision resources without their knowledge.

5.5.4 Key Management Service

Customers are granted full control over the management of keys that are used to encrypt/decrypt data on the Alibaba Cloud platform, ensuring optimum data privacy and security.

06 How Alibaba Cloud Leads the Way

6.1 Anti-DDoS Security

Anti-DDoS Pro supports both BGP and DNS diversion technologies. Its primary protection method is the automatic mitigation technique supplemented by active suppression. Besides traditional mitigation policies such as proxy, detection, authentication, blacklisting/whitelisting, and packet compliance, Anti-DDoS Pro also integrates web security, reputation analysis, layer-7 application analysis, user behavior analysis, feature learning, and other advanced technologies. Thus, the service blocks and filters all threats, ensuring uninterrupted services even in the case of a sustained attack. It also provides TBPS level protection mitigation capacity, and over 2 Tbps DDoS mitigation capacity.

The Anti-DDoS Pro team includes industry veterans and experts working under various departments including hardware R&D, software R&D, software/hardware testing, technology support, and security operations.

6.2 Web Application Firewall

Alibaba Cloud WAF fulfills the web security requirements of all HTTPS websites. In addition to stability, it provides powerful mitigation capabilities. It includes big data capabilities to provide more precise and accurate attack detection services based on advanced threat intelligence techniques.

WAF offers a convenient and straightforward access model as compared to conventional WAF vendors, allowing users to deploy its security services within minutes. It also lets users customize protection rules as per the requirement of different websites. Its entire inspection process takes place within minutes without affecting business operations.

Alibaba Cloud WAF also provides detailed business data analysis and security data reports to improve customers understanding of their business and security risk situations. Furthermore, WAF clusters ensure the security of websites which experience high traffic. Its advanced security operation capabilities include zero-day patching, website rule maintenance, detailed attack analysis, and other value-added services.

6.3 Big Data Capability

Alibaba Cloud uses threat intelligence from insights derived from big data. With cloud computing aggregating tons of data, there is ample opportunity to detect trends for superior insights. Latest threat intelligence is acquired by analyzing and computing PB-level data every day, which builds the core competitiveness of Alibaba Cloud Security. Further, Alibaba Cloud monitors over 2.5 million active malicious IPs globally, with samples for over 10 million backdoor files as well as their usages recorded. This empowers customers to make data-driven decisions, and ensure we are ready to deal with security threats as they evolve.

Alibaba Cloud blocks more than 0.8 billion attacks every day, while also blocking 200 million brute-force attacks and 20 million web application attacks each day. Alibaba Cloud also maintains an updated malicious IP database, along with information on popular patterns, methods, and signatures deployed by cyber criminals.

07 Conclusion

Security is of paramount importance for organizations, and especially as the growing influence of new technologies like IoT and Mobility increase the number of security threats. While these technologies have made processes more efficient, they have offered new avenues for cyber criminals to exploit. As such, enhancing defense mechanisms to stay on top of threats is critical.

It is imperative for organizations to deploy a converged security strategy, with physical and logical security going hand in hand. This is the only way to achieve organizational objectives from a security standpoint.

Alibaba Cloud offers a gamut of security solutions that include Anti-DDoS security, Web Application Firewall, mobile security, and access management that help organizations safeguard their data and overcome all types of security threats while enjoying the benefits of developing technologies. With extensive experience in defending against multiple malicious web-based attacks, Alibaba Cloud is well placed to assist your organization in achieving superior security outcomes.

References

1. http://www.cloudsecurityresource.com/topics/cloud-security/articles/423953-why-need-web-application-firewall-waf.htm

2. http://www.securitysales.com/article/physical_identity_and_acccess_management_critical_for_stopping_insider_cybe

3. http://www.information-age.com/internet-things-impacting-enterprise-networks-123463122/

4. http://www.hexatier.com/why-web-application-firewalls-waf-only-cannot-protect-your-databases/

5. https://blog.apnic.net/2014/11/11/physical-security-is-part-of-cyber-security

6. https://esj.com/articles/2012/03/19/integrating-physical-and-cyber-security.aspx

7. https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/

8. https://cloudtweaks.com/2016/10/ddos-iot-new-era-cyber-crime/

9. http://blog.trendmicro.com/cyber-crime-the-2-trillion-problem-part-1/

10. http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

Alibaba Cloud